Algebra

by

Stephen S. Shatz* and Jean Gallier**

*Department of Mathematics
**Department of Computer and Information Science
University of Pennsylvania
Philadelphia, PA 19104, USA

August 5, 2023

To the memories of Peter A. Cassileth, Stanley M.K. Chung, and Ralph C. Marcove, physicians and friends all. Being mortal and denied the gift of life, he gives and they gave the next best thing: Time.

To Anne, Mia, Philippe and Sylvie

Contents

Preface **vii**

For the Student **ix**

Problems **1**

1 Group Theory **57**
1.1 Introduction . . . 57
1.2 Group Actions and First Applications; The Three Sylow Theorems . . . 57
1.3 Elementary Theory of p-Groups . . . 69
1.4 Group Extensions . . . 75
1.5 Solvable and Nilpotent Groups . . . 88
1.6 Ω-Groups and the Jordan-Hölder-Schreier Theorem . . . 92
1.7 Categories, Functors and Free Groups . . . 95
1.8 Further Readings . . . 108

2 Rings and Modules **109**
2.1 Introduction . . . 109
2.2 Polynomial Rings, Commutative and Noncommutative . . . 109
2.3 Operations on Modules; Finiteness Conditions . . . 115
2.4 Projective and Injective Modules . . . 125
2.5 The Five Lemma and the Snake Lemma . . . 137
2.6 Tensor Products and Flat Modules . . . 140
2.7 Limit Processes in Algebra . . . 157
2.8 Flat Modules (Again) . . . 164
2.9 Further Readings . . . 172

3 Commutative Rings **173**
3.1 Introduction . . . 173
3.2 Classical Localization . . . 173
3.3 Prime and Maximal Ideals . . . 179
3.4 First Applications of Fraction Rings . . . 194
3.5 Integral Dependence . . . 203
3.6 Primary Decomposition . . . 223
3.7 Theorems of Krull and Artin–Rees . . . 236
3.8 Further Readings . . . 242

4 Fields and Galois Theory **243**
4.1 Introduction . . . 243
4.2 Algebraic Extensions . . . 243
4.3 Separable Extensions, Kähler Differentials, Mac Lane's Criterion . . . 248
4.4 The Extension Lemma and Splitting Fields . . . 256
4.5 The Theorems of Dedekind and Artin; Galois Groups . . . 260
4.6 Primitive Elements, Normal Bases . . . 270
4.7 Galois Cohomology, Norms and Traces . . . 277
4.8 Krull's Galois Theory . . . 284
4.9 Kummer Theory . . . 289
4.10 An Amazing Theorem of Galois Theory . . . 294
4.11 Algebraic Closures; Steinitz's Theory of Fields . . . 298
4.12 Further Readings . . . 308

5 Homological Algebra **309**
5.1 Introduction . . . 309
5.2 Complexes, Resolutions, Derived Functors . . . 309
5.3 Various (Co)homological Functors . . . 327
5.4 Spectral Sequences; First Applications . . . 355
5.5 The Koszul Complex and Applications . . . 378
5.6 Concluding Remarks . . . 397
5.7 Supplementary Readings . . . 397

Index **401**

Preface

A book on "Abstract" or "Modern" Algebra is a commonplace thing in today's mathematical milieu. Even a book for *well-prepared, serious* beginning graduate students who intend to become research mathematicians is not so strange any longer. But, the genesis of this book, which *is* intended for serious, *well-prepared* graduate students, is somewhat strange.

To begin with, it is a reworking of notes for a year long graduate course I gave several years ago–not in itself a strange thing. But, I possess no such notes nor did I ever make any and I never lecture with a written *aide memoir* of any sort. Rather, my method is to work out fully during lecture (at the board) each proof and example. Students will thus see what are the "inner workings" of the subject. Of course, this is pedagogically to their advantage and, furthermore, it slows me down.

Then where did the notes (to be reworked) come from? They were provided by my friend and colleague Jean H. Gallier (of the Computer Science Department at Penn). Determined to augment his mathematical knowledge, he began several years ago to audit some of my graduate courses. "Audit" for him means faithfully attending lectures, doing all the problem assignments, participating in each bi-weekly problem session (where he takes his turn presenting problems), writing excellent notes from my oral presentation *and rendering these notes in LaTeX form*.[1] That this book will appear is, in large measure, his doing. While I have been responsible for its writing, he has on occasion introduced results and/or alternate proofs that have rendered some material more perspicacious from a student's point of view–these have improved the text. He is in every sense a joint author, save that errors are solely my responsibility. There is no way I can thank him adequately here in plain words and I won't try except to say, *Je te remercie vivement, mon ami Jean, pour tout ton travail*.

Others should be thanked as well–in particular the members of the class that attended the course from which the book is formed.[2] By their interest and attention to detail, they kept me on my toes. One particular member of that class deserves special mention: Mathew Cross.[3] Mathew started the index and set the original 115 problems in LaTeX. He lightened our burden by a considerable amount.

The content of the book follows rather closely the oral lectures–with just a few exceptions. These are: In Chapter 3, the section on Integral Dependence is now augmented by proofs of all results, the original lectures had statements only of some of these (due to exigencies of time) and Gallier insisted on a full treatment. In Chapter 4, the sections on Norms and Traces as well as Kummer Theory and Transcendental Extensions are likewise augmented by full proofs. In Chapter 5, there is now more to the section on (co)homological functors and there are full proofs in the last section on the Koszul Complex. Otherwise, the material is just (a smoothed out version of) what was presented. One will have to move fast to present it to students in one year, at least I did.

But the heart of the book is the Problem section. Here, I've attempted to simulate at the beginning graduate level some of the features of real mathematical work. There is a jumbling of the problems *vis a*

[1] One must realize he maintains a full research and teaching schedule, directs Ph.D. students, attends to administrative duties and has a family life in addition to this "auditing"!

[2] The members of the class were: A. Bak, D. Boyarchenko, S. Brooks, M. Campbell, S. Corry, M. Cross, C. Daenzer, C. Devena, J. Gallier, S. Guerra, C. Hoelscher, T. Jaeger, J. Long, S. Mason, T. Zhu.

[3] Mathew spells his name with but one "t"; there is no misprint.

vis subject matter just as in real research one never knows what kind of mathematics will be needed in the solution of a problem. There is no hint of the level of difficulty of a problem (save for the few problems where suggestions are offered), and anyway the notion of difficulty is ill-defined. And, the problems refer to each other, just as in real work one is constantly reminded of past efforts (successful or not). In effect, as suggested in the preface for students, one should begin with the problems and use the text as a means to fill in knowledge as required to do them (as well as to do other problems assigned by an instructor in this course or another course).

This brings me to the text material itself. There is no attempt to be encyclopedic. After all, the material is a faithful copy of what was actually covered in a year and any competent instructor can add material that has been omitted. I regret not covering the Wederburn-Artin Theory of DCC rings, the Brauer Group, and some basic material on group representations. What is covered, however, is to my mind central to the education of any prospective mathematician who aspires to contribute to what is now the mainstream of mathematical endeavor. Also, while there are over 150 problems filling some 55 pages of text (some of the problems are rather long being multi-part), other problems of an instructor's choosing can certainly be assigned. As to the attribution of the origins of these problems, I have assigned names when they are known to me. If no name is assigned, the problem comes from some source in my past (perhaps one of my own teachers or their teachers) and in no way do I claim it as my own. Good problems from all sources are the treasure hoard of practicing mathematicians in their role as passers on of our common heritage.

I refer to the special symbols (DX) and the "curves ahead" road sign (appearing at odd places in the text) in the student preface; no repeat of the explanations I offer there is necessary. If you as instructor are lucky enough to have a class as interested and tough to satisfy as I did, you are lucky indeed and need no further assurance that mathematics will be in good hands in the future. I intend this book to be of service to such individuals as they begin their long climb to mathematical independence and maturity.

Tolda Santa Cotogna
Summer, 2006

For the Student

It may be surprising but the most important part of the book you now hold before you is the very first section–the one labeled "Problems." To learn mathematics one must *do* mathematics. Indeed, the best way to read this book is to turn immediately to the problem section and begin to do the problems. Of course, you will soon reach some unknown terminology or not have enough knowledge to meet the technical demands of a problem and this is where you turn to the text to fill in gaps, see ideas explained and techniques demonstrated. Then you plunge once more back into the problems and repeat the whole process.

The book is designed for serious, well-prepared students who plan on becoming research mathematicians. It presumes you have had previous acquaintance with algebra; in particular you have met the concepts of group, ring, field, vector space, homomorphism, isomorphism, and the elementary theorems about these things. No book on mathematics can be simply read, rather you must recreate the text yourself line by line checking at each stage all details including those omitted. This is slow work and, as you know, mathematics has very high density on the page.

In the text, you will find two special symbols: (DX) and a sign such as one sees on the road warning of dangerous curves ahead. The symbol (DX) stands for "diagnostic exercise", it means some elementary details have been omitted and that supplying them should be easy. However, if supplying them is not easy, then you should go back a page or two as something fundamental has skipped you by. In this way, the sign (DX) is like a medical test: failing it is sure to tell you if something is wrong (no false positives), however, if you pass it (supply the details), something still might be wrong. Just read on and anything wrong will surface later. As for the dangerous curves sign, it precedes counter-examples to naively made conjectures, it warns when things could go wrong if hypotheses are omitted, and generally forces you to slow down in the reading and recreating.

If you use this book in a course or even for self study, I recommend that you tackle the problems in a small group (two to four persons, total). This is because no person has a monopoly on ideas, a good idea or half-idea can germ in any head, and the working out of a problem by a committed group is akin to the actual way much research mathematics is accomplished. In your group, you want constant give and take, and there must be time to think alone so that a real contribution to the group's effort can be made.

The problems are all jumbled up by area and there is no signal given as to a problem's difficulty (exceptions are the few cases where hints or suggestions are given). In real mathematical life, no signs are given that a question being attacked involves a certain small area of mathematical knowledge or is hard or easy; any such sign is gleaned by virtue of experience and that is what you are obtaining by *doing* mathematics in these problems. Moreover, hard and easy are in the eyes of the beholder; they are not universal characteristics of a problem. About all one can say is that if a large number of people find a problem difficult, we may classify it so. However, we shouldn't be surprised when an individual solves it and claims that, "it was not that hard". In any case, guard against confusing mathematical talent either with overall intelligence or with mathematical speed. Some quick people are in fact talented, many are just quick. Don't be discouraged if you find yourself slower than another, the things that really count in doing mathematics (assuming talent) are persistence and courage.

I can think of no better lines to close with than these which come from B. Pasternak's poem entitled "*Night*"[4]

"And maybe in an attic
And under ancient slates
A man sits wakeful working
He thinks and broods and waits."

"He looks upon the planet,
As if the heavenly spheres
Were part of his entrusted
Nocturnal private cares."

"Fight off your sleep: be wakeful,
Work on, keep up your pace,
Keep vigil like the pilot,
Like all the stars in space."

"Work on, work on, creator–
To sleep would be a crime–
Eternity's own hostage,
And prisoner of Time."

Tolda Santa Cotogna
Summer, 2006

[4]From the collection entitled "*When It Clears Up*", 1956. Translated by Lydia Pasternak Slater (the poet's sister).

Problems

"... den Samen in den Wind streuend; fasse, wer es fassen kann".
—**Hermann Weyl**

Problem 1

1. Suppose G is a finite group and that $\mathrm{Aut}_{\mathrm{Gr}}(G) = \{1\}$. (Here, $\mathrm{Aut}_{\mathrm{Gr}}(G)$ is the group of all bijections, $G \to G$, which are also group homomorphisms.) Find *all* such groups G.

2. Write $\mathbb{Z}/2\mathbb{Z}$ for the cyclic group of order 2. If $G = \mathbb{Z}/2\mathbb{Z} \prod \cdots \prod \mathbb{Z}/2\mathbb{Z}$, t-times, compute $\#\big(\mathrm{Aut}_{\mathrm{Gr}}(G)\big)$. When $t = 2$, determine the group $\mathrm{Aut}_{\mathrm{Gr}}(G)$. When $t = 3$, determine the structure of the odd prime Sylows. Can you decide whether $\mathrm{Aut}_{\mathrm{Gr}}(G)$ has any normal subgroups in the case $t = 3$?

Problem 2

1. (Poincaré). In an infinite group, prove that the intersection of two subgroups of finite index has finite index itself.

2. Show that if a group, G, has a subgroup of finite index, then it possesses a normal subgroup of finite index. Hence, an infinite simple group has no subgroups of finite index.

3. Sharpen (2) by proving: if $(G : H) = r$, then G possesses a normal subgroup, N, with $(G : N) \leq r!$. Conclude immediately that a group of order 36 cannot be simple.

Problem 3 Let $G = \mathrm{GL}(n, \mathbb{C})$ and Δ_n be the subgroup of matrices with entries only along the diagonal. Describe precisely $N_G(\Delta_n)$ in terms of what the matrices look like.

Problem 4 Say G is a group and $\#(G) = p^r g_0$, where p is a prime and $(p, g_0) = 1$. Assume

$$r > \sum_{j=1}^{g_0 - 1} \sum_{k>0} [j/p^k]$$

$\big([x] = \text{largest integer} \leq x\big)$. Prove that G is not simple. Show that this governs all groups of order < 60, except for $\#(G) = 30, 40, 56$. We know that $\#(G) = 30 \implies G$ not simple. Show by explicit argument that groups of orders $40, 56$ are not simple. (Here, of course, by simple we mean non-abelian and simple.)

Problem 5 In a p-group, G, we cannot have

$$(G\colon Z(G)) = p.$$

Show that for non-abelian groups of order p^3, $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ and $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \prod \mathbb{Z}/p\mathbb{Z}$.

Problem 6 Let G be the group of automorphisms of a regular polyhedron with v vertices, e edges, and f faces. Show that G has order $g = fs = vr = 2e$, where s is the number of sides to a face and r is the number of edges emanating from a vertex. From topology, one knows Euler's formula

$$v - e + f = 2.$$

Find the only possible values for v, e, f, r, s, g. Make a table.

Problem 7 Let p be a prime number. Find all non-abelian groups of order p^3. Get started with the Burnside basis theorem, but be careful to check that the groups on your list are non-isomorphic. Also make sure your list is exhaustive. Your list should be a description of the generators of your groups and the relations they satisfy.

Problem 8 Let G be a finite group and write $c(G)$ for the number of distinct conjugacy classes in G. This number will increase (in general) as $\#(G) \to \infty$; so, look at

$$\overline{c}(G) = \frac{c(G)}{\#(G)}.$$

The number $\overline{c}(G)$ measures the "average number of conjugacy classes per element of G" and is 1 if G is abelian. Assume G is *non-abelian* from now on. Then $0 < \overline{c}(G) < 1$.

1. Prove that for all such G, we have $\overline{c}(G) \leq 5/8$.
2. Suppose p is the smallest prime with $p \,|\#(G)$. Prove that

$$\overline{c}(G) \leq \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3}.$$

Is the bound of (1) sharp; that is, does there exist a G with $\overline{c}(G) = 5/8$? How about the bound of (2)?

Problem 9 If G is a finite group and H a normal subgroup of G, write P for a p-Sylow subgroup *of* H.

1. Show that the natural injection
$$N_G(P)/N_H(P) \to G/H$$
(why does it exist, why injective?) is actually an isomorphism.
2. Prove that the Frattini subgroup, $\Phi(G)$, of ANY finite group, G, has property N (cf. Section 1.3, Chapter 1).

Problem 10 We've remarked that $\Phi(G)$ is a kind of "radical" in the group-theoretic setting. In this problem we study various types of radicals.
A *normal* subgroup, H, of G is called *small* iff for every $X \lhd G$, the equality $H \cdot X = G$ implies that $X = G$. (Note: $\{1\}$ is small, $\Phi(G)$ is small; so they exist.) Check that if H and L are small, so is HL, and if H is small and $K \lhd G$, then $K \subseteq H \implies K$ is small.

1. The *small radical* of G, denoted $\mathcal{J}^{**}(G)$, is
$$\mathcal{J}^{**}(G) = \big\{x \in G \,\big|\, \mathrm{Gp}\{\mathrm{Cl}(x)\} \text{ is small}\big\}.$$
(Here, $\mathrm{Cl}(x)$ is the conjugacy class of x in G, and $\mathrm{Gp}\{S\}$ is the group generated by S.) Prove that $\mathcal{J}^{**}(G)$ is a subgroup of G.
2. The *Jacobson radical* of G, denoted $\mathcal{J}^{*}(G)$, is the intersection of all maximal, normal subgroups of G; while the *Baer radical* of G, denoted $\mathcal{J}(G)$, is the product (inside G) of *all* the small subgroups of G. Prove
$$\mathcal{J}^{**}(G) \subseteq \mathcal{J}(G) \subseteq \mathcal{J}^{*}(G).$$

3. Prove *Baer's Theorem*: $\mathcal{J}^{**}(G) = \mathcal{J}(G) = \mathcal{J}^{*}(G)$. (Suggestion: if $x \notin \mathcal{J}^{**}(G)$, find $N \lhd G$ $(\neq G)$ so that $\mathrm{Gp}\{\mathrm{Cl}(x)\}N = G$. Now construct an appropriate maximal normal subgroup not containing x.)

Problem 11 Recall that a *characteristic* subgroup is one taken into itself by *all* automorphisms of the group.

1. Prove that a group possessing no proper characteristic subgroups is isomorphic to a product of isomorphic simple groups. (Hints: Choose $\widetilde{G}$ of smallest possible order (> 1) normal in G. Consider all subgroups, H, for which $H \cong G_1 \prod \cdots \prod G_t$, where each $G_j \lhd G$ and each $G_j \cong \widetilde{G}$. Pick t so that $\#(H)$ is maximal. Prove that H is characteristic. Show $K \lhd G_1$ (say) $\implies K \lhd G$.)

2. Prove: In every finite group, G, a minimal normal subgroup, H, is either an elementary abelian p-group or is isomorphic to a product of mutually isomorphic, non-abelian, simple groups.

3. Show that in a solvable group, G, only the first case in (2) occurs.

Problem 12 Let G be a finite p-group and suppose $\varphi \in \mathrm{Aut}(G)$ has order n (i.e., $\varphi\big(\varphi(\cdots(\varphi(x))\cdots)\big) = \mathrm{Id}$, all $x \in G$: we do φ n-times in succession and n is minimal). Suppose $(n, p) = 1$. Now φ induces an automorphism of $G/\Phi(G)$, call it $\overline{\varphi}$, as $\Phi(G)$ is characteristic. Remember that $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$; so, $\overline{\varphi} \in \mathrm{GL}\big(G/\Phi(G)\big)$.

1. Prove $\overline{\varphi} = \text{identity} \iff \varphi = \text{identity}$.

2. Show that if d is the Burnside dimension of G, then

$$\#\big(\mathrm{GL}(G/\Phi(G))\big) = p^{\frac{d(d-1)}{2}} \prod_{k=1}^{d} (p^k - 1),$$

   and that if P is a p-Sylow subgroup of $\mathrm{GL}\big(G/\Phi(G)\big)$, then $P \subseteq \mathrm{SL}\big(G/\Phi(G)\big)$; i.e., $\sigma \in P \implies \det(\sigma) = 1$.

3. Let $\mathcal{P} = \{\varphi \in \mathrm{Aut}(G) \mid \overline{\varphi} \in P, \text{ no restriction on the order of } \varphi\}$. Show that $\mathcal{P}$ is a p-subgroup of $\mathrm{Aut}(G)$.

4. Call an element $\sigma \in \mathrm{GL}\big(G/\Phi(G)\big)$ *liftable* iff it is $\overline{\varphi}$ for some $\varphi \in \mathrm{Aut}(G)$. Examine all G of order p, p^2, p^3 to help answer the following: Is every σ liftable? If not, how can you tell (given σ) if σ is liftable?

Problem 13 Let p be a prime number and consider a set, S, of p objects: $S = \{\alpha_1, \ldots, \alpha_p\}$. Assume G is a *transitive* group of permutations of S (i.e., the elements of S form an orbit under G); further assume $(\alpha_1\alpha_2) \in G$ (here $(\alpha_1\alpha_2)$ is the transposition). Prove: $G = \mathfrak{S}_p$. (Suggestion: let $M = \{\alpha_j | (\alpha_1\alpha_j) \in G\}$, show if $\sigma \in \mathfrak{S}_p$ and $\sigma = 1$ outside M then $\sigma \in G$. Now prove $\#(M) | p$.)

Problem 14 A *Fermat prime*, p, is a prime number of the form $2^\alpha + 1$. E.g., $2, 3, 5, 17, 257, \ldots$.

1. Show if $2^\alpha + 1$ is prime then $\alpha = 2^\beta$.

2. Say p is a Fermat prime (they are quite big) and g_0 is an *odd* number with $g_0 < p$. Prove that any group of order $g_0 p$ is isomorphic to a product $G_0 \prod(\mathbb{Z}/p\mathbb{Z})$, where $\#(G_0) = g_0$. Hence, for example, the groups of orders $51 (= 3 \cdot 17)$, $85 (= 5 \cdot 17)$, $119 (= 7 \cdot 17)$, $153 (= 9 \cdot 17)$, $187 (= 11 \cdot 17)$, $221 (= 13 \cdot 17)$, $255 (= 3 \cdot 5 \cdot 17)$ are all abelian. Most we knew already, but $153 = 3^2 \cdot 17$ and $255 = 3 \cdot 5 \cdot 17$ are new.

3. Generalize to any prime, p, and $g_0 < p$, with $p \not\equiv 1 \bmod g_0$. For example, find all groups of order 130.

Problem 15 Recall that a group, G, is *finitely generated* (f.g.) iff $(\exists\, \sigma_1, \ldots, \sigma_n \in G)(G = \mathrm{Gp}\{\sigma_1, \ldots, \sigma_n\})$.

1. If G is an *abelian* f.g. group, prove each of its subgroups is f.g.

2. In an arbitrary group, G, an element $\sigma \in G$ is called *n-torsion* ($n \in \mathbb{N}$) $\iff$ $\sigma^n = 1$; σ is torsion iff it is n-torsion for some $n \in \mathbb{N}$. The element $\sigma \in G$ is *torsion free* $\iff$ it is not torsion. Show that in an abelian group, the set
$$t(G) = \{\sigma \in G \mid \sigma \text{ is torsion}\}$$
is a subgroup and that $G/t(G)$ is torsion free (i.e., all its non-identity elements are torsion free).

3. In the solvable group $0 \to \mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 0$ (split extension, non-trivial action) find two elements x, y satisfying: $x^2 = y^2 = 1$ and xy is torsion free. Can you construct a group, $\widetilde{G}$, possessing elements x, y of order 2, so that xy has order n, where n is predetermined in $\mathbb{N}$? Can you construct $\widetilde{G}$ solvable with these properties?

4. Back to the abelian case. If G is abelian and finitely generated show that $t(G)$ is a finite group.

5. Say G is abelian, f.g., and torsion-free. Write d for the minimal number of generators of G. Prove that G is isomorphic to a product of d copies of $\mathbb{Z}$.

6. If G is abelian and f.g., prove that
$$G \cong t(G) \prod \big(G/t(G)\big).$$

Problem 16 Let (P) be a property of groups. We say a group, G, is *locally (P)* $\iff$ each f.g. subgroup of G has (P). Usually, one says a locally cyclic group is a *rank one group*.

1. Prove that a rank one group is abelian.

2. Show that the additive group of rational numbers, $\mathbb{Q}^+$, is a rank one group.

3. Show that every torsion-free, rank one group is isomorphic to a subgroup of $\mathbb{Q}^+$.

Problem 17 Fix a group, G, and consider the set, $\mathcal{M}_n(G)$, of $n \times n$ matrices with entries from G or so that $\alpha_{ij} = 0$ (i.e., entries are 0 or from G). Assume for each row and each column there is one and only one non-zero entry. These matrices form a group under ordinary "matrix multiplication" if we define $0 \cdot \text{group element} = \text{group element} \cdot 0 = 0$. Establish an isomorphism of this group with the wreath product $G^n \wr \mathfrak{S}_n$. As an application, for the subgroup of $\mathrm{GL}(n, \mathbb{C})$ consisting of diagonal matrices, call it Δ_n, show that
$$N_G(\Delta_n) \cong \mathbb{C}^n \wr \mathfrak{S}_n, \quad \text{here } G = \mathrm{GL}(n, \mathbb{C}).$$

Problem 18

1. Say G is a simple group of order n and say p is a prime number dividing n. If $\sigma_1, \ldots, \sigma_t$ is a listing of the elements of G of exact order p, prove that $G = \mathrm{Gp}\{\sigma_1, \ldots, \sigma_t\}$.

2. Suppose G is any finite group of order n and that d is a positive integer relatively prime to n. Show that every element of G is a dth power.

Problem 19 We know that when G is a (finite) cyclic group, and A is any G-module, we have an isomorphism
$$A^G/\mathcal{N}(A) \xrightarrow{\sim} H^2(G, A).$$
This problem is designed to lead to a proof. There are other proofs which you might dig out of books (after some effort), but do *this* proof.

1. Suppose G is any group and A, B, C are G-modules. Suppose further, we are given a *G-pairing of* $A \prod B \to C$ i.e., a map
$$\theta : A \prod B \to C$$
which is bi-additive and "G-linear":
$$\sigma\theta(a,b) = \theta(\sigma a, \sigma b).$$
If f, g are r-, s-cochains of G with values in A, B (respectively), we can define an $(r+s)$-cochain of G with values in C *via* the formula:
$$(f \smile_\theta g)(\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}) = \theta\big(f(\sigma_1, \ldots, \sigma_r), \sigma_1 \ldots \sigma_r g(\sigma_{r+1}, \ldots, \sigma_{r+s})\big).$$
Prove that $\delta(f \smile_\theta g) = \delta f \smile_\theta g + (-1)^r f \smile_\theta \delta g$. Show how you conclude from this that we have a pairing of abelian groups
$$\smile_\theta : H^r(G, A) \prod H^s(G, B) \to H^{r+s}(G, C).$$
(Notation and nomenclature: $\alpha \smile_\theta \beta$, *cup-product*.)

2. Again G is any group, this time finite. Let $\mathbb{Z}$ and $\mathbb{Q}/\mathbb{Z}$ be G-modules with trivial action. Consider the abelian group $\mathrm{Hom}_{\mathrm{gr}}(G, \mathbb{Q}/\mathbb{Z}) = \widetilde{G}$, where addition in $\widetilde{G}$ is by pointwise operation on functions. If $\chi \in \widetilde{G}$, then $\chi(\sigma) \in \mathbb{Q}/\mathbb{Z}$, all $\sigma \in G$. Show that the function
$$f_\chi(\sigma, \tau) = \delta\chi(\sigma, \tau) = \sigma\chi(\tau) - \chi(\sigma\tau) + \chi(\sigma)$$
has values in $\mathbb{Z}$ and actually is a 2-cocycle with values in $\mathbb{Z}$. (This is an example of the principle: If it looks like a coboundary, it is certainly a cocycle.) The map
$$\chi \in \widetilde{G} \mapsto \text{cohomology class of } f_\chi(\sigma, \tau) \qquad (\dagger)$$
gives a homomorphism $\widetilde{G} \to H^2(G, \mathbb{Z})$.
Now *any* 2-cocycle $g(\sigma, \tau)$ with values in $\mathbb{Z}$ can be regarded as a 2-cocycle with values in $\mathbb{Q}$ (corresponding to the injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$). Show that *as a 2-cocycle in* $\mathbb{Q}$ it is a coboundary (of some $h(\sigma)$, *values in* $\mathbb{Q}$). So, $g(\sigma, \tau) = \delta h(\sigma, \tau)$, some h. Use this construction to prove:

For any finite group, G, the map $(\dagger)$ above gives an *isomorphism* of $\widetilde{G}$ with $H^2(G, \mathbb{Z})$.

3. Now let G be finite, A be any G-module, and $\mathbb{Z}$ have the trivial G-action. We have an obvious G-pairing $\mathbb{Z} \prod A \to A$, namely $(n, a) \mapsto na$, hence by (1) and (2) we obtain a pairing
$$\widetilde{G}(= H^2(G, \mathbb{Z})) \prod A^G \to H^2(G, A).$$
Show that if $\xi = \mathcal{N}\alpha$, for $\alpha \in A$, then (χ, ξ) goes to 0 in $H^2(G, A)$; hence, we obtain a pairing:
$$\widetilde{G} \prod (A^G/\mathcal{N}A) \to H^2(G, A).$$
(Hint: If $f(\sigma, \tau)$ is a 2-cocycle of G in A, consider the 1-cochain $u_f(\tau) = \sum_{\sigma \in G} f(\sigma, \tau)$. Using the cocycle condition and suitable choices of the variables, show the values of u_f are in A^G and that u_f is related to $\mathcal{N}f$, i.e., $\mathcal{N}f(\tau, \rho) = \sum_\sigma \sigma f(\tau, \rho)$ can be expressed by u_f.)

4. Finally, when G is cyclic, we pick a generator σ_0. There exists a distinguished element, χ_0, of $\widetilde{G}$ corresponding to σ_0, namely χ_0 is that homomorphism $G \to \mathbb{Q}/\mathbb{Z}$ whose value at σ_0 is $\frac{1}{n} \bmod \mathbb{Z}$, where $n = \#(G)$. Show that the map
$$A^G/\mathcal{N}A \to H^2(G, A)$$
via
$$\alpha \mapsto (\chi_0, \alpha) \mapsto \delta\chi_0 \smile \alpha \in H^2(G, A)$$
is the required isomorphism. For surjectivity, I suggest you consider the construction of u_f in part (3) above.

Problem 20 Let $G = \mathrm{SL}(2,\mathbb{Z})$ be the group of all 2×2 integral matrices of determinant 1; pick a prime, p, and write U for the set of 2×2 integral matrices having determinant p. G acts on U *via* $u(\in U)\mapsto \sigma u$, where $\sigma \in G$.

1. Show that the orbit space has $p+1$ elements: $0,1,\ldots,p-1,\infty$, where j corresponds to the matrix
$$w_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$$
and ∞ corresponds to the matrix $w_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

2. If $\tau \in G$ and $r \in S = \{0,1,\ldots,p-1,\infty\} = G\backslash U$, show there exists a unique $r' \in S$ with $w_r\tau^{-1}$ in the orbit of $w_{r'}$. Write $\tau\cdot r = r'$ and prove this gives an action of G on S. Hence, we have a group homomorphism $P : G \to \mathrm{Aut}(S) = \mathfrak{S}_{p+1}$.

3. If $N = \ker P$, prove that G/N is isomorphic to the group $\mathrm{PSL}(2,\mathbb{F}_p)$ consisting of all "fractional linear transformations"
$$x \mapsto x' = \frac{ax+b}{cx+d}, \quad a,b,c,d \in \mathbb{F}_p,\ ad-bc=1.$$
Show further that

   i. $\#\big(\mathrm{PSL}(2,\mathbb{F}_p)\big) = \begin{cases} \dfrac{p(p+1)(p-1)}{2} & \text{if } p\neq 2 \\ 6 & \text{if } p = 2 \end{cases}$

   and

   ii. $\mathrm{PSL}(2,\mathbb{F}_p)$ acts transitively on S under the action of (2).

4. Now prove: $\mathrm{PSL}(2,\mathbb{F}_p)$ is simple if $p \geq 5$. (Note: $\mathrm{PSL}(2,\mathbb{F}_3)$ is A_4, $\mathrm{PSL}(2,\mathbb{F}_5)$ is A_5, but $\mathrm{PSL}(2,\mathbb{F}_p)$ is not A_n if $p \geq 7$. So, you now have a second infinite collection of simple finite groups—these are finite group analogs of the Lie groups $\mathrm{PSL}(2,\mathbb{C})$).

Problem 21 We write $\mathrm{PSL}(2,\mathbb{Z})$ for the group $\mathrm{SL}(2,\mathbb{Z})/(\pm I)$.

(1) Let ξ be a chosen generator for $\mathbb{Z}/3\mathbb{Z}$ and η the generator of $\mathbb{Z}/2\mathbb{Z}$. Map $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ to $\mathrm{PSL}(2,\mathbb{Z})$ *via*
$$\varphi(\xi) = x = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} (\mathrm{mod}\ \pm I)$$
and
$$\psi(\eta) = y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (\mathrm{mod}\ \pm I)$$
Then we obtain a map
$$\varphi \amalg \psi \colon \mathbb{Z}/3\mathbb{Z} \amalg \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{PSL}(2,\mathbb{Z})$$
(here, the coproduct is in the category Grp). What is the image of $\varphi \amalg \psi$? What is the kernel?

(2) If
$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \text{in } \mathrm{PSL}(2,\mathbb{Z})$$
express x and y above (in $\mathrm{SL}(2,\mathbb{Z})$) in terms of a and b and show that $\mathrm{SL}(2,\mathbb{Z}) = \mathrm{Grp}\{a,b\}$. Can you express a and b in terms of x and y?

(3) For any odd prime number, p, the element

$$\sigma(p) = \begin{pmatrix} 1 & \frac{p-1}{2} \\ 0 & 1 \end{pmatrix}$$

is equal to $a^{(p-1)/2}$. For any $\sigma \in \mathrm{SL}(2,\mathbb{Z})$, we define the *weight of* σ *with respect to* a *and* b by

$$\mathrm{wt}(\sigma) = \inf(\text{length of all words in } a, b, a^{-1}, b^{-1}, \text{ which words equal } \sigma)$$

By deep theorems of Selberg, Margulis and others (in geometry and analysis) one knows that

$$\mathrm{wt}(\sigma(p)) = O(\log p) \qquad \text{as } p \to \infty.$$

(Our expression for $\sigma(p)$ as a power of a shows that we have a word of size $O(p)$ for $\sigma(p)$, yet no explicit word of size $O(\log p)$ is known as of now (Fall, 2005) and the role of b in this is very mysterious.) Now the *Cayley graph* of a group, G, generated by the elements $g_1, \ldots, g_t$ is that graph whose vertices are the elements of G and whose edges emanating from a vertex $\tau \in G$ are the ones connecting τ and $\tau g_1, \ldots, \tau g_t$. Show that the diameter of the Cayley graph of the group $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ with respect to the generators $\overline{a}$ and $\overline{b}$ is $O(\log p)$.

Problem 22 Let G be a finite group in this problem.

1. Classify all group extensions
$$0 \to \mathbb{Q} \to \mathcal{G} \to G \to 0. \tag{E}$$
Your answer should be in terms of the collection of all subgroups of G, say H, with $(G : H) \leq 2$, plus, perhaps, other data.

2. Same question as (1) for group extensions
$$0 \to \mathbb{Z} \to \mathcal{G} \to G \to 0, \tag{E}$$
same kind of answer.

3. Write V for the "four-group" $\mathbb{Z}/2\mathbb{Z} \prod \mathbb{Z}/2\mathbb{Z}$. There are two actions of $\mathbb{Z}/2\mathbb{Z}$ on V: Flip the factors, take each element to its inverse. Are these the only actions? Find all group extensions
$$0 \to V \to \mathcal{G} \to \mathbb{Z}/p\mathbb{Z} \to 0. \tag{E}$$
The group $\mathcal{G}$ is a group of order 8; compare your results with what you know from Problems 1–6.

4. Say H is any other group, G need no longer be finite and A, B are abelian groups. Suppose $\varphi : H \to G$ is a homomorphism and we are given a group extension
$$0 \to A \to \mathcal{G} \to G \to 0. \tag{E}$$
Show that, in a canonical way, we can make a group extension
$$0 \to A \to \widetilde{\mathcal{G}} \to H \to 0. \tag{$\varphi^* E$}$$
(Note: your answer has to be in terms of G, H, $\mathcal{G}$ and any homomorphisms between them as these are the only "variables" present. You'll get the idea if you view an extension as a fibre space.)

   Now say $\psi : A \to B$ is a group homomorphism and we are given an extension
$$0 \to A \to \mathcal{G} \to G \to 0. \tag{E}$$
Construct, in a canonical way, an extension
$$0 \to B \to \widetilde{\mathcal{G}} \to G \to 0. \tag{$\psi_* E$}$$

5. Explain, carefully, the relevance of these two constructions to parts (1) and (2) of this problem.

Problem 23 Say A is any abelian group, and write G for the *wreath product* $A^n \wr \mathfrak{S}_n$. Show:

1. $[G, G] \neq G$
2. $\big(G : [G, G]\big) = \infty \iff A$ is infinite
3. If $n \geq 2$, then $[G, G] \neq \{1\}$.
4. Give a restriction on n which prevents G from being solvable.

Problem 24 If $\{G_\alpha\}_{\alpha \in \Lambda}$ is a family of *abelian* groups, write $\coprod_\alpha G_\alpha$ for

$$\coprod_\alpha G_\alpha = \left\{ (\xi_\alpha) \in \prod_\alpha G_\alpha \mid \text{ for all but finitely many } \alpha, \text{ we have } \xi_\alpha = 0 \right\}.$$

Then $\coprod_\alpha G_\alpha$ is the *coproduct* of the G_α in $\mathcal{A}\mathrm{b}$. Write as well

$$(\mathbb{Q}/\mathbb{Z})_p = \{\xi \in \mathbb{Q}/\mathbb{Z} \mid p^r \xi = 0, \text{ some } r > 0\};$$

here, p is a prime. Further, call an *abelian* group, A, *divisible* iff

$$(\forall\, n)(A \xrightarrow{n} A \to 0 \text{ is exact}).$$

Prove: Theorem Every divisible (abelian) group is a coproduct of copies of $\mathbb{Q}$ and $(\mathbb{Q}/\mathbb{Z})_p$ for various primes p. The group is torsion iff no copies of $\mathbb{Q}$ appear, it is torsion-free iff no copies of $(\mathbb{Q}/\mathbb{Z})_p$ appear (any p). Every torsion-free, divisible, abelian group is naturally a vector space over $\mathbb{Q}$.

Problem 25

1. If G is a group of order n, show that $G \wr \mathrm{Aut}(G)$ is isomorphic to a subgroup of $\mathfrak{S}_n$.
2. Consider the cycle $(1, 2, \ldots, n) \in \mathfrak{S}_n$; let H be the subgroup (of $\mathfrak{S}_n$) generated by the cycle. Prove that
$$\mathcal{N}_{\mathfrak{S}_n}(H) \cong (\mathbb{Z}/n\mathbb{Z}) \wr \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}).$$

Problem 26 Let TOP denote the category of topological spaces.

1. Show that TOP possesses finite fibred products and finite fibred coproducts.
2. Is (1) true without the word "finite"?
3. Write T2TOP for the full subcategory of TOP consisting of Hausdorff topological spaces. Are (1) and (2) true in T2TOP? If you decide the answer is "no", give reasonable conditions under which a positive result holds. What relation is there between the product (coproduct) you constructed in (1) (or (2)) and the corresponding objects in this part of the problem?

Problem 27 Let R be a ring (not necessarily commutative) and write $\mathcal{M}\mathrm{od}(R)$ for the category of (left) R-modules; i.e., the action of R on a module, M, is on the left. We know $\mathcal{M}\mathrm{od}(R)$ has finite products and finite fibred products.

1. What is the situation for infinite products and infinite fibred products?
2. What is the situation for coproducts (finite or infinite) and for fibred coproducts (both finite and infinite)?

Problem 28 As usual, write $\mathcal{G}\mathrm{r}$ for the category of groups. Say G and G' are groups and $\varphi : G \to G'$ is a homomorphism. Then $(G, \varphi) \in \mathcal{G}\mathrm{r}_{G'}$, the comma category of "groups over G'". The group $\{1\}$ possess a canonical morphism to G', namely the inclusion, i. Thus, $\big(\{1\}, i\big) \in \mathcal{G}\mathrm{r}_{G'}$, as well. We form their product in $\mathcal{G}\mathrm{r}_{G'}$, i.e., we form the fibred product $G \prod\limits_{G'} \{1\}$. Prove that there exists a canonical *monomorphism*

$$G \prod_{G'} \{1\} \to G.$$

Identify its image in G.
Now consider the "dual" situation: G' maps to G, so $G \in \mathcal{G}\mathrm{r}^{G'}$ (*via* φ) the "groups co-over G'". We also have the canonical map $G' \to \{1\}$, killing all the elements of G'; so, as above, we can form the fibred coproduct of G and $\{1\}$: $G \overset{G'}{\amalg} \{1\}$. Prove that there exists a canonical epimorphism

$$G \to G \overset{G'}{\amalg} \{1\},$$

identify its kernel in G.

Problem 29 Write CR for the category of commutative rings with unity and RNG for the category of rings with unity.

1. Consider the following two functors from CR to $\mathcal{S}$ets:

   (a) $|\mathcal{M}_{pq}| : A \rightsquigarrow$ underlying set of $p \times q$ matrices with entries from A

   (b) $|\mathrm{GL}_n| : A \rightsquigarrow$ underlying set of all invertible $n \times n$ matrices with entries from A.

   Prove the these two functors are representable.

2. A slight modification of (b) above yields a functor from CR to $\mathcal{G}\mathrm{r}$: namely,

   $$\mathrm{GL}_n : A \rightsquigarrow \textit{group} \text{ of all invertible } n \times n \text{ matrices with entries from } A.$$

   When $n = 1$, we can extend this to a functor from RNG to $\mathcal{G}\mathrm{r}$. That is we get the functor

   $$\mathbb{G}_m : A \rightsquigarrow \text{group of all invertible elements of } A.$$

   Prove that the functor $\mathbb{G}_m$ has a left adjoint, let's temporarily call it (†); that is: There is a functor (†) from $\mathcal{G}\mathrm{r}$ to RNG, so that

   $$(\forall\, G \in \mathcal{G}\mathrm{r})(\forall\, R \in \mathrm{RNG})(\mathrm{Hom}_{\mathrm{RNG}}((\dagger)(G), R) \cong \mathrm{Hom}_{\mathcal{G}\mathrm{r}}(G, \mathbb{G}_m(R))),$$

   via a functorial isomorphism.

3. Show that without knowing what ring (†)(G) is, namely that it exists and that (†) is left adjoint to $\mathbb{G}_m$, we can prove: the category of (†)(G)-modules, $\mathcal{M}\mathrm{od}\big((\dagger)(G)\big)$, is equivalent—in fact isomorphic—to the category of G-modules.

4. There is a functor from $\mathcal{G}\mathrm{r}$ to Ab, namely send G to $G^{\mathrm{ab}} = G/[G, G]$. Show this functor has a right adjoint, call it I. Namely, there exists a functor $I : \mathrm{Ab} \to \mathcal{G}\mathrm{r}$, so that

   $$(\forall\, G \in \mathcal{G}\mathrm{r})(\forall\, H \in \mathrm{Ab})(\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(G, I(H)) \cong \mathrm{Hom}_{\mathrm{Ab}}(G^{\mathrm{ab}}, H)).$$

   Does $G \rightsquigarrow G^{\mathrm{ab}}$ have a left adjoint?

Problem 30 (Kaplansky) If A and B are 2×2-matrices with entries in $\mathbb{Z}$, we embed A and B into the 4×4 matrices as follows:

$$\begin{aligned} A^{\text{aug}} &= \begin{pmatrix} 0 & I \\ A & 0 \end{pmatrix} \\ B^{\text{aug}} &= \begin{pmatrix} 0 & I \\ B & 0 \end{pmatrix}. \end{aligned}$$

Is it true that if A^{aug} and B^{aug} are similar over $\mathbb{Z}$, then A and B are similar over $\mathbb{Z}$? Proof or counter-example. What about the case where the entries lie in $\mathbb{Q}$?

Problem 31 We fix a commutative ring with unity, A, and write $\mathcal{M}$ for $\mathcal{M}_{pq}(A)$, the $p\times q$ matrices with entries in A. Choose a $q\times p$ matrix, Γ, and make $\mathcal{M}$ a ring *via*:

Addition: as usual among $p\times q$ matrices
Multiplication: if $R,S\in\mathcal{M}$, set $R*S=R\Gamma S$, where $R\Gamma S$ is the ordinary product of matrices.

Write $\mathcal{M}(\Gamma)$ for $\mathcal{M}$ with these operations, then $\mathcal{M}(\Gamma)$ is an A-algebra (a ring which is an A-module).

1. Suppose that A is a field. Prove that the isomorphism classes of $\mathcal{M}(\Gamma)$'s are finite in number (here p and q are fixed while Γ varies); in fact, are in natural one-to-one correspondence with the integers $0,1,2,\dots,B$ where B is to be determined by you.

2. Given two $q\times p$ matrices Γ and $\widetilde{\Gamma}$ we call them equivalent iff $\widetilde{\Gamma}=W\Gamma Z$, where $W\in \mathrm{GL}(q,A)$ and $Z\in\mathrm{GL}(p,A)$. Prove: each Γ is equivalent to a matrix

$$\begin{pmatrix} I_r & 0 \\ 0 & H \end{pmatrix}$$

where $I_r=r\times r$ identity matrix and the entries of H are non-units of A. Is r uniquely determined by Γ? How about the matrix H?

3. Call the commutative ring, A, a *local ring* provided it possesses exactly one maximal ideal, $\mathfrak{m}_A$. For example, any field is a local ring; the ring $\mathbb{Z}/p^n\mathbb{Z}$ is local if p is a prime; other examples of this large, important class of rings will appear below. We have the descending chain of ideals

$$A\supseteq \mathfrak{m}_A\supseteq \mathfrak{m}_A^2\supseteq\cdots.$$

For some local rings one knows that $\bigcap_{t\geq 0}\mathfrak{m}_A^t=(0)$; let's call such local rings "good local rings" for temporary nomenclature. If A is a good local ring, we can define a function on A to $\mathbb{Z}\cup\{\infty\}$, call it ord, as follows:

$\mathrm{ord}(\xi)=0$ if $\xi\notin\mathfrak{m}_A$
$\mathrm{ord}(\xi)=n$ if $\xi\in\mathfrak{m}_A^n$ but $\xi\notin\mathfrak{m}_A^{n+1}$
$\mathrm{ord}(0)=\infty$.

The following properties are simple to prove:

$\mathrm{ord}(\xi\pm\eta)\geq\min\{\mathrm{ord}(\xi),\mathrm{ord}(\eta)\}$
$\mathrm{ord}(\xi\eta)\geq\mathrm{ord}(\xi)+\mathrm{ord}(\eta)$.

Consider the $q\times p$ matrices under equivalence and look at the following three conditions:

(i) Γ is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & H \end{pmatrix}$, with $H=(0)$

(ii) Γ is equivalent to $\begin{pmatrix} I_r & 0 \\ 0 & H \end{pmatrix}$ with H having non-unit entries and $r \geq 1$

(iii) $(\exists\, Q \in \mathcal{M})(\Gamma Q \Gamma = \Gamma)$.

Of course, i. $\Longrightarrow$ ii. if $\Gamma \neq (0)$, A any ring. Prove: if A is any (commutative) ring then i. $\Longrightarrow$ iii., and if A is good local i. and iii. are equivalent. Show further that if A is good local then $\mathcal{M}(\Gamma)$ possesses a non-trivial idempotent, P, (an element such that $P * P = P$, $P \neq 0, \neq 1$) if and only if Γ has ii.

4. Write $\mathcal{I} = \{U \in \mathcal{M}(\Gamma) \mid \Gamma U \Gamma = 0\}$ and given $P \in \mathcal{M}(\Gamma)$, set

$$B(P) = \{V \in \mathcal{M}(\Gamma) \mid (\exists\, Z \in \mathcal{M}(\Gamma))(V = P * Z * P)\}.$$

If iii. above holds, show there exists $P \in \mathcal{M}(\Gamma)$ so that $P * P = P$ and $\Gamma P \Gamma = \Gamma$. For such a P, prove that $B(P)$ is a subring of $\mathcal{M}(\Gamma)$, that $\mathcal{M}(\Gamma) \cong B(P) \amalg \mathcal{I}$ in the category of A-modules, and that $\mathcal{I}$ is a two-sided ideal of $\mathcal{M}(\Gamma)$ (by exhibiting $\mathcal{I}$ as the kernel of a surjective ring homomorphism whose image you should find). Further show if i. holds, then $B(P)$ is isomorphic to the ring of $r \times r$ matrices with entries from A. When A is a field show $\mathcal{I}$ is a maximal 2-sided ideal of $\mathcal{M}(\Gamma)$, here $\Gamma \neq (0)$. Is $\mathcal{I}$ the unique maximal (2-sided) ideal in this case?

5. Call an idempotent, P, of a ring *maximal* (also called *principal*) iff when L is another idempotent, then $PL = 0 \implies L = 0$. Suppose Γ satisfies condition iii. above, prove that an idempotent, P, of $\mathcal{M}(\Gamma)$ is maximal iff $\Gamma P \Gamma = \Gamma$.

Problem 32 Let A be the field of real numbers $\mathbb{R}$ and conserve the notations of Problem 31. Write X for a $p \times q$ matrix of functions of one variable, t, and consider the Γ-*Riccati Equation*

$$\frac{dX}{dt} = X \Gamma X. \tag{$(*)_\Gamma$}$$

1. If $q = p$ and Γ is invertible, show that either the solution, $X(t)$, blows up at some finite t, or else $X(t)$ is equivalent to a matrix

$$\widetilde{X}(t) = \begin{pmatrix} 0 & O(1) & O(t) & \dots & O(t^{p-1}) \\ 0 & 0 & O(1) & \dots & O(t^{p-2}) \\ & & \cdots\cdots\cdots & & \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

where $O(t^s)$ means a polynomial of degree $\leq s$. Hence, in this case, $X(t)$ must be nilpotent.

2. Suppose $q \neq p$ and Γ has rank r. Let P be an idempotent of $\mathcal{M}(\Gamma)$ with $\Gamma P \Gamma = \Gamma$. If $Z \in \mathcal{M}(\Gamma)$, write $Z^\flat$ for $Z - P * Z * P$; so $Z^\flat \in \mathcal{I}$. Observe that $\mathcal{I}$ has dimension $pq - r^2$ as an $\mathbb{R}$-vector space. Now assume that for a solution, $X(t)$, of $(*)_\Gamma$, we have $X(0) \in \mathcal{I}$. Prove that $X(t)$ exists for all t. Can you give necessary and sufficient conditions for $X(t)$ to exist for all t?

3. Apply the methods of (2) to the case $p = q$ but $r = \operatorname{rank} \Gamma < p$. Give a similar discussion.

Problem 33 A module, M, over a ring, R, is called *indecomposable* iff we *cannot* find two submodules M_1 and M_2 of M so that $M \xrightarrow{\sim} M_1 \amalg M_2$ in the category of R-modules.

1. Every ring is a module over itself. Show that if R is a local ring, then R is indecomposable as an R-module.

2. Every ring, R, with unity admits a homomorphism $\mathbb{Z} \to R$ (i.e., $\mathbb{Z}$ is an *initial object* in the category RNG). The kernel of $\mathbb{Z} \to R$ is the principal ideal $n\mathbb{Z}$ for some $n \geq 0$; this n is the *characteristic of* R. Show that the characteristic of a local ring must be 0 or a prime power. Show by example that every possibility occurs as a characteristic of some local ring.

3. Pick a point in $\mathbb{R}$ or $\mathbb{C}$; without loss of generality, we may assume this point is 0. If f is a function we say f is locally defined at 0 iff f has a domain containing some (small) open set, U, about 0 (in either $\mathbb{R}$ or $\mathbb{C}$). Here, f is $\mathbb{R}$- or $\mathbb{C}$-valued, independent of where its domain is. When f and g are locally defined at 0, say f makes sense on U and g on V, we'll call f and g *equivalent at* 0 $\iff$ there exists open W, $0 \in W$, $W \subseteq U \cap V$ and $f \restriction W = g \restriction W$. A *germ of a function at* 0 is an equivalence class of a function. If we consider germs of functions that are at least continuous near 0, then when they form a ring they form a local ring.
Consider the case $\mathbb{C}$ and complex valued germs of holomorphic functions at 0. This is a local ring. Show it is a good local ring.
In the case $\mathbb{R}$, consider the germs of real valued C^k functions at 0, for some k with $0 \leq k \leq \infty$. Again, this is a local ring; however, show it is NOT a good local ring.
Back to the case $\mathbb{C}$ and the good local ring of germs of complex valued holomorphic functions at 0. Show that this local ring is also a principal ideal *domain*.

   In the case of real valued C^∞ germs at $0 \in \mathbb{R}$, exhibit an infinite set of germs, each in the maximal ideal, no finite subset of which generates the maximal ideal (in the sense of ideals). These germs are NOT to belong to $\mathfrak{m}^2$.

Problem 34 Recall that for every integral domain, A, there is a field, $\mathrm{Frac}(A)$, containing A minimal among all fields containing A. If B is an A-algebra, an element $b \in B$ is *integral over* $A \iff$ there exists a *monic* polynomial, $f(X) \in A[X]$, so that $f(b) = 0$. The domain, A, is *integrally closed in* B iff every $b \in B$ which is integral over A actually comes from A (*via* the map $A \to B$). The domain, A, is *integrally closed* (also called *normal*) iff it is integrally closed in $\mathrm{Frac}(A)$. Prove:

1. A is integrally closed $\iff$ $A[X]/\big(f(X)\big)$ is an integral domain for every MONIC irreducible polynomial, $f(X)$.

2. A is a UFD $\iff$ A possesses the ACC on principal ideals and $A[X]/\big(f(X)\big)$ is an integral domain for every irreducible polynomial $f(X)$. (It follows that every UFD is a normal domain.)

3. If k is a field and the characteristic of k is not 2, show that $A = k[X, Y, Z, W]/(XY - ZW)$ is a normal domain. What happens if $\mathrm{char}(k) = 2$?

Problem 35 Suppose that R is an integral domain and F is its fraction field, $\mathrm{Frac}(R)$. Prove that, as R-module, the field F is "the" injective hull of R. A sufficient condition that F/R be injective is that R be a PID. Is this condition necessary? Proof or counter-example.

Problem 36 If A is a ring, write $\mathrm{End}^*(A)$ for the collection of *surjective* ring endomorphisms of A. Suppose A is commutative and noetherian, prove $\mathrm{End}^*(A) = \mathrm{Aut}(A)$.

Problem 37 Write $M(n, A)$ for the ring of all $n \times n$ matrices with entries from A (A is a ring). Suppose K and k are fields and $K \supseteq k$.

1. Show that if $M, N \in M(n, k)$ and if there is a $P \in \mathrm{GL}(n, K)$ so that $PMP^{-1} = N$, then there is a $Q \in \mathrm{GL}(n, k)$ so that $QMQ^{-1} = N$.

2. Prove that (1) is false for rings $B \supseteq A$ *via* the following counterexample:
   $A = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$, $B = \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$. Find two matrices similar in $M(2, B)$ but NOT similar in $M(2, A)$.

3. Let S^n be the n-sphere and represent $S^n \subseteq \mathbb{R}^{n+1}$ as $\{(z_0, \ldots, z_n) \in \mathbb{R}^{n+1} \mid \sum_{j=0}^n z_j^2 = 1\}$. Show that there is a *natural injection* of $\mathbb{R}[X_0, \ldots, X_n]/(\sum_{j=0}^n X_j^2 - 1)$ into $C(S^n)$, the ring of (real valued) continuous functions on S^n. Prove further that the former ring is an integral domain but $C(S^n)$ is not. Find the group of units in the former ring.

Problem 38 (Rudakov) Say A is a ring and M is a rank 3 free A-module. Write Q for the bilinear form whose matrix (choose some basis for M) is

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus, if $v = (x, y, z)$ and $w = (\xi, \eta, \zeta)$, we have

$$Q(v, w) = (x, y, x) \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix}.$$

Prove that $Q(w, v) = Q(v, Bw)$ with $B = I + \text{nilpotent} \iff a^2 + b^2 + c^2 = abc$.

Problem 39 Let M be a Λ-module (Λ is not necessarily commutative) and say N and N' are submodules of M.

1. Suppose $N + N'$ and $N \cap N'$ are f.g. Λ-modules. Prove that both N and N' are then f.g. Λ-modules.
2. Give a generalization to finitely many submodules, $N_1, \ldots, N_t$ of M.
3. Can you push part (2) to an infinite number of N_j?
4. If M is noetherian as a Λ-module, is Λ necessarily noetherian as a ring (left noetherian as M is a left module)? What about $\overline{\Lambda} = \Lambda/\text{Ann}(M)$?

Problem 40 Suppose that V is a not necessarily finite dimensional vector space over a field, k. We assume given a map from *subsets*, S, of V to *subspaces*, $[S]$, of V which map satisfies:

(a) For every S, we have $S \subseteq [S]$

(b) $[\,]$ is monotone; that is, $S \subseteq T \quad \text{implies} \quad [S] \subseteq [T]$.

(c) For every S, we have $[S] = [[S]]$

(d) If W is a subspace of V and $W \neq V$, then $[W] \neq V$.

(1) Under conditions (a)—(d), prove that $[S] = \text{Span}\, S$.

(2) Give counter-examples to show that the result is false if we remove either (a) or (d). What about (b) or (c)?

(3) What happens if we replace k by a ring R, consider subsets and submodules and replace $\text{Span}\, S$ by the R-module generated by S?

Problem 41 (Continuation of Problem 34)

1. Consider the ring $A(n) = \mathbb{C}[X_1, \ldots, X_n]/(X_1^2 + \cdots + X_n^2)$. There is a condition on n, call it $C(n)$, so that $A(n)$ is a UFD iff $C(n)$ holds. Find explicitly $C(n)$ and prove the theorem.
2. Consider the ring $B(n) = \mathbb{C}[X_1, \ldots, X_n]/(X_1^2 + X_2^2 + X_3^3 + \cdots + X_n^3)$. There is a condition on n, call it $D(n)$, so that $B(n)$ is a UFD iff $D(n)$ holds. Find explicitly $D(n)$ and prove the theorem.
3. Investigate exactly what you can say if $C(n)$ (respectively $D(n)$) does not hold.
4. Replace $\mathbb{C}$ by $\mathbb{R}$ and answer (1) and (2).

5. Can you formulate a theorem about the ring $A[X,Y]/\big(f(X,Y)\big)$ of the form $A[X,Y]/\big(f(X,Y)\big)$ is a UFD provided $f(X,Y)\cdots$? Here, A is a given UFD and f is a polynomial in $A[X,Y]$. Your theorem must be general enough to yield (1) and (2) as easy consequences. (You must prove it too.)

Problem 42 (Exercise on projective modules) In this problem, $A \in \mathcal{O}\mathrm{b}(\mathrm{CR})$.

1. Suppose P and P' are projective A-modules, and M is an A-module. If
$$0 \to K \to P \to M \to 0 \qquad \text{and}$$
$$0 \to K' \to P' \to M \to 0$$
are exact, prove that $K' \amalg P \cong K \amalg P'$.

2. If P is a f.g. projective A-module, write P^D for the A-module $\mathrm{Hom}_A(P,A)$. We have a canonical map $P \to P^{DD}$. Prove this is an isomorphism.

3. Again, P is f.g. projective; suppose we're given an A-linear map $\mu : \mathrm{End}_A(P) \to A$. Prove: there exists a unique element $f \in \mathrm{End}_A(P)$ so that $(\forall\, h \in \mathrm{End}_A(P))(\mu(h) = \mathrm{tr}(hf))$. Here, you must define the trace, tr, for f.g. projectives, P, as a well-defined map, then prove the result.

4. Again, P is f.g. projective; μ is as in (3). Show that $\mu(gh) = \mu(hg) \iff \mu = a\,\mathrm{tr}$ for some $a \in A$.

5. Situation as in (2), then each $f \in \mathrm{End}_A(P)$ gives rise to $f^D \in \mathrm{End}_A(P^D)$. Show that $\mathrm{tr}(f) = \mathrm{tr}(f^D)$.

6. Using categorical principles, reformulate (1) for injective modules and prove your reformulation.

Problem 43 Suppose K is a commutative ring and $a, b \in K$. Write $A = K[T]/(T^2 - a)$; there is an automorphism of A (the identity on K) which sends t to $-t$, where t is the image of T in A. If $\xi \in A$, we write $\overline{\xi}$ for the image of ξ under this automorphism. Let $\mathbb{H}(K; a, b)$ denote the set
$$\mathbb{H}(K;a,b) = \left\{ \begin{pmatrix} \xi & b\eta \\ \overline{\eta} & \overline{\xi} \end{pmatrix} \;\middle|\; \xi, \eta \in A \right\},$$
this is a subring of the 2×2 matrices over A. Observe that $q \in \mathbb{H}(K; a, b)$ is a unit there iff q is a unit of the 2×2 matrices over A.

1. Consider the non-commutative polynomial ring $K\langle X, Y\rangle$. There is a 2-sided ideal, $\mathcal{I}$, in $K\langle X, Y\rangle$ so that $\mathcal{I}$ is symmetrically generated *vis a vis* a and b and $K\langle X, Y\rangle/\mathcal{I}$ is naturally isomorphic to $\mathbb{H}(K; a, b)$. Find the generators of $\mathcal{I}$ and establish the explicit isomorphism.

2. For pairs (a, b) and (α, β) decide exactly when $\mathbb{H}(K; a, b)$ is isomorphic to $\mathbb{H}(K; \alpha, \beta)$ as objects of the comma category RNG^K.

3. Find all isomorphism classes of $\mathbb{H}(K; a, b)$ when $K = \mathbb{R}$ and when $K = \mathbb{C}$. If $K = \mathbb{F}_p$, $p \neq 2$ answer the same question and then so do for $\mathbb{F}_2$.

4. When K is just some field, show $\mathbb{H}(K; a, b)$ is a "division ring" (all non-zero elements are units) $\iff$ the equation $X^2 - aY^2 = b$ has no solution in K (here we assume a is not a square in K). What is the case if a *is* a square in K?

5. What is the center of $\mathbb{H}(K; a, b)$?

6. For the field $K = \mathbb{Q}$, prove that $\mathbb{H}(\mathbb{Q}; a, b)$ is a division ring $\iff$ the surface $aX^2 + bY^2 = Z^2$ has no points whose coordinates are integers except 0.

Problem 44

1. If A is a commutative ring and $f(X) \in A[X]$, suppose $(\exists\, g(X) \neq 0)(g(X) \in A[X]$ and $g(X)f(X) = 0)$. Show: $(\exists\, \alpha \in A)(\alpha \neq 0$ and $\alpha f(X) = 0)$. *Caution*: A may possess non-trivial nilpotent elements.

2. Say K is a field and $A = K[X_{ij},\, 1 \leq i, j \leq n]$. The matrix

$$M = \begin{pmatrix} X_{11} & \dots & X_{1n} \\ & \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ X_{n1} & \dots & X_{nn} \end{pmatrix}$$

has entries in A and $\det(M) \in A$. Prove that $\det(M)$ is an irreducible polynomial of A.

Problem 45 Let A be a commutative noetherian ring and suppose B is a commutative A-algebra which is f.g. as an A-algebra. If $G \subseteq \mathrm{Aut}_{A-\mathrm{alg}}(B)$ is a *finite* subgroup, write

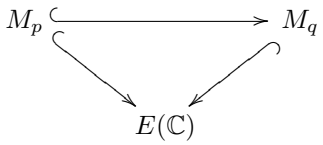
$$B^G = \{b \in B \mid \sigma(b) = b,\ \text{all } \sigma \in G\}.$$

Prove that B^G is also f.g. as an A-algebra; hence B^G is noetherian.

Problem 46 Again, A is a commutative ring. Write $\mathrm{RCF}(A)$ for the ring of $\infty \times \infty$ matrices all of whose rows and all of whose columns possess but finitely many (*not* bounded) non-zero entries. This *is* a ring under ordinary matrix multiplication (as you see easily).

1. Specialize to the case $A = \mathbb{C}$; find a *maximal* two-sided ideal, $\mathcal{E}$, of $\mathrm{RCF}(\mathbb{C})$. Prove it is such and is the only such. You are to find $\mathcal{E}$ explicitly. Write $E(\mathbb{C})$ for the ring $\mathrm{RCF}(\mathbb{C})/\mathcal{E}$.

2. Show that there exists a natural injection of rings M_n ($= n \times n$ complex matrices) $\hookrightarrow \mathrm{RCF}(\mathbb{C})$ so that the composition $M_n \to E(\mathbb{C})$ is *still* injective. Show further that if $p \mid q$ we have a commutative diagram



Problem 47 (Left and right noetherian) For parts (1) and (2), let $A = \mathbb{Z}\langle X, Y\rangle/(YX, Y^2)$—a non-commutative ring.

1. Prove that

$$\mathbb{Z}[X] \hookrightarrow \mathbb{Z}\langle X, Y\rangle \to A$$

is an injection and that $A = \mathbb{Z}[X] \amalg \big(\mathbb{Z}[X]y\big)$ as a left $\mathbb{Z}[X]$-module (y is the image of Y in A); hence A is a left noetherian ring.

2. However, the right ideal generated by $\{X^n y \mid n \geq 0\}$ is NOT f.g. (prove!); so, A is not right noetherian.

3. Another example. Let

$$C = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a \in \mathbb{Z};\, b, c, \in \mathbb{Q} \right\}.$$

Then C is right noetherian but NOT left noetherian (prove!).

Problem 48 If $\{B_\alpha, \varphi_\alpha^\beta\}$ is a right mapping system of Artinian rings and if $B = \varinjlim_\alpha B_\alpha$ and B is noetherian, prove that B is Artinian.

Problem 49 Suppose that A is a commutative noetherian ring and B is a given A-algebra which is flat and finite as an A-module. Define a functor $Idem_{B/A}(-)$ which associates to each A-algebra, T the set $Idem_{B/A}(T) = \mathrm{Idem}(B \otimes_A T)$ consisting of all idempotent elements of the ring $B \otimes_A T$.

(1) Prove the functor $Idem_{B/A}$ is representable.

(2) Show the representing ring, C, is a noetherian A-algebra and that it is *étale* over A.

Problem 50 (Vector bundles) As usual, TOP is the category of topological spaces and k will be either the real or complex numbers. All vector spaces are to be finite dimensional. A *vector space family over* X is an object, V, of TOP_X (call p the map $V \to X$) so that

i. $(\forall\, x \in X)(p^{-1}(x)$ (denoted V_x) is a k-vector space)

ii. The induced topology on V_x is the usual topology it has as a vector space over k.

Example: The trivial family $X \amalg k^n$ (fixed n).
Vector space families over X form a category, $\mathrm{VF}(X)$, if we define the morphisms to be those morphisms, φ, from TOP_X which satisfy:

$$(\forall\, x \in X)(\varphi_x : V_x \to W_x \text{ is a linear map.})$$

1. Say $Y \xrightarrow{\theta} X$ is a continuous map. Define a functor $\theta^* : \mathrm{VF}(X) \rightsquigarrow \mathrm{VF}(Y)$, called pullback. When Y is a subspace of X, the pullback, $\theta^*(V)$, is called the restriction of V to Y, written $V \restriction Y$.
A vector space family is a *vector bundle* $\iff$ it is *locally trivial*, that is:
$(\forall\, x \in X)(\exists$ open $U)(x \in U)$ (so that $V \restriction U$ is isomorphic (in $\mathrm{VF}(U)$) to $U \amalg k^n$, some n). Let $\mathrm{Vect}(X)$ denote the *full* subcategory of $\mathrm{VF}(X)$ formed by the objects that are vector bundles.

2. Say X is an r-dimensional vector space considered in TOP. Write $\mathbb{P}(X)$ for the collection of all hyperplanes through $0 \in X$, then $\mathbb{P}(X)$ is a topological space and is covered by opens each isomorphic to an $(r-1)$-dimensional vector space. On $\mathbb{P}(X)$ we make an element of $\mathrm{VF}\big(\mathbb{P}(X)\big)$: W is the set of pairs $(\xi, \nu) \in \mathbb{P}(X) \amalg X^D$ so that $\xi \subset \ker \nu$. Here, X^D is the dual space of X. Show that W is a line bundle on $\mathbb{P}(X)$.

3. If $V \in \mathrm{Vect}(X)$ and X is connected, then $\dim(V_x)$ is constant on X. This number is the *rank* of V.

4. A *section of* V *over* U is a map $\sigma : U \to V \restriction U$ so that $p \circ \sigma = \mathrm{id}_U$. Write $\Gamma(U, V)$ for the collection of sections of V over U. Show: If $V \in \mathrm{Vect}(X)$, each section of V over U is just a compatible family of locally defined vector valued functions on U. Show further that $\Gamma(U, V)$ is a vector space in a natural way.

5. Say V and W are in $\mathrm{Vect}(X)$, with ranks p and q respectively. Show: $\mathrm{Hom}(V, W)$ is isomorphic to the collection of locally defined "compatible" families of *continuous* functions $U \to \mathrm{Hom}(k^p, k^q)$, *via* the local description
$$\varphi \in \mathrm{Hom}(V, W) \rightsquigarrow \widetilde{\varphi} : U \to \mathrm{Hom}(k^p, k^q),$$
where $\varphi(u, v) = \big(u, \widetilde{\varphi}(u)(v)\big)$. Here, $V \restriction U$ is trivial and $v \in k^p$.

   Now $\mathrm{Iso}(k^p, k^q) = \{\psi \in \mathrm{Hom}(k^p, k^q) \mid \psi \text{ is invertible}\}$ is an open of $\mathrm{Hom}(k^p, k^q)$.

6. Show: $\varphi \in \mathrm{Hom}(V, W)$ is an isomorphism $\iff$ for a covering family of opens, $U(\subseteq X)$, we have $\widetilde{\varphi}(U) \subseteq \mathrm{Iso}(k^p, k^q) \iff (\forall\, x \in X)(\varphi_x : V_x \to W_x$ is an isomorphism).

7. Show $\{x \mid \varphi_x$ is an isomorphism (here, $\varphi \in \mathrm{Hom}(U, V))\}$ is open in X.

8. Show all of (1) to (6) go over when $X \in C^k\text{–MAN}$ $(0 \le k \le \infty)$ with appropriate modifications; C^k replacing continuity where it appears.

Problem 51 (Linear algebra for vector bundles). First just look at finite dimensional vector spaces over k (remember k is $\mathbb{R}$ or $\mathbb{C}$) and say F is some functor from vector spaces to vector spaces (F might even be a several variable functor). Call F *continuous* $\iff$ the map $\mathrm{Hom}(V,W) \to \mathrm{Hom}\big(F(V),F(W)\big)$ is continuous. (Same definition for C^k, $1 \le k \le \infty$, ω). If we have such an F, extend it to bundles *via* the following steps:

1. Suppose V is the trivial bundle: $X \amalg k^p$. As sets, $F(X \amalg k^p)$, is to be just $X \amalg F(k^p)$, so we give $F(X \amalg k^p)$ the product topology. Prove: If $\varphi \in \mathrm{Hom}(V,W)$, then $F(\varphi)$ is continuous, therefore $F(\varphi) \in \mathrm{Hom}\big(F(V),F(U)\big)$. Show, further, φ is an isomorphism $\implies$ $F(\varphi)$ is an isomorphism.

2. Set $F(V) = \bigcup_{x\in X}(x, V_x)$, then the topology on $F(V)$, when V is trivial, appears to depend on the specific trivialization. Show this is not true—it is actually independent of same.

3. If V is any bundle, then $V \restriction U$ is trivial for small open U, so by (1) and (2), $F(V \restriction U)$ is a trivial bundle. Topologize $F(V)$ by calling a set, Z, open iff $Z \cap \big(F(V \restriction U)\big)$ is open in $F(V \restriction U)$ for all U where $V \restriction U$ is trivial. Show that if $Y \subseteq X$, then the topology on $F(V \restriction Y)$ is just that on $F(V) \restriction Y$, that $\varphi : V \to W$ continuous $\implies$ $F(\varphi)$ is continuous and extend all these things to C^k. Finally prove: If $f : Y \to X$ in TOP then $f^*\big(F(V)\big) \cong F\big(f^*(V)\big)$ and similarly in C^k-MAN.

4. If we apply (3) , we get for vector bundles:

   (a) $V \amalg W$, more generally finite coproducts

   (b) V^D, the dual bundle

   (c) $V \otimes W$

   (d) $\mathcal{H}om(V,W)$, the vector bundle of (locally defined) homomorphisms.

   Prove: $\Gamma\big(U, \mathcal{H}om(V,W)\big) \cong \mathrm{Hom}(V \restriction U, W \restriction U)$ for *every* open, U, of X. Is this true for the bundles of (a), (b), (c)?

Problem 52 Recall that if $R \in \mathrm{RNG}$, $J(R)$—the Jacobson radical of R— is just the intersection of all (left) maximal ideals of R. The ideal, $J(R)$, is actually 2-sided.

1. Say $J(R) = (0)$ (e.g., $R = \mathbb{Z}$). Show that no non-projective R-module has a projective cover.

2. Suppose M_i, $i = 1, \dots, t$ are R-modules with projective covers $P_1, \dots, P_t$. Prove that $\coprod_i P_i$ is a projective cover of $\coprod_i M_i$.

3. Say M and N are R-modules and assume M and $M \amalg N$ have projective covers. Show that N has one.

4. In M is an R-module, write (as usual) $M^D = \mathrm{Hom}_R(M,R)$. Then M^D is an R^{op}-module. Prove that if M is finitely generated and projective as an R-module, then M^D has the same properties as an R^{op}-module.

Problem 53 Let $\{M_\alpha\}$ be a given family of R^{op}-modules. Define, for R-modules, two functors:

$$U : N \rightsquigarrow \left(\left(\prod_\alpha M_\alpha\right) \otimes_R N\right)$$

$$V : N \rightsquigarrow \prod_\alpha (M_\alpha \otimes_R N).$$

1. Show that V is right-exact and is exact iff each M_α is flat over R.

2. Show there exists a morphism of functors $\theta : U \to V$. Prove that $\theta_N : U(N) \to V(N)$ is surjective if N is finitely generated, while θ_N is an isomorphism if N is finitely presented.

Problem 54 (Continuation of Problems 50 and 51). Let V and W be vector bundles and $\varphi\colon V \to W$ a homomorphism. Call φ a *monomorphism* (respectively *epimorphism*) iff
$(\forall\, x \in X)(\varphi_x\colon V_x \to W_x$ is a monomorphism (respectively epimorphism)). Note: φ is a monomorphism iff $\varphi^D\colon W^D \to V^D$ is an epimorphism. A *sub-bundle* of V is a subset which is a vector bundle in the induced structure.

1. Prove: If $\varphi\colon V \to W$ is a monomorphism, then $\varphi(V)$ is a sub-bundle of W. Moreover, locally on X, there exists a vector bundle, G, say on the open $U \subseteq X$, so that $(V \restriction U) \amalg G \cong W \restriction U$ (i.e., every sub-bundle is *locally* part of a coproduct decomposition of W). Prove also: $\{x \mid \varphi_x$ is a monomorphism$\}$ is open in X. (Suggestion: Say $x \in X$, pick a subspace of W_x complementary to $\varphi(V_x)$, call it Z. Form $G = X \amalg Z$. Then there exists a homomorphism $V \amalg G \to W$, look at this homomorphism near the point x.)

2. Say V is a sub-bundle of W, show that $\bigcup_{x\in X}(x, W_x/V_x)$ (with the quotient topology) is actually a vector bundle (not just a vector space family) over X.

3. Now note we took a full subcategory of $\mathrm{VF}(X)$, so for $\varphi \in \mathrm{Hom}(V, W)$ with $V, W \in \mathrm{Vect}(X)$, the dimension of $\ker \varphi_x$ need not be locally constant on X. When it is locally constant, call φ a *bundle homomorphism*. Prove that if φ is a bundle homomorphism from V to W, then

   (i) $\bigcup_x(x, \ker \varphi_x)$ is a sub-bundle of V

   (ii) $\bigcup_x(x, \operatorname{Im} \varphi_x)$ is a sub-bundle of W, hence

   (iii) $\bigcup_x(x, \operatorname{coker} \varphi_x)$ is a vector bundle (quotient topology).

   We refer to these bundles as $\ker \varphi$, $\operatorname{Im} \varphi$ and $\operatorname{coker} \varphi$, respectively. Deduce from your argument for (i) that

   (iv) Given $x \in X$, there exists an open U, with $x \in U$, so that $(\forall\, y \in U)(\operatorname{rank} \varphi_y \geq \operatorname{rank} \varphi_x)$. Of course, this φ is not necessarily a bundle homomorphism.

Problem 55 (Continuation of Problem 54) In this problem, X is *compact Hasudorff*. We use two results from analysis:

A) (Tietze extension theorem). If X is a normal space and Y a closed subspace while V is a real vector space, then every continuous map $Y \to V$ admits an extension to a continuous map $X \to V$. Same result for $X \in C^k\text{−MAN}$ and C^k maps.

B) (Partitions of unity). Say X is compact Hausdorff and $\{U_\alpha\}$ is a finite open cover of X. There exist continuous maps, f_α, taking X to $\mathbb{R}$ such that

   (i) $f_\alpha \geq 0$, (all α)

   (ii) $\operatorname{supp}(f_\alpha) \subseteq U_\alpha$ (so $f_\alpha \in C^0_0(U_\alpha)$)

   (iii) $(\forall\, x \in X)(\sum_\alpha f_\alpha(x) = 1)$.

   The same is true for $C^k\text{−MAN}$ (X compact!) and C^k functions ($1 \leq k \leq \infty$).

1. Extend Tietze to vector bundles: If X is compact Hausdorff, $Y \subseteq X$ closed and $V \in \mathrm{Vect}(X)$, then every section $\sigma \in \Gamma(Y, V \restriction Y)$ extends to a section in $\Gamma(X, V)$. (Therefore, there exist *plenty* of continuous or C^∞ global sections of V. FALSE for holomorphic sections). Apply this to the bundle $\mathcal{H}om(V, W)$ and prove: If Y is closed in X with X (as usual) compact Hausdorff or compact C^k-manifold and if $\varphi\colon V \restriction Y \to W \restriction Y$ is an isomorphism of vector bundles, then there exists an open, U, with $Y \subseteq U$, so that φ extends to an isomorphism $V \restriction U \to W \restriction U$.

2. Every vector space possesses a metric (take any of the p-norms, or take the 2-norm for simplicity). It's easy to see that metrics then exist on trivial bundles. In fact, use the 2-norm, so we can "bundleize" the notion of Hermitian form (Problem 51) and get the bundle $\mathcal{H}erm(V)$. Then an Hermitian metric on V is a global section of $\mathcal{H}erm(V)$ which is positive definite, at each $x \in X$. Show every bundle possesses an Hermitian metric.

3. If we are given vector bundles and *bundle homomorphisms*, we say the sequence

$$\cdots \to V_j \to V_{j+1} \to V_{j+2} \to \cdots$$

of such is *exact* iff for each $x \in X$, the sequence of vector spaces

$$\cdots \to V_{j,x} \to V_{j+1,x} \to V_{j+2,x} \to \cdots$$

is exact. Prove: If $0 \to V' \to V \to V'' \to 0$ is an exact sequence of vector bundles and bundle homomorphisms, then $V \cong V' \amalg V''$. (This is not true for holomorphic bundles.)

4. Consider a vector bundle, V, and a subspace, Σ, of the vector space $\Gamma(X, V)$. We get the trivial bundle $X \amalg \Sigma$ and a natural homomorphism $X \amalg \Sigma \to V$, *via*

$$(x, \sigma) \to \sigma(x).$$

Prove: If X is compact Hausdorff (or compact C^k-MAN), there exists a *finite dimensional* subspace, Σ, of $\Gamma(X, V)$ so that the map $X \amalg \Sigma \to V$ is *surjective*. Thus there exists a finite dimensional surjective family of C-(respectively C^k-) sections of V. Use (3) to deduce: Under the usual assumption on X, for each vector bundle, V, on X, there exists a vector bundle, W, on X, so that $V \amalg W$ is a trivial bundle.

5. Write $C(X)$ (respectively $C^k(X)$, $1 \leq k \leq \infty$) for the ring of continuous (respectively C^k) functions (values in our field) on X, where X is compact Hausdorff (respectively a compact manifold). In a natural way (pointwise multiplication), $\Gamma(X, V)$ is an A-module ($A = C(X)$, $C^k(X)$), and Γ gives a functor from vector bundles, V, to $\mathcal{M}\mathrm{od}(A)$. Trivial bundles go to free modules of finite rank over A (why?) Use the results above to prove:

> Γ gives an equivalence of categories: $\mathrm{Vect}(X)$ (as full subcaregory of $VF(X)$) and the full subcategory of A-modules whose objects are f.g. projective modules.

Problem 56

1. Say M is a f.g. $\mathbb{Z}$-module, $\neq (0)$. Prove there exists a prime p so that $M \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \neq (0)$. Deduce: No divisible abelian group [cf. Problem 24] can be f.g.

2. Say M, M'' are $\mathbb{Z}$-modules and M is f.g. while M'' is torsion free. Given $\varphi \in \mathrm{Hom}(M, M'')$ suppose $(\forall \text{ primes } p)$(the induced map $M \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \to M'' \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ *is* a monomorphism). Show that φ is a monomorphism and M is free.

3. If M is a divisible abelian group, prove that M possesses no maximal subgroup. Why does Zorn's Lemma fail?

Problem 57 Given Λ, $\Gamma \in \mathrm{RNG}$ and a ring homomorphism $\Lambda \to \Gamma$ (thus, Γ is a Λ-algebra), if M is a Λ-module, then $M \otimes_\Lambda \Gamma$ has the natural structure of a Γ^{op}-module. Similarly, if Z is both a Λ^{op}-module and a Γ-module, then $Z \otimes_\Lambda M$ is still a Γ-module. Now let N be a Γ-module,

1. Prove there is a *natural* isomorphism

$$\mathrm{Hom}_\Gamma(Z \otimes_\Lambda M, N) \xrightarrow{\sim} \mathrm{Hom}_\Lambda(M, \mathrm{Hom}_\Gamma(Z, N)). \qquad (*)$$

Prove, in fact, the functors $M \rightsquigarrow M \otimes_\Lambda Z$ and $N \rightsquigarrow \mathrm{Hom}_\Gamma(Z, N)$ are adjoint functors, i.e., $(*)$ is functorial.

2. Establish an analog of $(*)$:

$$\mathrm{Hom}_\Gamma(M, \mathrm{Hom}_\Lambda(Z, N)) \cong \mathrm{Hom}_\Lambda(Z \otimes_\Gamma M, N) \qquad (**)$$

under appropriate conditions on Z, M and N (what are they?)

3. Show: M projective as a Λ^{op}-module, Z projective as a Γ^{op}-module $\implies$ $M \otimes_\Lambda Z$ is projective as a Γ^{op}-module. In particular, M projective as a Λ^{op}-module $\implies$ $M \otimes_\Lambda \Gamma$ is projective as a Γ^{op}-module and of course, the same statement (without the op) for $Z \otimes_\Lambda M$ and $\Gamma \otimes_\Lambda M$. Show further that, if N is Λ-injective, then $\mathrm{Hom}_\Lambda(\Gamma, N)$ is Γ-injective.

4. For abelian groups, M, write $M^D = \mathrm{Hom}_\mathbb{Z}(M, \mathbb{Q}/\mathbb{Z})$. Then, if M is free, M^D is injective as a $\mathbb{Z}$-module (why?). From this deduce: Every abelian group is a subgroup of an injective abelian group.

5. (Eckmann) Use (3) and (4) to prove the Baer Embedding Theorem: For every ring, Γ, each Γ-module is a submodule of an injective Γ-module.

Problem 58 Here, A and B are commutative rings and $\varphi : A \to B$ a ring homomorphism so that B is an A-algebra. Assume B is flat (i.e., as an A-module, it's flat). Define a homomorphism

$$\theta : \mathrm{Hom}_A(M, N) \otimes_A B \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$$

(functorial in M and N)—how?

1. If M is f.g. as an A-module, θ is injective.

2. If M is f.p. as an A-module, θ is an isomorphism.

3. Assume M is f.p. as an A-module, write $\mathfrak{a}$ for the annihilator of M $(= (M \to (0)))$. Prove that $\mathfrak{a} \otimes_A B$ is the annihilator of $M \otimes_A B$ in B.

Problem 59 Let k be a field and f be a *monic* polynomial of *even* degree in $k[X]$.

1. Prove there exist g, $r \in k[X]$ such that $f = g^2 + r$ and $\deg r < \frac{1}{2} \deg f$. Moreover, g and r are unique.

   Now specialize to the case $k = \mathbb{Q}$, and suppose f has *integer* coefficients. Assume $f(X)$ is *not* the square of a polynomial with rational coefficients.

2. Prove there exist only *finitely* many integers, x, such that the value $f(x)$ is a square, say y^2, where $y \in \mathbb{Z}$. In which ways can you get the square of an integer, y, by adding 1 to third and fourth powers of an integer, x?

3. Show there exists a constant, K_N, depending ONLY on the degree, N, of f so that:

   > If all coefficients of f are bounded in absolute value by C (≥ 1) then whenever $\langle x, y\rangle$ is a solution of $y^2 = f(x)$ (with x, $y \in \mathbb{Z}$) we have $|x| \leq K_N C^N$.

4. What can you say about the number of points $\langle x, y\rangle$ with rational coordinates which lie on the (hyper-elliptic) curve $Y^2 = f(X)$?

Problem 60 Consider $\mathcal{M}\mathrm{od}(\mathbb{Z})$ and copies of $\mathbb{Z}$ indexed by $\mathbb{N} = \{1, 2, \ldots\}$. Form the module $\prod_{\mathbb{N}} \mathbb{Z}$. It is a product of $\aleph_0$ projective modules. Show $M = \prod_{\mathbb{N}} \mathbb{Z}$ is *not* projective as a $\mathbb{Z}$-module. (Suggestions: Establish that each submodule of a free module over a PID is again free, therefore we need to show M is not free. Look at

$$K = \{\xi = (\xi_j) \in M \mid (\forall\, n)(\exists\, k = k(n))(2^n \mid \xi_j \text{ if } j > k(n))\}.^5$$

This is a submodule of M; show $K/2K$ is a vector space over $\mathbb{Z}/2\mathbb{Z}$ of the same dimension as K and finish up. Of course, 2 could be replaced by any prime). So, products of projectives need not be projective.

[5] The condition means that $\lim_{j \mapsto \infty} \xi_j$ is zero in the "2-adic numbers" $\mathbb{Q}_2$.

Problem 61

1. Say $A \xrightarrow{\theta} B$ is a homomorphism of commutative rings and suppose it makes B a faithfully flat A-module. Show that θ is injective.

2. Hypotheses as in (1), but also assume B is finitely presented as an A-algebra (e.g., B is finitely generated and A is noetherian). Show that there exists an A-module, M, so that $B \cong A \amalg M$, as A-modules.

3. Assume A and B are local rings, $\theta : A \to B$ is a ring map (N.B. so that we assume $\theta(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$) and B, as an A-module, is flat. Write $\mathcal{N}(A)$, respectively $\mathcal{N}(B)$, for the nilradicals of A, respectively B. [That is,

$$\mathcal{N}(A) = \big\{\xi \in A \mid (\exists n \in \mathbb{N})(\xi^n = 0)\big\}, \text{ etc.}]$$

   Prove:

   (a) If $\mathcal{N}(B) = (0)$, then $\mathcal{N}(A) = (0)$.

   (b) If B is an integral domain, so is A.

   Are the converses of (a), (b) true? Proof or counter-example.

Problem 62 Here, I is an index set and $\mathcal{S}(I)$ is the set of all *finite* subsets of I. Partially order $\mathcal{S}(I)$ by inclusion, then it is directed[6] Also, let $\mathcal{C}$ be a category having *finite* products or *finite* coproducts as the case may be below (e.g., groups, Ω-groups, modules). Say for each $\alpha \in I$ we are given an object $M_\alpha \in \mathcal{C}$. For ease of notation below, write $M_S = \coprod_{\alpha \in S} M_\alpha$ and $M_S^* = \prod_{\alpha \in S} M_\alpha$, where $S \in \mathcal{S}(I)$ is given. Prove:
If $\mathcal{C}$ has right limits and finite coproducts, then $\mathcal{C}$ has arbitrary coproducts; indeed,

$$\varinjlim_{S \in \mathcal{S}(I)} M_S = \coprod_{\alpha \in I} M_\alpha.$$

Prove a similar statement for left limits and products.

Problem 63 Recall that a ring, Λ, is *semi-simple*[7] iff every Λ-module, M, has the property:

($\forall$ submodules, M', of M)($\exists$ another submodule, M'', of M)($M \cong M' \amalg M''$).

There is a condition on the positive integer, n, so that n has this condition $\iff$ $\mathbb{Z}/n\mathbb{Z}$ is semi-simple. Find the condition and prove the theorem.

Problem 64 In this problem, $A \in$ CR. If $\alpha_1, \ldots, \alpha_m$ are in A, write $\big(\alpha_1, \ldots, \alpha_n\big)$ for the ideal generated by $\alpha_1, \ldots, \alpha_n$ in A. Recall that $K_0(A)$, the *Grothendieck group* of A, is the quotient of the free abelian group on the (isomorphism classes of) finitely generated A-modules (as generators) by the subgroup generated by the relations: if $0 \to M' \to M \to M'' \to 0$ is exact in $\mathcal{M}\text{od}(A)$, then $[M] - [M'] - [M'']$ is a relation.

1. If $\alpha \in A$, show that in $K_0(A)$ we have

$$\big[((\alpha) \to 0)\big] = \big[A/(\alpha)\big]$$

2. If A is a PID and M is a finite length A-module, show that $[M] = 0$ in $K_0(A)$.

3. Prove: If A is a PID, then for all finitely generated A-modules, M, there exists a unique integer $r = r(M)$, so that $[M] = r[A]$ in $K_0(A)$; hence, $K_0(A)$ is $\mathbb{Z}$. Prove further that $r(M) = \dim(M \otimes_A \text{Frac}(A))$.

[6] One also says $\mathcal{S}(I)$ has the Moore–Smith property.
[7] Cf. also, Problem 145.

Problem 65 Write $\mathcal{LCA}$b for the category of locally compact abelian topological groups, the morphisms being continuous homomorphisms. Examples include: Every abelian group with the discrete topology; $\mathbb{R}$; $\mathbb{C}$; $\mathbb{R}/\mathbb{Z} = \mathbb{T}$, etc. If $G \in \mathcal{LCA}$b, write

$$G^D = \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{T}),$$

make G^D a group *via* pointwise operations and topologize G^D *via* the compact-open topology; that is, take the sets

$$U(C, \epsilon) = \left\{ f \in G^D \mid \mathrm{Im}(f \restriction C) \subseteq -\epsilon < \arg z < \epsilon \right\}$$

—where C runs over the compact subsets of G containing 0, ϵ is positive and we identify $\mathbb{T}$ with the unit circle in $\mathbb{C}$—as a fundamental system of neighborhoods at 0 in G^D.

1. Suppose G is actually compact. Prove G^D is discrete in this topology. Likewise, prove if G is discrete, then G^D is compact in this topology. Finally prove G^D is locally compact in this topology.

2. If $\{G_\alpha, \varphi_\alpha^\beta\}$ is a right (respectively left) mapping family of *finite* abelian groups, then $\left\{G_\alpha^D, \left(\varphi_\alpha^\beta\right)^D\right\}$ becomes a left (respectively right) mapping family, again of *finite* abelian groups (how, why?). Prove that

   $$\left(\varinjlim_\alpha G_\alpha \right)^D \cong \varprojlim_\alpha G_\alpha^D$$

   and

   $$\left(\varprojlim_\alpha G_\alpha \right)^D \cong \varinjlim_\alpha G_\alpha^D$$

   as *topological* groups. We call a group *profinite* $\iff$ it is isomorphic, as a *topological* group, to a left limit of finite groups.

3. Prove the following three conditions are equivalent for an abelian topological group, G:

   (a) G is profinite

   (b) G is a compact, Hausdorff, totally disconnected group

   (c) G^D is a discrete torsion group.

4. For this part, $\left\{G_\alpha\right\}$ is a family of *compact* groups, not necessarily abelian, and the index set has Moore–Smith. Assume we are given, for each α, a closed, normal subgroup of G_α, call it S_α, and that $\beta \geq \alpha \implies G_\beta \subseteq G_\alpha$ and $S_\beta \subseteq S_\alpha$. Show that the family $\left\{H_\alpha = G_\alpha / S_\alpha\right\}_\alpha$ can be made into a left mapping family, in a natural way, and that

   $$\varprojlim_\alpha H_\alpha \cong \bigcap_\alpha G_\alpha / \bigcap_\alpha S_\alpha \quad \text{(as topological groups.)}$$

5. If G is a compact topological group, write $\left\{U_\alpha | \alpha \in I\right\}$ for the family of *all open, normal* subgroups of G. Continue (3) by proving:

   $$G \text{ is profinite} \iff G \text{ is compact and } \bigcap_\alpha U_\alpha = \{1\}.$$

6. Here, G need not be abelian. We define $\mathbb{Z}_p$ as $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ and $\hat{\mathbb{Z}}$ as $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$ (Artin ordering for the n's). Quickly use (2) to compute $\mathbb{Z}_p^D$ and $(\hat{\mathbb{Z}})^D$. Now consider the following mathematical statements:

   (a) $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$

   (b) $\mathbb{Q}^* \cong \mathbb{Z}/2\mathbb{Z} \amalg \prod_p \mathbb{Z}$

(c) $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\frac{1}{1-1/p^s}$, if Re $s>1$

(d) A statement you know well and are to fill in here concerning arithmetic in $\mathbb{Z}$.

Show (a)-(d) are mutually equivalent.

Problem 66 Fix an abelian group, A, for what follows. Write $A_n=A$, all $n\in\mathbb{N}$ and give $\mathbb{N}$ the Artin ordering. If $n\preceq m$ (i.e. $n|m$) define $\varphi_n^m:A_n\to A_m$ by $\varphi_n^m(\xi)=\left(\frac{m}{n}\right)\xi$, and define $\psi_m^n:A_m\to A_n$ by $\psi_m^n(\xi)=\left(\frac{m}{n}\right)\xi$, too. Let

$$\tilde{A}=\varinjlim\left\{A_n,\varphi_n^m\right\}\quad\text{and}\quad T(A)=\varprojlim\left\{A_m,\psi_m^n\right\}.$$

($T(A)=$ *full Tate group of* A).

1. Prove that both $\tilde{A}$ and $T(A)$ are divisible groups.
2. Show that if $A=A_1\xrightarrow{\varphi}\tilde{A}$ is the canonical map into the direct limit, then $\ker(\varphi)=t(A)$, the torsion subgroup of A. Hence, every torsion free abelian group is a subgroup of a divisible group. Given any abelian group , A, write
$$0\to K\to F\to A\to 0,$$
for some free abelian group F. Show that A may be embedded in $\tilde{F}/K$; hence deduce anew that every abelian group embeds in a divisible abelian group.
3. If A is a free $\mathbb{Z}$-module, what is $T(A)$?
4. If $A\to B\to 0$ is exact, need $T(A)\to T(B)\to 0$ also be exact? Proof or counterexample.
5. Show that if $T(A)\neq(0)$, then A is not finitely generated.

Problem 67 Again, as in Problem 61, let $\theta:A\to B$ be a homomorphism of commutative rings and assume B is faithfully flat over A *via* θ. If M is an A-module, write M_B for $M\otimes_A B$.

1. Prove: M is finitely generated as an A-module iff M_B is finitely generated as a B-module.
2. Same as (1) but for finite presentation instead of finite generation.
3. Show: M is locally free over A iff M_B is locally free over B.
4. When, if ever, is $S^{-1}A$ faithfully flat over A?

Note, of course, that these are results on faithfully flat descent.

Problem 68 Here, $\Lambda\in$ RNG and assume

$$0\to M'\to M\to M''\to 0$$

is an exact sequence of Λ-modules.

1. Assume further, M'' is a flat Λ-module. Prove: For all Λ^{op}-modules, N, the sequence
$$0\to N\otimes_\Lambda M'\to N\otimes_\Lambda M\to N\otimes_\Lambda M''\to 0$$
is again exact. (You might look at the special case when M is free first.)
2. Again assume M'' is flat; prove M and M' are flat $\iff$ either is flat. Give an example of Λ, M', M, M'' in which both M and M' are flat but M'' is not flat.

Problem 69 (Topologies, Sheaves and Presheaves). Let X be a topological space. We can make a category, $\mathcal{T}_X$, which is specified by and specifies the topology as follows: $\mathcal{O}\mathrm{b}\,\mathcal{T}_X$ consists of the open sets in X. If $U, V \in \mathcal{O}\mathrm{b}\,\mathcal{T}_X$, we let

$$\mathrm{Hom}(U,V) = \begin{cases} \emptyset & \text{if } U \not\subseteq V, \\ \{\mathrm{incl}\} & \text{if } U \subseteq V, \end{cases}$$

here $\{\mathrm{incl}\}$ is the one element set consisting of the inclusion map $\mathrm{incl} : U \to V$.

1. Show that $U \underset{X}{\amalg} V$—the fibred product of U and V (over X) in $\mathcal{T}_X$—is just $U \cap V$. Therefore $\mathcal{T}_X$ has finite fibred products.

2. If $\mathcal{C}$ is a given category (think of $\mathcal{C}$ as $\mathcal{S}$ets, $\mathcal{A}$b, or more generally Λ-$\mathcal{M}$odules) a *presheaf on X with values in $\mathcal{C}$* is a cofunctor from $\mathcal{T}_X$ to $\mathcal{C}$. So, F is a presheaf iff $(\forall \text{ open } U \subseteq X)(F(U) \in \mathcal{C})$ and when $U \hookrightarrow V$, we have a map $\rho_V^U : F(V) \to F(U)$ (in $\mathcal{C}$) usually called *restriction from V to U*. Of course, we have $\rho_V^W = \rho_U^W \circ \rho_V^U$. The basic example, from which all the terminology comes, is this:

$$\mathcal{C} = \mathbb{R}\text{-modules } (= \text{vector spaces over } \mathbb{R})$$
$$F(U) = \{\text{continuous real valued functions on the open set } U\}.$$

   Now recall that a category is an *abelian category* iff for each morphism $A \xrightarrow{\varphi} B$ in $\mathcal{C}$, there are two pairs: $(\ker\varphi, i)$ and $(\mathrm{coker}\,\varphi, j)$ with $\ker\varphi$ and $\mathrm{coker}\,\varphi$ objects of $\mathcal{C}$ and $i : \ker\varphi \to A$, $j : B \to \mathrm{coker}\,\varphi$ so that:

   (a) $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is an abelian group, operation denoted $+$
   (b) $\ker\varphi \to A \to B$ is zero in $\mathrm{Hom}_{\mathcal{C}}(\ker\varphi, B)$
   (c) If $C \xrightarrow{u} A \to B$ is zero, there is a unique morphism $C \to \ker\varphi$ so that u is the composition $C \to \ker\varphi \xrightarrow{i} A$
   (d) Similar to (c) for coker, with appropriate changes.

   Define $\mathrm{Im}\,\varphi$ as $\ker(B \xrightarrow{j} \mathrm{coker}\,\varphi)$. Now exact sequences make sense in $\mathcal{C}$ (easy, as you see). Write $\mathcal{P}(X, \mathcal{C})$ for the category of presheaves on X with values in $\mathcal{C}$. If $\mathcal{C}$ is abelian show that $\mathcal{P}(X, \mathcal{C})$ is an abelian category, too, in a natural way.

3. If $A \in \mathcal{O}\mathrm{b}\,\mathcal{C}$, we can make a presheaf $\mathfrak{A}$ by: $\mathfrak{A}(U) = A$, all open U and if $V \hookrightarrow U$ then $\rho_V^U = id_A$. This is the *constant presheaf* with values in A. Generalize it as follows: Fix open U of X, define $\mathfrak{A}_U$ by:

$$\mathfrak{A}_U(W) = \coprod_{\mathrm{Hom}(W,U)} A = \begin{cases} (0) & \text{if } W \not\subseteq U \\ A & \text{if } W \subseteq U. \end{cases}$$

   Show $\mathfrak{A}_U$ is a presheaf and $\mathfrak{A}$ is one of these $\mathfrak{A}_U$; which one? Generalize further: Say $\mathcal{F}$ is a presheaf of sets on X, define $\mathfrak{A}_{\mathcal{F}}$ by:

$$\mathfrak{A}_{\mathcal{F}}(W) = \coprod_{\mathcal{F}(W)} A = \big\{\text{functions} : \mathcal{F}(W) \to A \mid \text{these functions have finite support}\big\}.$$

   Make $\mathfrak{A}_{\mathcal{F}}$ into a presheaf on X; it is a clear generalization of $\mathfrak{A}_U$ and this, in turn, generalizes $\mathfrak{A}$.

4. Just as with the defining example in (2), which is called the *presheaf of germs of continuous functions on X*, so we can define the presheaf of germs of C^k-functions, real-analytic functions, complex holomorphic functions, meromorphic functions when X is a real (resp. complex) manifold. Namely:

$$C^k(U) = \{f : U \to \mathbb{R} \mid f \text{ is } C^k \text{ on } U\} \quad 0 \le k \le \infty$$
$$C^\omega(U) = \{f : U \to \mathbb{R} \mid f \text{ is real analytic on } U\}$$
$$\mathrm{Hol}(U) = \{f : U \to \mathbb{C} \mid f \text{ is holomorphic on } U\}$$
$$\mathrm{Mer}(U) = \{f : U \to \mathbb{C} \mid f \text{ is meromorphic on } U\}.$$

Prove: The collection $\{\mathfrak{Z}_U \mid U \text{ open in } X\}$ is *a set of generators* for $\mathcal{P}(X, \mathcal{A}\text{b})$; that is: For all presheaves $\mathcal{F}$, there is a subcollection of the U's, say $\{U_\alpha \mid \alpha \in \Lambda\}$, so that there is a surjection $\coprod_I \left(\coprod_{\alpha\in\Lambda} \mathfrak{Z}_U \right) \twoheadrightarrow \mathcal{F}$, for some *set* I. (Then it turns out that every presheaf embeds in an injective presheaf.)

5. Now sheaves are special kinds of presheaves. Say $U \in \mathcal{T}_X$ and we have a family of morphisms of $\mathcal{T}_X$: $\{U_\alpha \to U\}_{\alpha\in\Lambda}$ (we'll suppress mention of Λ in what follows). We call this family a *covering family* $\iff \bigcup_\alpha U_\alpha = U$, i.e. the U_α form an open covering of U. Of course, if $\xi \in F(U)$, then $\rho_U^{U_\alpha}(\xi) \in F\big(U_\alpha\big)$, each α; here, F is a presheaf. Hence we get a map

$$\theta : F(U) \to \prod_\alpha F\big(U_\alpha\big).$$

Now if $\xi_\alpha \in F\big(U_\alpha\big)$, for each α, then $\rho_{U_\alpha}^{U_\alpha\cap U_\beta}\big(\xi_\alpha\big)$ lies in $F\big(U_\alpha \cap U_\beta\big)$ therefore we get a map

$$p_{1,\alpha} : F\big(U_\alpha\big) \to \prod_\beta F\big(U_\alpha \cap U_\beta\big).$$

Take the product of these over α and get a map

$$p_1 : \prod_\alpha F\big(U_\alpha\big) \to \prod_{\alpha,\beta} F\big(U_\alpha \cap U_\beta\big).$$

If $\xi_\beta \in F\big(U_\beta\big)$ then $\rho_{U_\beta}^{U_\alpha\cap U_\beta}\big(\xi_\beta\big) \in F\big(U_\alpha \cap U_\beta\big)$ therefore we get a map

$$p_{2,\beta} : F\big(U_\beta\big) \to \prod_\alpha F\big(U_\alpha \cap U_\beta\big).$$

Again the product over β gives:

$$p_2 : \prod_\beta F\big(U_\beta\big) \to \prod_{\alpha,\beta} F\big(U_\alpha \cap U_\beta\big),$$

hence we get two maps:

$$\prod_\gamma F\big(U_\gamma\big) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\alpha,\beta} F\big(U_\alpha \cap U_\beta\big).$$

Here is the definition of a *sheaf*: A *sheaf, F, of sets* is a presheaf, F, of sets so that ($\forall$ open U) $\Big(\forall$ covers $\big\{U_\alpha \to U\big\}_\alpha\Big)$, the sequence

$$F(U) \xrightarrow{\theta} \prod_\gamma F\big(U_\gamma\big) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\alpha,\beta} F\big(U_\alpha \cap U_\beta\big) \tag{S}$$

is exact in the sense that θ *maps* $F(U)$ *bijectively* to the set $\big(\xi_\gamma\big) \in \prod_\gamma F\big(U_\gamma\big)$ for which $p_1\big(\big(\xi_\gamma\big)\big) = p_2\big(\big(\xi_\gamma\big)\big)$.

Show that the presheaves of germs of continuous, k-fold continuous, differentiable, analytic, holomorphic and meromorphic functions are all sheaves. In so doing understand what exactness of sequence (S) means. Prove, however, that $\mathfrak{A}$ is NOT generally a sheaf. (Note: a sheaf with values in $\mathcal{A}$b or RNG or Ω-groups is just a presheaf with these values which forms a sheaf of sets.) For which presheaves, $\mathcal{F}$, is $\mathfrak{A}_\mathcal{F}$ a sheaf?

Problem 70 Consider $\mathcal{P}(X)$ and $\mathcal{S}(X)$ the categories of presheaves and sheaves of sets on X (our results will also work for other image categories based on sets, e.g., $\mathcal{A}$b, RNG, TOP, etc.) We have the definition of a sheaf so that

$$F(U) \xrightarrow{\theta} \prod_{\alpha} F(U_\alpha) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\beta,\gamma} F(U_\beta \cap U_\gamma) \tag{S}$$

is exact for all open covers, $\{U_\alpha \longrightarrow U\}_\alpha$ of any open U.

(1) There are two parts to the exactness of (S): θ is injective and the image of θ is the equalizer of p_1 and p_2. Write that F satisfies (+) if θ is injective. Suppose that F is any presheaf, define

$$F^{(+)} = \varinjlim_{\{U_\alpha \longrightarrow U\}} \operatorname{Ker}\left(\prod_{\alpha} F(U_\alpha) \rightrightarrows \prod_{\beta,\gamma} F(U_\beta \cap U_\gamma)\right)$$

(the limit taken over all open covers, $\{U_\alpha \longrightarrow U\}$, of the open U). Show that $F^{(+)}$ satisfies (+).

(2) If $0 \longrightarrow F' \xrightarrow{\varphi} F$ is exact in $\mathcal{P}(X, \mathcal{A}\text{b})$, set $(\operatorname{Cok}\varphi)(U) = \operatorname{Coker}\varphi(U) = \operatorname{Coker}(F'(U) \longrightarrow F(U))$. Prove that $\operatorname{Cok}\varphi$ satisfies (+).

(3) Suppose that F satisfies (+) show that $F^{(+)}$ satisfies (S), i.e., $F^{(+)}$ is a sheaf. Show further that, if F satisfies (+), then $\operatorname{Ker}(F(U) \longrightarrow F^{(+)}(U)) = (0)$, i.e., $F \longrightarrow F^{(+)}$ is an injective map of presheaves. Set $F^{\#} = (F^{(+)})^{(+)}$, for any presheaf F.

(4) We know $\#$ is exact and $i\colon \mathcal{S}(X) \to \mathcal{P}(X)$ is left-exact. Prove that $\#$ is the left adjoint of i, that is

$$\operatorname{Hom}_{\mathcal{S}(X)}(F^{\#}, G) \cong \operatorname{Hom}_{\mathcal{P}(X)}(F, i(G)).$$

(5) For the derived functor $\mathcal{H}^q(F)$ $(= (R^q i)(F))$ of $i\colon \mathcal{S}(X, \mathcal{A}\text{b}) \rightsquigarrow \mathcal{P}(X, \mathcal{A}\text{b})$, prove that

$$(\mathcal{H}^q(F))^{\#} = (0).$$

Problem 71 (Grothendieck) In Problem 69, you proved the collection $\{\mathfrak{Z}_U \mid U \text{ open in } X\}$ is a set of generators for
$\mathcal{P}(X, \mathcal{A}\text{b})$.

(1) Show that the collection $\{\mathfrak{Z}_U\}$ has the following property:

(G): For each presheaf, F, and for each monomorphism $0 \longrightarrow F' \longrightarrow F$ (in $\mathcal{P}(X, \mathcal{A}\text{b})$) with $F' \neq F$, there is an open $U \subseteq X$ and a morphism $\mathfrak{Z}_U \xrightarrow{\varphi} F$, so that φ does not factor through a morphism $\mathfrak{Z}_U \longrightarrow F'$.

Prove moreover that property (G) is equivalent to the fact that $\{\mathfrak{Z}_U \mid U \text{ open in } X\}$ is a family of generators for $\mathcal{P}(X, \mathcal{A}\text{b})$.

(2) Write $\underline{\mathbb{Z}}$ for the coproduct $\coprod_{\text{all } U} \mathfrak{Z}_U$ in $\mathcal{P}(X, \mathcal{A}\text{b})$, then $\underline{\mathbb{Z}}$ is a generator for $\mathcal{P}(X, \mathcal{A}\text{b})$. Show that a presheaf, Q, on X is injective if and only if for each monomorphism $0 \longrightarrow W \longrightarrow \underline{\mathbb{Z}}$, every morphism $\theta\colon W \to Q$ extends to a morphism $\underline{\mathbb{Z}} \longrightarrow Q$.

(3) Imitate the construction for rings R, ideals $\mathfrak{A} \subseteq R$ and R-modules M, of an injective hull for M (with the correspondence $R \longleftrightarrow \underline{\mathbb{Z}}$; $\mathfrak{A} \longleftrightarrow W$; $M \longleftrightarrow$ a presheaf F) to show:

There exists a functor $Q\colon F \rightsquigarrow Q(F)$ and a morphism of functors $\psi\colon \mathrm{id} \to Q$ so that

(a) $(\forall F \in \mathcal{P}(X, \mathcal{A}\text{b}))(\psi_F\colon F \to Q(F) \quad \text{is a monomorphism})$

and

(b) Each $Q(F)$ is an injective presheaf.

This gives the proof that $\mathcal{P}(X, \mathcal{A}\mathrm{b})$ has enough injective objects.

(4) The $\mathbb{Z}_U$ in $\mathcal{S}(X, \mathcal{A}\mathrm{b})$ defined as $\mathfrak{Z}_U^{\#}$ form a set of generators for $\mathcal{S}(X, \mathcal{A}\mathrm{b})$. The same argument as in (3) goes through and we obtain another proof (but similar to the text's proof) that $\mathcal{S}(X, \mathcal{A}\mathrm{b})$ has enough injectives.

Problem 72 (Grothendieck) Let $\mathcal{P}$ stand for the category of abelian presheaves, $\mathcal{P}(X, \mathcal{A}\mathrm{b})$, on the space X.

(1) If U is an open in X and $\{U_\alpha \longrightarrow U\}_\alpha$ is an open covering of U, we have induced a diagram of families of maps

$$U \longleftarrow \{U_\alpha\} \;\; \begin{array}{c}\longleftarrow\\ \longleftarrow\end{array} \;\; \{U_\beta \cap U_\gamma\}_{\beta,\gamma} \;\; \begin{array}{c}\longleftarrow\\ \longleftarrow\\ \longleftarrow\end{array} \;\; \{U_\delta \cap U_\epsilon \cap U_\eta\}_{\delta,\epsilon,\eta} \;\; \begin{array}{c}\longleftarrow\\ \longleftarrow\\ \longleftarrow\\ \longleftarrow\end{array} \;\; \cdots$$

coming from the various projections (note that $U_\beta \cap U_\gamma = U_\beta \prod U_\gamma$; $U_\delta \cap U_\epsilon \cap U_\eta = U_\delta \prod U_\epsilon \prod U_\eta$; *etc.*). When F is a presheaf, we get a *simplicial diagram*

$$F(U) \longrightarrow \prod_\alpha F(U_\alpha) \;\; \begin{array}{c}\longrightarrow\\ \longrightarrow\end{array} \;\; \prod_{\beta,\gamma} F(U_\beta \cap U_\gamma) \;\; \begin{array}{c}\longrightarrow\\ \longrightarrow\\ \longrightarrow\end{array} \;\; \prod_{\delta,\epsilon,\eta} F(U_\delta \cap U_\epsilon \cap U_\eta) \;\; \begin{array}{c}\longrightarrow\\ \longrightarrow\\ \longrightarrow\\ \longrightarrow\end{array} \;\; \cdots$$

and, by taking the alternating sum of these maps, we make a sequence

$$F(U) \longrightarrow \prod_\alpha F(U_\alpha) \xrightarrow{\delta^0} \prod_{\beta,\gamma} F(U_\beta \cap U_\gamma) \xrightarrow{\delta^1} \prod_{\delta,\epsilon,\eta} F(U_\delta \cap U_\epsilon \cap U_\eta) \xrightarrow{\delta^2} \cdots . \tag{$*$}$$

For notation, write $C^r(\{U_\alpha \longrightarrow U\}, F) = \prod_{\alpha_0,\ldots,\alpha_r} F(U_{\alpha_0} \cap \cdots \cap U_{\alpha_r})$, so that $(*)$ becomes

$$F(U) \longrightarrow C^0(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^0} C^1(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^1} C^2(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^2} \cdots . \tag{$**$}$$

Show that $(**)$ is an augmented complex (of abelian groups). We'll call $(**)$ the *explicit Čech cochain complex of the cover* $\{U_\alpha \longrightarrow U\}$ *with coefficients in* F. Denote by $H^q_{\mathrm{xpl}}(\{U_\alpha \longrightarrow U\}, F)$ its q^{th} cohomology group ($= \mathrm{Ker}\ \delta^q / \mathrm{Im}\ \delta^{q-1}$).

(2) We know that $\mathrm{Hom}_{\mathcal{P}}(\mathfrak{Z}_V, F) = F(V)$ for all open V of X, show that

$$\mathfrak{Z}_V = \coprod_{\mathrm{Hom}(U,V)} \mathbb{Z}.$$

(3) Now let F be an injective presheaf from $\mathcal{P}$, show that

$$C^0(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^0} C^1(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^1} C^2(\{U_\alpha \longrightarrow U\}, F) \xrightarrow{\delta^2} \cdots \tag{$***$}$$

is an *exact* sequence. (Suggestions. Show that the exactness of $(***)$ is equivalent to the exactness of

$$\coprod_\alpha \mathfrak{Z}_{U_\alpha} \longleftarrow \coprod_{\beta,\gamma} \mathfrak{Z}_{U_\beta \cap U_\gamma} \longleftarrow \coprod_{\delta,\epsilon,\eta} \mathfrak{Z}_{U_\delta \cap U_\epsilon \cap U_\eta} \longleftarrow \cdots \tag{$\dagger$}$$

in the category $\mathcal{P}$ and check the latter exactness by evaluation on any open Y of X. For this, show that the last sequence is induced by the simplicial diagram of indexing sets

$$\coprod_\alpha \mathrm{Hom}(Y, U_\alpha) \;\; \begin{array}{c}\longleftarrow\\ \longleftarrow\end{array} \;\; \coprod_{\beta,\gamma} \mathrm{Hom}(Y, U_\beta \cap U_\gamma) \;\; \begin{array}{c}\longleftarrow\\ \longleftarrow\\ \longleftarrow\end{array} \;\; \coprod_{\delta,\epsilon,\eta} \mathrm{Hom}(Y, U_\delta \cap U_\epsilon \cap U_\eta) \;\; \begin{array}{c}\longleftarrow\\ \longleftarrow\\ \longleftarrow\\ \longleftarrow\end{array} \;\; \cdots$$

and we can identify $\coprod_{\beta,\gamma} \mathrm{Hom}(Y, U_\beta \cap U_\gamma)$ with $M \coprod M$, where $M = \coprod_\alpha \mathrm{Hom}(Y, U_\alpha)$, *etc.* Thus, that (†) is exact comes down to the exactness of the diagram

$$\coprod_M \mathbb{Z} \;\leftleftarrows\; \coprod_{M \coprod M} \mathbb{Z} \;\substack{\leftarrow\\ \leftarrow\\ \leftarrow}\; \coprod_{M \coprod M \coprod M} \mathbb{Z} \;\substack{\leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow}\; \cdots .$$

But, construct a contracting homotopy for this last diagram and so complete proving (⁎⁎⁎) is exact.)

(4) Prove that the δ-functor $F \rightsquigarrow H^\bullet_{\mathrm{xpl}}(\{U_\alpha \longrightarrow U\}, F)$ is universal and show that we have an isomorphism

$$H^\bullet(\{U_\alpha \longrightarrow U\}, F) \cong H^\bullet_{\mathrm{xpl}}(\{U_\alpha \longrightarrow U\}, F)$$

(functorial in F). Thus, the complex (⁎⁎⁎) gives an explicit method for computing the cohomology groups, $H^\bullet(\{U_\alpha \longrightarrow U\}, -)$, of the covering $\{U_\alpha \longrightarrow U\}_\alpha$.

(5) Pass to the limit over all coverings of X and give an explicit complex to compute the Čech cohomology groups $\check{H}^\bullet(X, -)$.

Problem 73 If F is a sheaf of abelian groups on the space X, let's agree to write F again when we consider F as a presheaf.

(1) Show that there is an exact sequence

$$0 \longrightarrow \check{H}^2(X, F) \longrightarrow H^2(X, F) \longrightarrow \check{H}^1(X, \mathcal{H}^1(F))$$

and that if $\check{H}^3(X, F) = (0)$, then

$$0 \longrightarrow \check{H}^2(X, F) \longrightarrow H^2(X, F) \longrightarrow \check{H}^1(X, \mathcal{H}^1(F)) \longrightarrow 0$$

is exact.

(2) Let $\{U_\alpha \longrightarrow X\}_\alpha$ be an open cover of X and assume that

$$(\forall \alpha, \beta)(H^1(U_\alpha \cap U_\beta, F) = (0)).$$

Deduce that the natural map

$$\check{H}^2(X, F) \longrightarrow H^2(X, F)$$

is an isomorphism. If you assume only that

$$(\forall \alpha)(H^1(U_\alpha, F) = (0))$$

can you still deduce that $\check{H}^2(X, F) \cong H^2(X, F)$? Proof or counter-example.

(3) Can you continue the line of argument of (2) applied to groups such as $H^?(U_\alpha \cap U_\beta \cap U_\gamma, F)$, *etc.* and deduce further isomorphisms between Čech and derived functor cohomology? For example, try $\check{H}^3(X, F) \cong H^3(X, F)$.

(4) In a similar vein to (2) and (3) above, prove the following (known as Cartan's Isomorphism Theorem):

For the space X, let $\mathcal{U}$ be a family of open sets covering X so that

(a) If $U, V \in \mathcal{U}$, then $U \cap V \in \mathcal{U}$

(b) $\mathcal{U}$ contains arbitrarily small opens of X

(c) If $U \in \mathcal{U}$ and $q > 0$, then $\check{H}^q(U, F) = (0)$.

Then, the natural maps

$$\check{H}^q(X, F) \longrightarrow H^q(X, F)$$

are isomorphisms for all $q \geq 0$.

(Suggestions: Use induction on q, but replace X by any of the U of $\mathcal{U}$. Use a spectral sequence at the induction step to get $\check{H}^q(X,F) \cong H^q(X,F)$. Now how do you further deduce $\check{H}^q(U,F) \cong H^q(U,F)$ all $U \in \mathcal{U}$ to complete the induction?)

Remark: Two main uses of Cartan's Theorem are when X is a manifold and $\mathcal{U}$ is the family of all finite intersections of all sufficiently small open balls around each point of X and when X is an algebraic variety (over a field) and $\mathcal{U}$ is the collection of its affine open subvarieties.

Problem 74 Let k be a field, X an indeterminate (or transcendental) over k. Write $A = k[X]$ and consider an ideal, $\mathfrak{a}$, of A. The ideal, $\mathfrak{a}$, determines a topology on $k[X]$—called the $\mathfrak{a}$-*adic topology*—defined by taking as a fundamental system of neighborhoods of 0 the powers $\{\mathfrak{a}^n \mid n \geq 0\}$ of $\mathfrak{a}$. Then a fundamental system of neighborhoods at $\xi \in A$ is just the collection $\{\xi + \mathfrak{a}^n \mid n \geq 0\}$.

1. Show A becomes a topological ring (i.e. addition and multiplication are continuous) in this topology. When is A Hausdorff in this topology?

2. The rings $A/\mathfrak{a}^n = A_n$ form a left mapping system. Write

$$\widehat{A} = \varprojlim_n A/\mathfrak{a}^n$$

and call $\widehat{A}$ the $\mathfrak{a}$-*adic completion of* A. There is a map $A \to \widehat{A}$; when is it injective?

3. Consider $\mathfrak{a} = (X) =$ all polynomials with no constant term. The ring $\widehat{A}$ in this case has special notation: $k[[X]]$. Establish an isomorphism of $k[[X]]$ with the *ring of formal power series over* k (in X) i.e. with the ring consisting of sequences $\big(c_n\big)$, $n \geq 0$, $c_n \in k$ with addition and multiplication defined by:

$$\big(c_n\big) + \big(d_n\big) = \big(c_n + d_n\big)$$
$$\big(c_n\big) \cdot \big(d_n\big) = \big(e_n\big), \quad e_n = \sum_{i+j=n} c_i d_j$$

$\Big(\big(c_n\big) \leftrightarrow \sum_{n=0}^{\infty} c_n X^n$ explains the name$\Big)$.

4. Show $k[X] \hookrightarrow k[[X]]$, that $k[[X]]$ is an integral domain and a local ring. What is its maximal ideal? Now $(X) = \mathfrak{a}$ is a prime ideal of $k[X]$, so we can form $k[X]_{(X)}$. Prove that

$$k[X] \subseteq k[X]_{(X)} \subseteq k[[X]].$$

We have the (prime) ideal $(X)^e$ of $k[X]_{(X)}$. Form the completion of $k[X]_{(X)}$ with respect to the $(X)^e$-adic topology. What ring do you get?

Problem 75 If k is any field, write $A = k[[T_1, \ldots, T_n]]$ for the ring of formal power series over k in the indeterminates $T_1, \ldots, T_n$. Denote by $\mathrm{Aut}_k(A)$ the group of all k-automorphisms of A.

(1) Give necessary and sufficient conditions on the n power series $S_1(T_1, \ldots, T_n), \ldots, S_n(T_1, \ldots, T_n)$ in order that the map

$$\sigma \colon T_j \mapsto S_j(T_1, \ldots, T_n)$$

be an element of $\mathrm{Aut}_k(A)$. In so doing, describe the group $\mathrm{Aut}_k(A)$.

(2) If now k is no longer necessarily a field but merely a commutative ring with unity, answer question (1) for this case.

(3) Fix k, a commutative ring with unity, and consider the category, $\mathrm{Alg}(k)$, of k-algebras (say commutative). Define a functor $Aut(k[[T_1, \ldots, T_n]]/k)(-)$ by sending $B \in \mathrm{Alg}(k)$ to $\mathrm{Aut}_B(B[[T_1, \ldots, T_n]]) \in \mathrm{Grp}$. Is this functor representable? How?

Problem 76 Prove that in the category of commutative A-algebras, the tensor product is the coproduct:

$$B \otimes_A C \cong B \coprod_A C.$$

Which A-algebra is the product $B \prod_A C$ (in commutative A-algebras)?

Problem 77 Suppose A is a (commutative) semi-local ring obtained by localizing a f.g. $\mathbb{C}$-algebra with respect to a suitable multiplicative subset. Let J be the Jacobson radical of A and write $\widehat{A}$ for the J-adic completion of A. Is it true that every finitely generated $\widehat{A}$-module, M, has the form $M = M_0 \otimes_A \widehat{A}$ for some finitely generated A-module, M_0? Proof or counter-example.

Problem 78 Here A is a commutative ring and we write $M_n(A)$ for the ring of $n \times n$ matrices over A.

1. Prove: The following are equivalent
   (a) A is noetherian
   (b) For some n, $M_n(A)$ has the ACC on 2-sided ideals
   (c) For all n, $M_n(A)$ has the ACC on 2-sided ideals.
2. Is this still valid if "noetherian" is replaced by "artinian" and "ACC" by "DCC"? Proof or counterexample.
3. Can you make this quantitative? For example, suppose all ideals of A are generated by less than or equal to N elements. What can you say about an upper bound for the number of generators of the ideals of $M_n(A)$? How about the converse?

Problem 79 Refer to Problem 74. Write $k((X))$ for $\mathrm{Frac}(k[[X]])$.

1. Show that
$$k((X)) = \left\{ \sum_{j=-\infty}^{\infty} a_j X^j \mid a_j \in k \text{ and } (\exists\, N)(a_j = 0 \text{ if } j < N) \right\}$$
where on the right hand side we use the obvious addition and multiplication for such expressions. If $\xi \in k((X))$, write $\mathrm{ord}(\xi) = N \iff N =$ largest integer so that $a = 0$ when $j < N$; here, $\xi \neq 0$. If $\xi = 0$, set $\mathrm{ord}(\xi) = \infty$. One sees immediately that $k[[X]] = \big\{\xi \in k((X)) \mid \mathrm{ord}(\xi) \geq 0\big\}$.
2. Write $\mathcal{U}$ for $\mathbb{G}_m\big(k[[X]]\big)$ and $\mathcal{M}$ for $\{\xi \mid \mathrm{ord}(\xi) > 0\}$. Prove that $k((X)) = \mathcal{M}^{-1} \cup \mathcal{U} \cup \mathcal{M}$ (disjointly), where
$$\mathcal{M}^{-1} = \{\xi \mid 1/\xi \in \mathcal{M}\}.$$
Now fix a real number, c, with $0 < c < 1$. Define for $\xi, \eta \in k((X))$,
$$d(\xi, \eta) = c^{\mathrm{ord}(\xi - \eta)},$$
then it should be clear that $k((X))$ becomes a metric space and that addition and multiplication are continuous in the metric topology. Prove that $k((X))$ is complete in this topology (i.e., Cauchy sequences converge), and that the topology is independent of which number c is chosen (with $0 < c < 1$).
3. Suppose $u \in k[[X]]$, $u = \sum_{j=0}^{\infty} a_j X^j$, and $a_0 = 1$. Pick an integer $n \in \mathbb{Z}$ and assume $(n, \mathrm{char}(k)) = 1$. Prove: There exists $w \in k[[X]]$ such that $w^n = u$. There is a condition on k so that $k((X))$ is locally compact. What is it? Give the proof. As an example of limiting operations, prove
$$\frac{1}{1-x} = \sum_{j=0}^{\infty} X^j = \lim_{N \to \infty} (1 + X + \cdots + X^N).$$

4. Given $\sum_{j=-\infty}^{\infty} a_j X^j \in k((X))$, its derivative is defined formally as

$$\sum_{j=-\infty}^{\infty} j a_j X^{j-1} \in k((X)).$$

Assume $\mathrm{ch}(k) = 0$. Check mentally that $\alpha' = 0$ $\big(\alpha \in k((X))\big) \implies \alpha \in k$. Is the map $\alpha \mapsto \alpha'$ a *continuous* linear transformation $k((X)) \to k((X))$? Set $\eta = \sum_{j=0}^{\infty} \frac{1}{j!} X^j$, so $\eta \in k((X))$. Prove that X and η are independent transcendentals over k.

5. Assume $\mathrm{ch}(k) = 0$. A topological ring is one where addition and multiplication are continuous and we have a Hausdorff topology. Topological k-algebras (k has the discrete topology) form a category in which the morphisms are *continuous* k-algebra homomorphisms. An element λ in such a ring is *topologically nilpotent* iff $\lim_{n\to\infty} \lambda^n = 0$. Let $\mathcal{N}_{\mathrm{top}}$ denote the functor which associates to each topological k-algebra the set of its topological nilpotent elements. Prove that $\mathcal{N}_{\mathrm{top}}$ is representable. As an application, let

$$s(X) = \sum_{j=0}^{\infty} (-1)^j \frac{X^{2j+1}}{(2j+1)!}, \quad c(X) = \sum_{j=0}^{\infty} (-1)^j \frac{X^{2j}}{(2j)!}.$$

Then $s'(X) = c(X)$ and $c'(X) = -s(X)$, so $c^2(X) + s^2(X)$ lies in k (the constants). Without computing $c^2(X) + s^2(X)$, show it is 1. (You'll need $\mathcal{N}_{\mathrm{top}}$, so be careful.)

6. Show that even though $k(X)$ is dense in $k((X))$, the field $k((X))$ possesses infinitely many algebraically independent transcendental elements over $k(X)$. (Suggestion: Look in a number theory book under "Liouville Numbers"; mimic what you find there.)

7. Assume $\mathrm{ch}(k) = 0$. Let $C_k\big(k((X))\big) = \big\{\alpha \in k((X)) \mid \alpha \text{ is algebraic over } k\big\}$. Show that $C_k\big(k((X))\big) = k$.
If $\mathbb{R} \subseteq k$, write $\binom{m}{j} = \dfrac{m(m-1)\cdots(m-j+1)}{j(j-1)\cdots 3\cdot 2\cdot 1}$ for $m \in \mathbb{R}$. If $\mathbb{R} \not\subseteq k$, do this only for $m \in \mathbb{Q}$. Set

$$y_m = \sum_{j=0}^{\infty} \binom{m}{j} X^j \in k[[X]].$$

If $m \in \mathbb{Q}$ and $m = r/s$, prove that $y_m^s = (1+x)^r$.
Note that $y_m = 1 + O(X)$ and that $O(X) \in \mathcal{N}_{\mathrm{top}}\big(k[[X]]\big)$. Let $L(1+X) = \sum_{j=0}^{\infty} (-1)^j \frac{X^{j+1}}{(j+1)}$, and set $f(X)^m = \eta\big(m \cdot L(f(X))\big)$, where

$$\eta(X) = \sum_{j=0}^{\infty} \frac{1}{j!} X^j \quad \text{and} \quad f(X) = 1 + O(X), \text{ some } O(X)$$

and $m \in \mathbb{R}$ (here, $\mathbb{R} \subseteq k$). Show that

$$(1+X)^m = y_m.$$

Problem 80 Say K is a field, A is a subring of K. Write $k = \mathrm{Frac}\, A$.

1. If K is a finitely generated A-module, prove that $k = A$.

2. Suppose there exist finitely many elements $\alpha_1, \ldots, \alpha_m \in K$ *algebraic over* k such that

$$K = A[\alpha_1, \ldots, \alpha_m].$$

Prove $\big(\exists\, b \in A\big)\big(b \neq 0\big)\big(\text{so that } k = A[1/b]\big)$. Prove, moreover, that b belongs to every maximal ideal of A.

Problem 81 Refer to Problem 69. Look at $\mathcal{P}(X, \mathcal{A}\mathrm{b})$. We know that the functor $F \rightsquigarrow F(U)$ taking $\mathcal{P}(X, \mathcal{A}\mathrm{b})$ to $\mathcal{A}\mathrm{b}$ is representable.

1. Grothendieck realized that when computing algebraic invariants of a "space" (say homology, cohomology, homotopy, K-groups, ...) the sheaf theory one needs to use could be done far more generally and with far more richness if one abstracted the notion of "topology". Here is the generalization:

   (a) Replace $\mathcal{T}_X$ by *any* category $\mathcal{T}$.

   To do sheaves, we need a notion of "covering":

   (b) We isolate for each $U \in \mathcal{O}\mathrm{b}\,\mathcal{T}$ some families of morphisms $\{U_\alpha \to U\}_\alpha$ and call each of these a "covering" of U. So we get a whole collection of families of morphisms called $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ *and we require*

   (i) Any isomorphism $\{V \to U\}$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$

   (ii) If $\{U_\alpha \to U\}_\alpha$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ and for all α, $\{V_\beta^{(\alpha)} \to U_\alpha\}_\beta$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$, then $\Big\{V_\beta^{(\alpha)} \to U\Big\}_{\alpha,\beta}$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ (*i.e.*, a covering of a covering is a covering).

   (iii) If $\{U_\alpha \to U\}_\alpha$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ and $V \to U$ is *arbitrary* then $U_\alpha \underset{U}{\coprod} V$ exists in $\mathcal{T}$ *and*

$$\Big\{U_\alpha \underset{U}{\coprod} V \to V\Big\}_\alpha$$

   is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ (*i.e.*, the restriction of a covering to V is a covering of V; this allows the relative topology—it is the axiom with teeth).

Intuition: A morphism $V \to U$ in $\mathcal{T}$ is an "open subset of U". N.B. The same V and U can give more than one "open subset" (vary the morphism) so the theory is very rich. In our original example: $\mathcal{T} = \mathcal{T}_X$; the family $\{U_\alpha \to U\}_\alpha$ is in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ when and only when $\bigcup_\alpha U_\alpha = U$. Check the axioms (i), (ii) and (iii).
Now a presheaf is just a cofunctor $\mathcal{T} \to \mathcal{S}\mathrm{ets}$ or $\mathcal{A}\mathrm{b}$, etc. and a sheaf is a presheaf for which

$$F(U) \to \prod_\gamma F\big(U_\gamma\big) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \prod_{\alpha,\beta} F\Big(U_\alpha \underset{U}{\coprod} U_\beta\Big) \tag{S}$$

is exact for *every* $U \in \mathcal{T}$ and *every* $\{U_\gamma \to U\}_\gamma$ in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$. One calls the category $\mathcal{T}$ and its distinguished families $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ a *site* (topology used to be called "analysis situs").

Given a category, say $\mathcal{T}$, assume $\mathcal{T}$ has finite fibred products. A family of morphisms $\{U_\alpha \to U\}_\alpha$ in $\mathcal{T}$ is called a family of *universal, effective epimorphisms* iff

(a) $\forall Z \in \mathcal{O}\mathrm{b}\,\mathcal{T}$

$$\mathrm{Hom}(U, Z) \to \prod_\gamma \mathrm{Hom}\big(U_\gamma, Z\big) \rightrightarrows \prod_{\alpha,\beta} \mathrm{Hom}\big(U_\alpha \underset{U}{\coprod} U_\beta, Z\big)$$

is exact (in $\mathcal{S}\mathrm{ets}$) AND

(b) The same for $\Big\{U_\alpha \underset{U}{\coprod} V \to V\Big\}_\alpha$ *vis a vis* all Z as in (a). (Condition (b) expresses universality, and (a) expresses effectivity of epimorphisms.)

Decree that $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ is to consist of families of universal, effective epimorphisms. Show that $\mathcal{T}$ with this $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ is a site—it is called the *canonical site on* $\mathcal{T}$, denoted $\mathcal{T}_{\mathrm{can}}$.

2. For $\mathcal{T}_{\mathrm{can}}$, every representable cofunctor on $\mathcal{T}$ is a sheaf (give the *easy* proof). Note that if $\mathcal{T} \subseteq \widetilde{\mathcal{T}}$ where $\widetilde{\mathcal{T}}$ is a bigger category, and if $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ lies in the universal, effective epimorphisms for $\widetilde{\mathcal{T}}$, then any cofunctor on $\mathcal{T}$, *representable in* $\widetilde{\mathcal{T}}$, is a sheaf on $\mathcal{T}_{\mathrm{can}}$. For example, prove that if $\widetilde{\mathcal{T}}$ is all topological spaces and $\mathcal{T}_X$ is our beginning category of Problem 69, then $\mathcal{T}_X \subseteq \widetilde{\mathcal{T}}$ and prove that open coverings in $\mathcal{T}_X$ (as in Problem 69) *are* universal, effective epimorphisms in $\widetilde{\mathcal{T}}$. Hence, for ANY topological space, Y, $U \rightsquigarrow \mathrm{Hom}_{\mathrm{top.spaces}}(U, Y)$ *is a sheaf* on $\mathcal{T}_X$.

3. Let $\mathcal{T} = \mathcal{S}\mathrm{ets}$ and let $\{U_\alpha \to U\}_\alpha$ be in $\mathcal{C}\mathrm{ov}\,\mathcal{T}$ when $\bigcup_\alpha(\text{Images of } U_\alpha) = U$. Prove that the sheaves on $\mathcal{T}$ with values in $\mathcal{S}\mathrm{ets}$ are exactly the representable cofunctors on $\mathcal{T}$.

4. Generalize (3): If G is a given group, let $\mathcal{T}_G$ be the category of sets with a G-action. Make $(\mathcal{T}_G)_{\mathrm{can}}$ the canonical site on $\mathcal{T}_G$. Prove: Coverings are families $\{U_\alpha \to U\}_\alpha$ so that $\bigcup_\alpha(\mathrm{Im}\, U_\alpha) = U$ (all are G-sets, morphisms are G-morphisms). Once again, prove: The sheaves on $(\mathcal{T}_G)_{\mathrm{can}}$ are exactly the representable cofunctors on $\mathcal{T}_G$. Prove further: The sheaves on $(\mathcal{T}_G)_{\mathrm{can}}$ with values in $\mathcal{A}\mathrm{b}$ form a category equivalent to the category of G-modules; namely the equivalence is given by taking a sheaf to its representing object, a G-module.

Problem 82 Consider the two rings $A = \mathbb{R}[T]$ and $B = \mathbb{C}[T]$. Show that $\mathrm{Max}(B)$ is in one-to-one correspondence with the points of the complex plane while $\mathrm{Max}(A)$ is in one-to-one correspondence with the closed upper half plane: $\{\xi \in \mathbb{C} \mid \mathrm{Im}(\xi) \geq 0\}$. Since A is a PID (so is B) we can characterize an ideal by its generator. In these terms, which ideals of $\mathrm{Max}(A)$ correspond to points in $\mathrm{Im}(\xi) > 0$, which to points on the real line? What about $\mathrm{Spec}\, B$ and $\mathrm{Spec}\, A$?

Problem 83 Suppose that $f(X, Y)$ and $g(X, Y)$ are two irreducible polynomials with complex coefficients. Assume neither is a scalar multiple of the other. Show that the set

$$S = \{(\alpha, \beta) \in \mathbb{C}^2 \mid f(\alpha, \beta) = g(\alpha, \beta) = 0\}$$

is finite. (There are many ways of doing this; try to pick a way that is as elementary as possible.)

Problem 84 When X is compact Hausdorff and $A = \mathbb{C}(X)$, we identified X and $\mathrm{Max}(A)$ in the text *via* $x \mapsto \mathfrak{m}_x$. Now $\mathrm{Max}(A)$ has the induced topology from $\mathrm{Spec}\, A$.

1. Show the induced topology on $\mathrm{Max}(A)$ is compact Hausdorff by proving $x \mapsto \mathfrak{m}_x$ is a homeomorphism.

2. Prove all finitely generated ideals of A are principal but that no maximal ideal is finitely generated. Note that some extra condition on X is needed. For example, X should not be finite.

Problem 85

1. Given $A \to B$ a homomorphism prove that B is faithfully flat over A iff B is flat over A and the map $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ is surjective.

2. Say $A \to B$ is a homomorphism and B is faithfully flat over A. Assume A is noetherian. Show that the topology on $\mathrm{Spec}\, A$ is the quotient topology from $\mathrm{Spec}\, B$.

Problem 86 Here A is a commutative ring, but *not necessarily with unity.* Let $A^{\#}$ denote $A \prod \mathbb{Z}$ (category of sets) with addition componentwise and multiplication given by

$$\langle a, n\rangle\langle b, q\rangle = \langle ab + nb + qa, nq\rangle.$$

1. Clearly, $A^{\#}$ is a commutative ring with unity $\langle 0, 1\rangle$. A is a subring of $A^{\#}$, even an ideal. Suppose A has the ACC on ideals, prove that $A^{\#}$ does, too. Can you make this quantitative as in Problem 78 part (3)?

2. If you know all the prime ideals of A, can you find all the prime ideals of $A^{\#}$?

Problem 87 Let B, C be commutative A-algebras, where A is also commutative. Write D for the A-algebra $B \otimes_A C$.

1. Give an example to show that $\operatorname{Spec} D$ is not $\operatorname{Spec} B \underset{\operatorname{Spec} A}{\times} \operatorname{Spec} C$ (category of sets over $\operatorname{Spec} A$).

2. We have A-algebra maps $B \to D$ and $C \to D$ and so we get maps $\operatorname{Spec} D \to \operatorname{Spec} B$ and $\operatorname{Spec} D \to \operatorname{Spec} C$ (even maps over $\operatorname{Spec} A$), and these are maps of topological spaces (over $\operatorname{Spec} A$). Hence, we do get a map

$$\theta : \operatorname{Spec} D \to \operatorname{Spec} B \underset{\operatorname{Spec} A}{\amalg} \operatorname{Spec} C \quad \text{(top. spaces)}.$$

Show there are closed sets in $\operatorname{Spec} D$ *not* of the form $\theta^{-1}(Q)$, where Q is a closed set in the product topology of $\operatorname{Spec} B \underset{\operatorname{Spec} A}{\amalg} \operatorname{Spec} C$.

Problem 88 Let $A = \mathbb{Z}[T]$, we are interested in $\operatorname{Spec} A$.

1. If $\mathfrak{p} \in \operatorname{Spec} A$, prove that $\operatorname{ht}(\mathfrak{p}) \leq 2$.

2. If $\{\mathfrak{p}\}$ is closed in $\operatorname{Spec} A$, show that $\operatorname{ht}(\mathfrak{p}) = 2$. Is the converse true?

3. We have the map $\mathbb{Z} \hookrightarrow \mathbb{Z}[T] = A$, hence the continuous map $\operatorname{Spec} A \xrightarrow{\pi} \operatorname{Spec} \mathbb{Z}$. Pick a prime number, say p, of $\mathbb{Z}$. Describe $\pi^{-1}(p)$, is it closed?

4. When exactly is a $\mathfrak{p} \in \operatorname{Spec} A$ the generic point (point whose closure is everything) of $\pi^{-1}(p)$ for some prime number p?

5. Describe exactly those $\mathfrak{p} \in \operatorname{Spec} A$ whose image, $\pi(\mathfrak{p})$, is dense in $\operatorname{Spec} \mathbb{Z}$. What is $\operatorname{ht}(\mathfrak{p})$ in these cases?

6. Is there a $\mathfrak{p} \in \operatorname{Spec} A$ so that the closure of $\{\mathfrak{p}\}$ is all of $\operatorname{Spec} A$? What is $\operatorname{ht}(\mathfrak{p})$?

7. For a general commutative ring, B, if $\mathfrak{p}$ and $\mathfrak{q}$ are elements of $\operatorname{Spec} B$ and if $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$ show that $\operatorname{ht}(\mathfrak{q}) \geq \operatorname{ht}(\mathfrak{p})$ (assuming finite height). If $\mathfrak{p}$, $\mathfrak{q}$ are as just given and $\operatorname{ht}(\mathfrak{q}) = \operatorname{ht}(\mathfrak{p})$ is $\mathfrak{q}$ necessarily $\mathfrak{p}$? Prove that the following are equivalent:

   (a) $\operatorname{Spec} B$ is *irreducible* (that is, it is *not* the union of two properly contained closed subsets)

   (b) $(\exists\, \mathfrak{p} \in \operatorname{Spec} B)$(closure of $\{\mathfrak{p}\} = \operatorname{Spec} B$)

   (c) $(\exists$ *unique* $\mathfrak{p} \in \operatorname{Spec} B)$(closure of $\{\mathfrak{p}\} = \operatorname{Spec} B$)

   (d) $\mathcal{N}(B) \in \operatorname{Spec} B$. (Here, $\mathcal{N}(B)$ is the nilradical of B)

8. Draw a picture of $\operatorname{Spec} \mathbb{Z}[T]$ as a kind of plane over the "line" $\operatorname{Spec} \mathbb{Z}$ and exhibit in your picture all the different kinds of $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[T]$.

Problem 89 If A is a commutative ring, we can view $f \in A$ as a "function" on the topological space $\operatorname{Spec} A$ as follows: for each $\mathfrak{p}$ in $\operatorname{Spec} A$, as usual write $\kappa(\mathfrak{p})$ for $\operatorname{Frac}(A/\mathfrak{p})$ [note that $\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/\text{its max. ideal}$] and set $f(\mathfrak{p}) =$ image of f in $A/\mathfrak{p}$ considered in $\kappa(\mathfrak{p})$. Thus, $f : \operatorname{Spec} A \to \bigcup_{\mathfrak{p} \in \operatorname{Spec} A} \kappa(\mathfrak{p})$. Observe that if $f \in \mathcal{N}(A)$, then $f(\mathfrak{p}) = 0$ all $\mathfrak{p}$, *yet f need not be zero as an element of A.*

1. Let $A = k[X_1, \ldots, X_n]$. There are fields, Ω, containing k so that

   (a) Ω has infinitely many transcendental elements independent of each other and of the X_j over k and

(b) Ω is algebraically closed, i.e., all polynomials with coefficients in Ω have a root in Ω.

An example of this is when $k = \mathbb{Q}$ or some finite extension of $\mathbb{Q}$ and we take $\Omega = \mathbb{C}$. In any case, fix such an Ω. Establish a set-theoretic map $\Omega^n \to \operatorname{Spec} A$ so that $f \in A = k[X_1, \ldots, X_n]$ viewed in the usual way as a function on Ω^n agrees with f viewed as a function on $\operatorname{Spec} A$. We can topologize Ω^n as follows: Call a subset of Ω^n k-closed iff there are finitely many polynomials $f_1, \ldots, f_p$ from A so that the subset is exactly the set of common zeros of $f_1, \ldots, f_p$. This gives Ω^n the *k-topology* (an honest topology, as one checks). Show that your map $\Omega^n \to \operatorname{Spec} A$ is continuous between these topological spaces. Prove, further, that Ω^n maps *onto* $\operatorname{Spec} A$.

2. Show that Ω^n is irreducible in the k-topology. (Definition in 7(a) of Problem 88)

3. Define an equivalence relation on Ω^n: $\xi \sim \eta \iff$ each point lies in the closure (k-topological) of the other. Prove that $\Omega^n/\sim$ is homeomorphic to $\operatorname{Spec} A$ under your map.

Problem 90 (Continuation of Problem 89) Let A be an integral domain and write K for $\operatorname{Frac}(A)$. For each $\xi \in K$, we set

$$\operatorname{dom}(\xi) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \xi \text{ can be written } \xi = a/b, \text{ with } a, b \in A \text{ and } b(\mathfrak{p}) \neq 0\}.$$

1. Show $\operatorname{dom}(\xi)$ is open in $\operatorname{Spec} A$.

2. If $A = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$, set $\xi = (1 - y)/x$ (where $x = \overline{X}$ and $y = \overline{Y}$). What is $\operatorname{dom}(\xi)$?

3. Set $A = \mathbb{C}[X, Y]/(Y^2 - X^2 - X^3)$ and let $\xi = y/x$. What is $\operatorname{dom}(\xi)$?

4. Note that as ideals of A (any commutative ring) are A-modules, we can ask if they are free or locally free. Check that the non-zero ideal, $\mathfrak{a}$, of A is free $\iff$ it is principal and $\big(\mathfrak{a} \to (0)\big) = (0)$. The second condition is automatic in a domain. Now look again at $A = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$, you should see easily that this is a domain. Characterize as precisely as you can the elements $\mathfrak{m} \in \operatorname{Max}(A)$ which are free as A-modules. If there are other elements of $\operatorname{Max}(A)$, are these locally free? What is the complement of $\operatorname{Max}(A)$ in $\operatorname{Spec} A$? Prove that $A \otimes_{\mathbb{R}} \mathbb{C}$ is a PID.

5. Consider the descent question for PIDs: Given rings S and T with $S \to T$ a homomorphism, suppose A is an S-algebra and T is faithfully flat over S. If $A \otimes_S T$ is a PID, is A necessarily a PID?

6. Do part (5) where PID is replaced by UFD.

Problem 91 Let p be an odd prime number, set $m = 2p - 1$ and write $A = \mathbb{Z}[\sqrt{-m}] \cong \mathbb{Z}[T]/(T^2 + m)$. Assume m is square free.

1. Let $\mathfrak{a}$ be the ideal $(p, 1 + \sqrt{-m})$ of A. Prove that $\mathfrak{a}$ is not principal, yet that $\mathfrak{a}$, as a module, is locally free (necessarily of rank one). Prove further that A is *not* a UFD.

2. For $p = 3$ and 7, find all the ideals, $\mathfrak{a}$, which are not free, yet are locally free.

N.B. By results of the text you have non-free projectives here.

Problem 92 In this problem A is an integral domain and $K = \operatorname{Frac}(A)$.

1. Is it true that if $\mathfrak{p} \in \operatorname{Spec}\big(A[X]\big)$ and if $\mathfrak{p} \cap A = (0)$, then $\mathfrak{p}$ is a principal ideal? Proof or counterexample.

2. Say A is a UFD and $\eta \in K$, with $\eta \neq 0$. Write $\eta = a/b$, where a and b are relatively prime. Prove that $A[\eta] \cong A[X]/(bX - a)$. When is $A[\eta]$ a flat A-module?

3. If k is a field and $\xi \in k(X)$ is a non-constant rational function, write $\xi = f(X)/g(X)$ where f and g are relatively prime polynomials. Of course, $k(\xi)$ is a subfield of $k(X)$, so $k(X)$ is a $k(\xi)$ vector space (and a $k(\xi)$-algebra). Prove that $\dim_{k(\xi)}\big(k(X)\big) < \infty$ and compute this dimension in terms of f and g.

Problem 93 If A is a commutative ring and $B = A[[X_1, \ldots, X_n]]$ denotes the ring of formal power series in the variables $X_1, \ldots, X_n$ (the case $n = 1$ was discussed in Problem 79) over A:

1. Prove:
$$\begin{aligned} A \text{ is noetherian} &\iff B \text{ is noetherian} \\ A \text{ is an integral domain} &\iff B \text{ is an integral domain} \\ A \text{ is a local ring} &\iff B \text{ is a local ring.} \end{aligned}$$
2. Write $K((X_1, \ldots, X_n))$ for $\operatorname{Frac} B$, where $K = \operatorname{Frac} A$ and A is a domain. Say $A = K = \mathbb{C}$, $n = 2$. Is $\mathbb{C}((X, Y))$ equal to $\mathbb{C}((X))((Y))$? If not, does one contain the other; which?

Problem 94 If A is a noetherian ring, write $X = \operatorname{Spec} A$ with the Zariski topology. Prove the following are equivalent:

1. X is T_1
2. X is T_2
3. X is discrete
4. X is finite and T_1.

Problem 95 Call a commutative ring *semi-local* iff it possesses just finitely many maximal ideals.

1. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_t \in \operatorname{Spec} A$ and $S = A - \bigcup_{j=1}^{t} \mathfrak{p}_j$, then $S^{-1}A$ is semi-local.
2. Say A is semi-local and $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ are its maximal ideals. Show that the natural map of rings
$$A/\mathcal{J}(A) \to \prod_{i=1}^{t} A/\mathfrak{m}_i$$
is an isomorphism. (Here, $\mathcal{J}(A)$ is the Jacobson radical of A)
3. If A is semi-local, show $\operatorname{Pic}(A) = (0)$.

Problem 96 Let A be a domain. An element $a \in A$, not a unit, is called *irreducible* iff it is *not* the product $a = bc$ in which neither b nor c is a unit. The element a is a *prime* iff the principal ideal, Aa, is a prime ideal. Of course, prime $\implies$ irreducible.

1. Assume A is noetherian, show each non-unit of A is a finite product of irreducible elements. (A need not be a domain for this.)
2. Prove that the factorization of (1) is unique (when it exists) iff every irreducible element of A is prime.
3. Say A is a UFD and S a multiplicative subset of A. Show that $S^{-1}A$ is a UFD. If A is locally a UFD is A a UFD?
4. Prove: If A is noetherian then A is a PID $\iff$ A is a UFD *and* $\dim A = 1$.
5. Assume A is just a domain. A *weight function*, w, *on* A is a function $A - \{0\} \to \mathbb{Z}_{\geq 0}$ so that
   (a) $a \mid b \implies w(a) \leq w(b)$, with equality $\iff$ $b \mid a$, too
   (b) If a and $b \in A$ and say $a \nmid b$ and $b \nmid a$, then $\exists\, p, q, r \in A$ so that $r = pa + qb$ and $w(r) < \min\{w(a), w(b)\}$.

   Prove: A domain is a PID $\iff$ it possesses a weight function. Can you characterize the fields among the PIDs by their weight functions?

Problem 97 Prove: A noetherian domain is a UFD iff each height 1 prime is principal.

Problem 98 Examples and Counterexamples:

1. Let $A = k[X, Y]$ with k a field; write $\mathfrak{m} = (X, Y)$. Show that $\mathfrak{q} = (X, Y^2)$ is $\mathfrak{m}$-primary, but $\mathfrak{q}$ is *not* a power of any prime ideal of A. Therefore, primary ideals need not be powers of prime ideals.

2. Let $A = k[X, Y, Z]/(XY - Z^2) = k[x, y, z]$. Write $\mathfrak{p}$ for the ideal (x, z) of A. Prove that $\mathfrak{p} \in \operatorname{Spec} A$, but $\mathfrak{p}^2$ is not primary. Hence, powers of non-maximal prime ideals need not be primary. What is the primary decomposition of $\mathfrak{p}^2$?

3. Say $A = k[X, Y]$ as in part (1) and write $\mathfrak{a} = (X^2, XY)$. Show that $\mathfrak{a}$ is *not* primary yet $\sqrt{\mathfrak{a}}$ is a prime ideal—which one? So, here a non-primary ideal has a prime radical. What is the primary decomposition of $\mathfrak{a}$?

4. If A is a UFD and p is a prime element of A, then $\mathfrak{q} = Ap^n$ is always primary. Conversely, show if $\mathfrak{q}$ is primary and $\sqrt{\mathfrak{q}} = Ap$, then $(\exists\, n \geq 1)(\mathfrak{q} = Ap^n)$. Compare with (3) above.

Problem 99 Assume A is a noetherian integral domain. The argument at the end of Theorem 3.56 shows that height one primes of A are elements of $\operatorname{Pic}(A)$ *if A is normal*.

(1) Use this remark to prove that in a normal (noetherian) domain, each isolated prime of a principal ideal has height one (special case of Krull's principal ideal theorem).

(2) Say A is a noetherian normal domain. Show that A is a UFD iff $\operatorname{Pic}(A) = (0)$.

Problem 100 A Little Number Theory.
Let $\mathbb{Q}$ be the rational numbers, and consider fields $k = \mathbb{Q}[X]/\big(f(X)\big)$ where $f(X)$ is an irreducible polynomial over $\mathbb{Q}$. (Each finite extension of $\mathbb{Q}$ has this form, by Chapter 4, Section 4.6.) Such a k will be called a "number field" and we write $\mathcal{O}_k$ for $\operatorname{Int}_k(\mathbb{Z})$.

1. Show $\mathcal{O}_k$ is a noetherian normal domain with $\dim \mathcal{O}_k = 1$.

2. If $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_k$, then $(\mathcal{O}_k)_{\mathfrak{p}}$ is a PID and $\mathcal{O}_k$ is a UFD iff $\operatorname{Pic}(\mathcal{O}_k) = (0)$ iff $\mathcal{O}_k$ is a PID.

3. Let k be the fields: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\zeta)$, where ζ is a primitive 7th root of 1. In each case, find $\mathcal{O}_k$ and compute $\operatorname{Pic}(\mathcal{O}_k)$. Make a table.

4. In $\mathbb{Q}(\sqrt{-3})$, look at $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$. Is $\mathbb{Z}[\sqrt{-3}] = \mathcal{O}_k$? If not, what is $\operatorname{Pic}\big(\mathbb{Z}[\sqrt{-3}]\big)$? Same question for $\mathbb{Z}[\sqrt{-5}]$.

5. Let A be a noetherian, normal domain of dimension 1, write $k = \operatorname{Frac} A$ (e.g., $\mathcal{O}_k = A$ by (1)). We examine submodules (for A) of k. Call one of these, M, a *fractional ideal* iff $(\exists\, b \in A)(b \neq 0)(bM \subseteq A)$. Prove that the following are equivalent for A-submodules of k:

   (a) M is a fractional ideal

   (b) M is a finitely generated A-module

   (c) M is a rank one projective A-module.

6. Under multiplication, MN, the fractional ideals form a group, denote it $\mathcal{I}(A)$. (MN goes over to $M \otimes_A N$ in $\operatorname{Pic}(A)$). Let $\mathcal{C}_A$ be the (localizing) category of finite length modules over A and write $\widetilde{K}(A)$ for the Grothendieck group, $K_0(\mathcal{C}_A)$, of $\mathcal{C}_A$. By the theory of associated primes, each M in $\mathcal{C}_A$ has a composition series

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_{n+1} = (0)$$

   and

$$M_i/M_{i+1} \cong A/\mathfrak{p}_i \text{ for some } \mathfrak{p}_i \in \operatorname{Max}(A).$$

These $\mathfrak{p}_i$ are unique up to order and we set

$$\chi_A(M) = \prod_{i=0}^{n} \mathfrak{p}_i \in \mathcal{I}(A).$$

Prove that χ_A is an isomorphism (first prove homomorphism) of the abelian groups $\widetilde{K}(A) \xrightarrow{\sim} \mathcal{I}(A)$. What is the kernel of the map $\widetilde{K}(A) \to \mathrm{Pic}(A)$?

7. Lastly, assume A is actually a PID. Say $M = A^n$ is a free A-module of rank n and choose $u \in \mathrm{End}_A M$. Assume $\det(u) \neq 0$ and show
$$\det(u) \cdot A = \chi_A(\mathrm{coker}\, u).$$

Problem 101 More examples.

1. Let $A = k[X, Y, Z, W]/(XY - ZW)$, where k is a field and $\mathrm{char}(k) \neq 2$. By Problem 34; A is a normal domain. Compute $\mathrm{Pic}(A)$.
2. If $A = \mathbb{C}[t^3, t^7, t^8] \subseteq \mathbb{C}[t]$, compute $\mathrm{Pic}(A)$. If $A = \{f \in \mathbb{C}[T] \mid f'(0) = f''(0) \text{ and } f(1) = f(-1)\}$ compute $\mathrm{Pic}(A)$.
3. If $A = \mathbb{C}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$, show $\mathrm{Pic}(A) \neq (0)$.

Problem 102

1. Write $A = K[X, Y, Z]$, with K a field. Set $\mathfrak{a} = (X, Y)(X, Z)$. Find a primary decomposition of $\mathfrak{a}$.
2. Let $A = K[X, XY, Y^2, Y^3] \subseteq K[X, Y] = B$, here K is a field. Write $\mathfrak{p} = YB \cap A = (XY, Y^2, Y^3)$. Prove that $\mathfrak{p}^2 = (X^2Y^2, XY^3, Y^4, Y^5)$ and is not primary. Find a primary decomposition of $\mathfrak{p}^2$ involving (Y^2, Y^3). All ideals are ideals of A.

Problem 103

1. Say A is an integral domain. Prove
$$A = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\, A} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} A_{\mathfrak{m}}.$$
2. Now let A be a commutative ring and let $f(T)$ be a polynomial of degree d in $A[T]$. Prove that $A[T]/\big(f(T)\big)$ is an A-projective module of rank d iff the coefficient of T^d in $f(T)$ is a unit of A.

Problem 104 Write A for the polynomial ring $k[T_1, \ldots, T_N]$ in which k is a field and $B = A/\mathfrak{p}$ for some prime ideal, $\mathfrak{p}$, of A. Let the transcendence degree of B over k be d and assume $d \geq 1$. Now let $S_0, S_1, \ldots, S_m$ be further indeterminates independent of the $T_1, \ldots, T_N$, write K for the rational function field $k(S_0, \ldots, S_m)$ and L for $k(S_1, \ldots, S_m)$.

(1) For a polynomial $f \in L \otimes_k A$, write $\mathfrak{P}$ for the ideal of $K \otimes_k A$ generated by $\mathfrak{p}$ and the element $f - S_0$ and prove that $\mathrm{tr.d.}_K(K \otimes_k A)/\mathfrak{P} \leq d - 1$.

(2) Assume further $m \leq N$ and consider the composed map

$$k[T_1, \ldots, T_m] \hookrightarrow A \longrightarrow B.$$

We assume the composed map is *injective* and further that the polynomial $f \in L \otimes_k A$ has the form

$$f = \sum_{j=1}^{m} S_j T_j + g(T_{m+1}, \ldots, T_N).$$

Prove that $\text{tr.d.}_K(K \otimes_k A)/\mathfrak{P} = d - 1$.

(3) Under the hypotheses of (2), assume for each prime ideal, $\mathfrak{B}$, of B, the local ring, $B_{\mathfrak{B}}$, is regular. Write $C = (K \otimes_k A)/\mathfrak{P}$, and let $\mathfrak{q}$ be any element of $\operatorname{Spec} C$. Show that $C_{\mathfrak{q}}$ is regular.

(4) Revisit Problem 83 and give a quick proof.

Problem 105 Suppose k is a field (if necessary, assume $\text{ch}(k) = 0$) and A and C are the following $n \times n$ matrices with entries from k:

$$A = \begin{pmatrix} a_0 & \cdot & \cdots & \cdot & a_{n-1} \\ a_{n-1} & a_0 & \cdots & \cdot & a_{n-2} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix}; \quad C = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Of course, $C^n = I$.

(1) In $\overline{k}$ find all the eigenvalues and eigenvectors of C.

(2) Find a polynomial, $f(X) \in k[X]$, so that $A = f(C)$.

(3) Compute the eigenvalues of A in $\overline{k}$ and show that the corresponding eigenvectors are those of C.

(4) Give a criterion for A to be invertible. Can you give a criterion (in the same spirit) for A to be diagonalizable?

Problem 106 A *discrete valuation*, ν, on a (commutative) ring A, is a function $\nu : A \to \mathbb{Z} \cup \{\infty\}$ satisfying

(a) $\nu(xy) = \nu(x) + \nu(y)$

(b) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, with equality if $\nu(x) \neq \nu(y)$

(c) $\nu(x) = \infty \iff x = 0$.

A pair (A, ν) where A a commutative ring and ν is a discrete valuation is called a *discrete valuation ring* (DVR). Prove the following are equivalent:

(1) A is a DVR

(2) A is a local PID

(3) A is a local, noetherian, normal domain of Krull dimension 1

(4) A is a local, noetherian, normal domain and $(\mathfrak{m}_A \to A)\big(= \{\xi \in \operatorname{Frac} A \mid \xi \mathfrak{m}_A \subseteq A\}\big) \neq A$. Here, $\mathfrak{m}_A$ is the maximal ideal of A.

Problem 107 Let A be a commutative ring with unity and assume A is semi-local (it possesses just finitely many maximal ideals). Write $\mathcal{J}$ for the Jacobson radical of A and give A its $\mathcal{J}$-adic topology.

1. Prove that A is noetherian iff each maximal ideal of A is finitely generated and each ideal is closed in the $\mathcal{J}$-adic topology.
2. Assume A is noetherian, then the map $A \to A_{\text{red}}$ gives A_{red} its $\mathcal{J}$-adic topology. If A_{red} is complete prove that A is complete.

Problem 108

1. Let A be a local ring, give A its $\mathfrak{m}$-adic topology ($\mathfrak{m} = \mathfrak{m}_A$ is the maximal ieal of A) and assume A is complete. Given an A-algebra, B, suppose B is finitely generated as an $\widehat{A}$-module. Prove that B is a finite product of A-algebras each of which is a local ring. Give an example to show that some hypothesis like completness is necessary for the conclusion to be valid.

2. (Hensel) Again A is complete and local, assume $f(X) \in A[X]$ is a monic polynomial. Write $\overline{f(X)}$ for the image of f in $(A/\mathfrak{m})[X]$. If $\overline{f(X)}$ factors as $g(X)h(X)$ where g and h are relatively prime in $(A/\mathfrak{m})[X]$, show that f factors as $G(X)H(X)$ where $\overline{G(X)} = g(X); \overline{H(X)} = h(X)$. What can you say about $\deg G$, $\deg H$ and uniqueness of this factorization? Compare parts (1) and (2).

Problem 109 In this problem, A is an integral domain and $k = \operatorname{Frac} A$. If ν and ω are two discrete valuations of k (cf. Problem 106), the functions ν and ω are defined on A and extended to k *via* $\nu(a/b) = \nu(a) - \nu(b)$, *etc.*), let's call ν, ω inequivalent iff one is not a constant multiple of the other. Write $\mathcal{S}$ for a set of *inequivalent* discrete valuations of k and say that A is *adapted to* $\mathcal{S}$ provided

$$A = \big\{x \in k \mid (\forall \nu \in \mathcal{S})(\nu(x) \geq 0)\big\}.$$

1. Prove the following are equivalent:
   (a) A is a Dedekind domain
   (b) $(\forall$ ideals, $\mathfrak{a},$ of $A)(\forall x, x \neq 0, x \in \mathfrak{a})(\exists\, y \in \mathfrak{a})(\mathfrak{a} = (x, y))$.
   (c) There is a family of discrete valuations of k, say $\mathcal{S}$, for which A is adapted to $\mathcal{S}$ and so that the following holds:
   $$(\forall \nu, \omega \in \mathcal{S})\big(\nu \neq \omega \implies (\exists\, a \in A)(\nu(a) \geq 1 \text{ and } \omega(a-1) \geq 1)\big).$$

2. *Vis a vis* part (1), describe a one-to-one correspondence $\mathcal{S} \leftrightarrow \operatorname{Max}(A)$.

3. Take $k = \mathbb{Q}$, consider all prime numbers p with $p \equiv 1 \pmod 4$, write $\operatorname{ord}_p(n)$ for the highest exponent, e, so that $p^e \mid n$. Then ord_p is a discrete valuation of $\mathbb{Q}$, and we set $\mathcal{S} = \big\{\operatorname{ord}_p \mid p \equiv 1 \pmod 4\big\}$. Illustrate (c) in part (1) above with this $\mathcal{S}$. What is A, in concrete terms? It is pretty clear now how to make many Dedekind domains.

4. Say A is a Dedekind domain and $\mathfrak{a}$, $\mathfrak{b}$ are two non-zero ideals of A. Show $\exists\, x \in k (= \operatorname{Frac} A)$, so that $\mathfrak{a} + x\mathfrak{b} = A$.

5. Again, let A be a Dedekind domain and let L be a *finite* subset of $\operatorname{Max}(A)$. Write $A^L = \bigcap\{A_{\mathfrak{p}} \mid \mathfrak{p} \notin L\}$, then $A \subseteq A^L$ and so $\mathbb{G}_m(A) \subseteq \mathbb{G}_m(A^L)$. Recall, $\mathbb{G}_m(B)$ is the group of units of the ring B. Prove that $\operatorname{Pic}(A)$ is a torsion group $\iff$ $\mathbb{G}_m(A^L)/\mathbb{G}_m(A)$ is a free abelian group of rank $\#(L)$ for every finite set, L, of $\operatorname{Max}(A)$.

Problem 110 (Suggested by A. Auel) Suppose that R is a P.I.D. and consider the functor

$$t\colon R\text{-mod} \rightsquigarrow R\text{-mod}$$

that assigns to each M its torsion submodule. Of course, t is left-exact; what are its right derived functors? If instead, R is just a domain but we assume the $R^p t$ are given as in your answer for the case of a P.I.D., must R be a P.I.D.? Proof or counter-example.

Problem 111 Here, k is a field and $A = k[X_\alpha]_{\alpha \in I}$. The index set, I, may possibly be infinite. Write $\mathfrak{m}$ for the ideal generated by all the X_α, $\alpha \in I$. Set $A_i = A/\mathfrak{m}^{i+1}$, so $A_0 = k$. These A_i form a left mapping system and we set

$$\widehat{A} = \varprojlim A_i$$

and, as usual, call $\widehat{A}$ the *completion of A in the $\mathfrak{m}$-adic topology*. Note that the kernel of $\widehat{A} \to A_j$ is the closure of $\mathfrak{m}^{j+1}$ in $\widehat{A}$.

1. Show that $\widehat{A}$ is canonically isomorphic to the ring of formal power series in the X_α in which only finitely many monomials of each degree occur.

2. Now let $I = \mathbb{N}$ (the counting numbers) and write $\widehat{\mathfrak{m}}$ for the closure of $\mathfrak{m}$ in $\widehat{A}$. By adapting Cantor's diagonal argument, prove that $\widehat{\mathfrak{m}}$ is *not* $\widehat{A}\mathfrak{m}$. Which is bigger?

3. (Bourbaki) Again, I as in (2). Let k be a finite field, prove the

   Lemma. If k is a finite field and $\lambda > 0$, $(\exists\, n_\lambda)(\forall n \geq n_\lambda)$, there is a *homogeneous* polynomial, $F_n \in k[n^2 \text{ variables}]$, so that $\deg F_n = n$ and F_n *cannot* be written as the sum of terms of degree n of *any* polynomial $P_1Q_1 + \cdots + P_\lambda Q_\lambda$, where P_j, Q_j are in $k[n^2 \text{ variables}]$ and have no constant term.

   Use the lemma to prove $(\widehat{m})^2 \neq \widehat{(\mathfrak{m}^2)}$.

4. Use (2) and (3) to prove that $\widehat{A}$ is *not* complete in the $\widehat{\mathfrak{m}}$-adic topology.

5. All the pathology exhibited in (2), (3) and (4) arises as I is not finite; indeed, when I is finite, prove:

   (a) $\widehat{\mathfrak{m}}$ is $\widehat{A}\mathfrak{m}$;

   (b) $\widehat{\mathfrak{m}}^2 = \widehat{(\mathfrak{m}^2)}$;

   (c) $\widehat{A}$ *is* complete in the $\widehat{\mathfrak{m}}$-adic topology.

Problem 112 Consider the category TOP (topological spaces and continuous maps) and T2TOP the full subcategory of Hausdorff topological spaces.

1. At first, use the ordinary Cartesian product in TOP, with the product topology. Denote this $Y \times Z$. Show that $Y \in \text{T2TOP} \iff$ the diagonal map $\Delta : Y \to Y \times Y$ is closed.

2. For $X, Y \in \text{T2TOP}$, recall that $X \xrightarrow{f} Y$ is called a *proper* map $\iff f^{-1}(\text{compact})$ is compact. (Of course, any map $f : X \to Y$ will be proper if X is compact.) Show that $f : X \to Y$ is proper iff $(\forall T \in \text{T2TOP})(f_T : X \underset{Y}{\times} T \to Y \underset{Y}{\times} T$ is a closed map.)

3. With (1) and (2) as background, look at another subcategory, AFF, of TOP: here A is a commutative ring, AFF consists of the topological spaces $\operatorname{Spec} B$, where B is an A-algebra. Maps in AFF are those coming from homomorphisms of A-algebras, viz: $B \to C$ gives $\operatorname{Spec} C \to \operatorname{Spec} B$. Define

   $$(\operatorname{Spec} B) \amalg (\operatorname{Spec} C) = \operatorname{Spec} (B \otimes_A C)$$

   and prove that AFF possesses products.

   NB:

   (a) The topology on $\operatorname{Spec} B \amalg \operatorname{Spec} C$ is *not* the product topology—it is stronger (more opens and closeds)

   (b) $\operatorname{Spec} B \amalg \operatorname{Spec} C \neq \operatorname{Spec} B \times \operatorname{Spec} C$ as sets.
   (Cf. Problem 87)

   Prove: The diagonal map $\Delta_Y : Y \to Y \underset{\operatorname{Spec} A}{\amalg} Y$ is closed ($Y = \operatorname{Spec} B$). This recaptures (1) in the non-Hausdorff setting of AFF.

4. Given $f : \operatorname{Spec} C \to \operatorname{Spec} B$ (arising from an A-algebra map $B \to C$) call f *proper* $\iff$

   (i) C is a finitely generated B-algebra and

   (ii) $(\forall T = \operatorname{Spec} D)(f_T : \operatorname{Spec} C \underset{\operatorname{Spec} A}{\amalg} \operatorname{Spec} D \to \operatorname{Spec} B \underset{\operatorname{Spec} A}{\amalg} \operatorname{Spec} D$ is a closed map.)

Prove: If C is integral over B, then f is proper. However, prove also, $\operatorname{Spec}\big(B[T]\big) \to \operatorname{Spec} B$ is *never* proper.

5. Say $A = \mathbb{C}$. For which A-algebras, B, is the map $\operatorname{Spec} B \to \operatorname{Spec} A$ proper?

Problem 113 Assume A is *noetherian* local, $\mathfrak{m}_A$ is its maximal ideal, and

$$\widehat{A} = \varprojlim_n A/\mathfrak{m}^{n+1} = \text{completion of } A \text{ in the } \mathfrak{m}\text{-adic topology.}$$

Let B, $\mathfrak{m}_B$ be another noetherian local ring and its maximal ideal. Assume $f : A \to B$ is a ring homomorphism and we *always assume* $f(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$.

1. Prove: f gives rise to a homomorphism $\widehat{A} \xrightarrow{\widehat{f}} \widehat{B}$ (and $\mathfrak{m}_{\widehat{A}} \to \mathfrak{m}_{\widehat{B}}$).
2. Prove: $\widehat{f}$ is an isomorphism $\iff$
   (a) B is flat over A
   (b) $f(\mathfrak{m}_A) \cdot B = \mathfrak{m}_B$
   (c) $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ is an isomorphism.
3. Use (2) to give examples of B's that are finite A-modules, non-isomorphic to A, yet $\widehat{A}$ and $\widehat{B}$ are isomorphic.

Problem 114 Suppose that $f \in \mathbb{Z}[X]$ is a non-constant polynomial.

(1) Show there exists an $n \in \mathbb{Z}$ so that $f(n)$ is not a prime number.

(2) Consider the sequence $\{f(n)\}_{n=1}^{\infty}$ and write P for the set of primes dividing at least one term of this sequence. Show P is infinite.

Problem 115 If k is a field and $f \in k[T]$, suppose f has degree n and has n distinct roots $\alpha_1, \ldots, \alpha_n$ in some extension of k. Write $\Omega = k(\alpha_1, \ldots, \alpha_n)$ for the splitting field of f and further take $n+1$ independent indeterminates $X, u_1, \ldots, u_n$ over Ω. Let $\widetilde{k} = k(u_1, \ldots, u_n)$, write $\widetilde{\Omega}$ for $\widetilde{k}(\alpha_1, \ldots, \alpha_n)$ and let $\omega = \alpha_1 u_1 + \cdots + \alpha_n u_n \in \widetilde{\Omega}$. If σ is an *arbitrary permutation* of $\alpha_1, \ldots, \alpha_n$ set

$$\sigma\omega = \sigma(\alpha_1)u_1 + \cdots + \sigma(\alpha_n)u_n,$$

and finally set

$$h(X) = \prod_{\sigma \in \mathcal{S}_n} (X - \sigma\omega).$$

1. Show that $h(X)$ has coefficients in $k[u_1, \ldots, u_n]$.
2. Split $h(X)$ into irreducible factors in $\widetilde{k}[X]$; show all the factors have the same degree, r. (Hint: Natural Irrationalities). Moreover, prove if $\sigma\omega$ is a root of a given factor, the other roots of this factor are exactly the $\tau\sigma\omega$, with $\tau \in \mathfrak{g}(\Omega/k)$. Hence, prove that $r = \#\big(\mathfrak{g}(\Omega/k)\big)$.
3. Using (2), give a procedure for explicitly determining those permutations, $\sigma \in \mathfrak{S}_n$, which belong to $\mathfrak{g}(\Omega/k)$. Illustrate your procedure with the examples: $k = \mathbb{Q}$, $f = T^3 - 2$ and $f = T^4 + T^3 + T^2 + T + 1$.

Problem 116 Here k is a field and Ω is a finite normal extension of k. Prove that there exists a normal tower of fields

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n = \Omega$$

so that

(a) the first r of these extensions are separable and the set $\{\mathfrak{g}(k_i/k_{i-1}) \mid 1 \leq i \leq r\}$ is exactly the set of composition factors of $\mathfrak{g}(\Omega/k)$, and

(b) The last $n-r$ are each purely inseparable over the previous and k_j arises from k_{j-1} by adjunction of a root of $X^p - a_j$, with $a_j \in k_{j-1}$. (Here, $p = \mathrm{char}(k)$.)

Problem 117 Let $g_1, \ldots, g_n$ be polynomials (one variable) with coefficients in $k = k_0, \ldots, k_{n-1}$ respectively, and with k_j the splitting field for g_j. In this case, we say k_n *arises from the successive solution of a chain of equations* $g_1 = 0, g_2 = 0, \ldots, g_n = 0$. If f is a polynomial, we say $f = 0$ *can be solved by means of an auxiliary chain,* $g_i = 0$*, of equations* $\iff$ k_n contains a splitting field for f. When the $g_i(X)$ have the special form $g_i(X) = X^{m_i} - a_i$, we say $f = 0$ may be solved by radicals.

1. Suppose $f = 0$ may be solved by means of the auxiliary chain $g_1 = 0, \ldots, g_n = 0$. Let $\mathfrak{s}(G)$ denote the set of simple constituents (composition factors) of a given finite group, G. Prove that $\mathfrak{s}\big(\mathfrak{g}_k(f)\big) \subseteq \bigcup \mathfrak{s}\big(\mathfrak{g}_{k_{j-1}}(g_j)\big)$.

2. Prove "Galois' Theorem": If k is a field, $f \in k[X]$, and Ω is a splitting field for f over k, assume $\big(\mathrm{char}(k), [\Omega : k]\big) = 1$; then $f = 0$ is solvable by radicals $\iff$ $\mathfrak{g}_k(f)$ is a solvable group.

Problem 118 Here k is a field, α is a root of an irreducible polynomial, $f \in k[X]$.

1. Prove: α lies in a field extension, L, of k obtained by successive solution of a chain of *quadratic* equations $g_1 = 0, \ldots, g_n = 0$ $\iff$ the degree of a splitting field for f over k is a power of 2.

2. Given a line in the plane, we conceive of the line as the real line and the plane as $\mathbb{C}$. *But*, no numbers are represented on the line. However, two points are indicated on the line; we take these as 0 and 1 and label them so. We are given a straight edge (*no markings on it*) and a pair of dividers (no scale on it either) which we can set to any length and which will hold that length. But, if we reset the dividers, the original setting cannot be recaptured if not marked on our plane as a pair of points "already constructed." We can use our implements to make any finite number of the following moves:

   (a) Set the dividers to a position corresponding to two points already constructed, make any arc or circle with the dividers where one leg is at a point already constructed. (A point is constructed iff it is the intersection of an arc and a line, an arc and an arc, a line and a line.)

   (b) Given any pair of previously constructed points use the straight edge to draw a line or segment of a line through these points.

   You should be able to see that from 0 and 1 we can construct $p/q \in \mathbb{Q}$ (all p, q) therefore it is legitimate to label $\mathbb{Q}$ on our real axis. Call a point $(x, y) \in \mathbb{C}$ constructible iff its real and imaginary parts are constructible; that is these numbers, constructed as lengths, can be obtained from $\mathbb{Q}$ by a finite number of moves (a) and (b). Show that $\alpha \in \mathbb{C}$ is constructible iff $\mathbb{Q}(\alpha)$ may be obtained from $\mathbb{Q}$ by the successive solution of a chain of quadratic equations.

3. Prove

   (a) The duplication of a cube by straight edge and dividers is impossible.

   (b) The trisection of an angle by straight edge and dividers is impossible (try $\pi/3$).

4. (Gauss) Prove that a regular n-gon is constructible by straight edge and dividers iff $n = 2^r p_1 p_2 \cdots p_t$, where r is non-negative and the p_j are distinct Fermat primes (cf. Problem 14).

Problem 119 What is wrong with the following argument?
Let k be a field, write $f(X) \in k[X]$, $\deg(f) = n$, and suppose f has n distinct roots $\alpha_1, \ldots, \alpha_n$, in a suitable extension field L/k. Write Ω for the normal extension $k(\alpha_1, \ldots, \alpha_n)$. An element, ω, of Ω has the form $\omega = g(\alpha_1, \ldots, \alpha_n)$, where g is a polynomial in n variables with coefficients in k. Let σ be an arbitrary

permutation of the α_i, then σ maps $g(\alpha_1, \ldots, \alpha_n)$ to $g(\alpha'_1, \ldots, \alpha'_n)$ where $\alpha'_j = \sigma(\alpha_j)$. If $h(\alpha_1, \ldots, \alpha_n)$ is another polynomial with coefficients in k, then $h(\alpha_1, \ldots, \alpha_n) \mapsto h(\alpha'_1, \ldots, \alpha'_n)$ by σ and we have

$$g(\alpha_1, \ldots, \alpha_n) + h(\alpha_1, \ldots, \alpha_n) \to g(\alpha'_1, \ldots, \alpha'_n) + h(\alpha'_1, \ldots, \alpha'_n)$$
$$g(\alpha_1, \ldots, \alpha_n)h(\alpha_1, \ldots, \alpha_n) \to g(\alpha'_1, \ldots, \alpha'_n)h(\alpha'_1, \ldots, \alpha'_n).$$

Thus, we have an automorphism of Ω and the elements of k remain fixed. So, the arbitrary permutation, σ, belongs to the group of k-automorphisms of Ω; hence, the latter group has order greater than or equal to $n!$. By Artin's Theorem, $[\Omega : k] \geq n!$. (Theorem 4.32)

Problem 120 If k is a field, $f \in k[X]$ a separable polynomial and Ω is a splitting field for f over k, write $\mathfrak{g} = \mathfrak{g}(\Omega/k)$ and consider $\mathfrak{g}$ as a subgroup of the permutation group on the roots of f. Show that $\mathfrak{g}$ is a transitive permutation group $\iff$ f is an irreducible polynomial over k. Use this to give a necessary condition that $\sigma \in \mathfrak{S}_n$ actually belongs to $\mathfrak{g}_k(f)$, for f an arbitrary separable polynomial of degree n over k. Illustrate your condition by finding the Galois groups over $\mathbb{Q}$ of the polynomials: $X^5 - 1$, $X^5 + X + 1$.

Problem 121 Here, K is a finite field of q elements and q is odd.

1. Let $\mathrm{sq} : K^* \to K^*$ be the homomorphism given by $\mathrm{sq}(x) = x^2$. Show that $\#\ker \mathrm{sq} = \#\operatorname{coker} \mathrm{sq} = 2$ and $\#\operatorname{Im} \mathrm{sq} = (q-1)/2$.
2. Prove:
$$(\forall x \in K^*)\left(x^{(q-1)/2} = \begin{cases} 1 & \text{if } x \text{ is a square in } K \\ -1 & \text{otherwise} \end{cases}\right)$$
3. If $K = \mathbb{F}_p$, then K contains a square root of -1 iff $p \equiv 1 \bmod 4$.
4. For any finite field, K, every element of K is a sum of squares. Is it true that each element of K is a sum of (at most) two squares?

Problem 122 If k is a field of characteristic zero and $f \in k[X]$ is a monic polynomial, factor f into monic irreducible polynomials in $k[X]$ and set
$$f = g_1 g_2^2 \cdots g_r^r$$
where g_j is the product of the distinct irreducible factors of f which divide f with exact exponent j. Prove that the g.c.d. of f and its, derivative, f', is
$$g_2 g_3^2 \cdots g_r^{r-1}.$$
Assume Euclid's algorithm for finding the g.c.d. of two polynomials. Show that $g_1, \ldots, g_r$ may be determined constructively. If n is an integer, illustrate with
$$f(X) = X^n - 1 \in \mathbb{Q}[X].$$

Problem 123 If k is a field and f, g are non-constant polynomials in $k[X]$, with f irreducible, prove that the degree of every irreducible factor of $f\big(g(X)\big)$ in $k[X]$ is divisible by $\deg f$.

Problem 124 If k is a field, X is transcendental over k, and $f(X) \in k[X]$ is irreducible in $k[X]$, write $\alpha_1, \ldots, \alpha_n$ for a full set of roots of f in a suitable extension field of k. If $\mathrm{char}(k) = 0$, prove that none of the differences $\alpha_i - \alpha_j$ $(i \neq j)$ can lie in k. Give a counterexample for $\mathrm{char}(k) = p > 0$ (*any* prime p).

Problem 125 Let $k \subseteq K$ be two fields of characteristic zero. Assume the following two statements:

(a) Every $f(X) \in k[X]$ of *odd* degree has a root in k

(b) $(\forall \alpha \in k)(X^2 - \alpha$ has a root in $K)$

1. Prove: Each non-constant polynomial $g \in k[X]$ has a root in K.

2. Assume as well that K/k is normal of finite degree. Prove that K is algebraically closed. (Suggestion: Use induction on ν where $\deg g = 2^\nu n_0$ (n_0 odd). If $r \in \mathbb{Z}$, set $\gamma_{ij}^{(r)} = \alpha_i + \alpha_j + r\alpha_i\alpha_j$, where $\alpha_1, \ldots, \alpha_n$ are the roots of g in some $\Omega \supseteq K$. Fix r, show there is a polynomial $h(X) \in k[X]$, so that the $\gamma_{ij}^{(r)}$ are roots of h; for all i, j. Show some $\gamma_{ij}^{(r)} \in K$; now vary r and find $r_1 \neq r_2$ so that $\gamma_{ij}^{(r_1)} \in K$, $\gamma_{ij}^{(r_2)} \in K$.)

3. Take $k = \mathbb{R}$ and $K = \mathbb{C}$. By elementary analysis, (a) and (b) hold. Deduce $\mathbb{C}$ is algebraically closed (Gauss' first proof).

Problem 126 Let $\mathbb{Q}$ be the rational numbers, $\mathbb{R}$ the real numbers , X a transcendental over $\mathbb{R}$ and suppose $f \in \mathbb{Q}[X]$ is a polynomial of degree 3 irreducible in $\mathbb{Q}[X]$ having three real roots α, β, γ. Show that if

$$k_0 = \mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_m$$

is a finite chain of fields each obtained from the preceding one by adjunction of a *real* radical $\rho_j = \sqrt[n_j]{c_j}$ ($n_j \in \mathbb{Z}, n_j > 0, c_j \in k_{j-1}$), the field k_m *cannot* contain ANY of the roots, α, β, γ of f. (Suggestion: If wrong, show we may assume each n_j is prime, let k_j be the field with maximal j where f is still irreducible. If $\alpha \in k_{j+1}$ show $\rho_{j+1} \in k_j(\alpha)$.) This is the famous "casus irreducibilis" of the cubic equation $f = 0$: if the three roots are real, the equation cannot be solved by real radicals.

Problem 127 Here, f is an irreducible quartic polynomial with coefficients in k; assume f has four distinct roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in some extension field of k. Write $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $L = k(\beta)$, and let Ω be $k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

1. Assume $\mathfrak{g}(\Omega/k)$ has full size, i.e., 24, find $\mathfrak{g}(\Omega/L)$.

2. Show that, in any case, β is the root of a cubic polynomial, h, with coefficients in k (Lagrange's "cubic resolvent" for f).

Problem 128 Let k be a field, $\mathrm{char}(k) \neq 2$, write K/k for an extension of degree 2 and L/K for an extension also of degree 2.

1. Show $\exists\, \alpha, \beta$ with $\alpha \in K$, in fact $K = k(\alpha)$, and $\alpha^2 = a \in k$ and $\beta \in L$, $\beta^2 = u + v\alpha$; $u, v \in k$ and $L = K(\beta)$. (All this is very easy).

2. Let Ω be a normal closure of k containing L. Show that $[\Omega : k]$ is 4 or 8. In the case $v = 0$ (part (1)), show $\Omega = k(\alpha, \beta) = L$ and that $\exists\, \sigma, \tau \in \mathfrak{g}(\Omega/k)$ so that $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$, $\tau(\alpha) = \alpha$, $\tau(\beta) = -\beta$. Determine precisely the group $\mathfrak{g}(\Omega/k)$.

3. When $v \neq 0$, let β_1 be a conjugate, not equal to $\pm\beta$, of β. Prove $\Omega = k(\beta, \beta_1)$ and that $\exists\, \sigma \in \mathfrak{g}(\Omega/k)$ such that $\sigma(\beta) = \beta_1$ and $\sigma(\beta_1)$ is one of β or $-\beta$.

4. Show if $[\Omega : k] = 8$ we may assume in (3) that σ maps β_1 to $-\beta$. Prove σ is an element of order 4 and that $\exists\, \tau \in \mathfrak{g}(\Omega/k)$, of order 2, with $\tau^{-1}\sigma\tau = \sigma^{-1}$. Deduce that $\mathfrak{g}(\Omega/k) = \mathrm{Gp}\{\sigma, \tau\}$; which of the two non-abelian groups of order 8 is it?

5. Illustrate (1)-(4) with a discussion of $X^4 - a$ over $\mathbb{Q}$.

6. With the above notation, show that the normal closure of K is cyclic of degree 4 iff a can be written as the sum of two squares, $b^2 + c^2$, in k. (Hints: if Ω is the field above, show $\mathfrak{g}(\Omega/k)$ is cyclic, order 4, iff Ω contains exactly one subfield of degree 2 over k. Then $u^2 - av^2$ must equal aw^2 for some $w \in k$. Now show a is the sum of two squares. You may need to prove that if -1 is a square then every element of k is a sum of two squares in k; cf. Problem 121.) Investigate, from the above, which primes, $p \in \mathbb{Z}$, are the sum of two squares in $\mathbb{Z}$.

Problem 129 Suppose p is a prime number, let $\mathfrak{S}_p$ denote the symmetric group on p letters and write G for a transitive subgroup of $\mathfrak{S}_p$ (i.e., the p letters form an orbit for G).

(1) If G contains a transposition, we know (Problem 13) that $G = \mathfrak{S}_p$. Use this to show there exist extensions, K, of $\mathbb{Q}$ whose Galois group is $\mathfrak{S}_p$.

(2) Hilbert proved the following theorem:

Hilbert Irreducibility Theorem. If $f \in \mathbb{Q}[T_1, \dots, T_r, Z_1, \dots, Z_s]$, where the T's and Z's are all algebraically independent, and if f is irreducible, then there exist integers $a_1, \dots, a_r$ so that substituting a_j for T_j ($j = 1, \dots, r$), the resulting polynomial $\widetilde{f} \in \mathbb{Q}[Z_1, \dots, Z_s]$ is still irreducible. (Actually, there are infinitely many choices for the a_js.)

Use Hilbert's theorem to exhibit $\mathfrak{S}_n$ as a Galois group over $\mathbb{Q}$.

(3) Now A_n is a subgroup of $\mathfrak{S}_n$; can you exhibit A_n as a Galois group over $\mathbb{Q}$? (There is an old open question: Is every finite group, G, the Galois group of some finite normal extension of $\mathbb{Q}$? If G is solvable, this is known (due to Shafarevich) and hard to prove. Many simple groups are known to be Galois groups over $\mathbb{Q}$.)

(4) Write $f(X) = X^5 + aX + 1$ with $a \in \mathbb{Z}$ and let Ω be the splitting field of f over $\mathbb{Q}$. Determine $\mathcal{G}(\Omega/\mathbb{Q})$.

Problem 130 *(Bourbaki)*

1. Say k is a field, $\mathrm{char}(k) = p > 2$; let $K = k(X, Y)$ where X and Y are independent transcendentals over k. Write $L = K(\theta)$, where θ is a root of

$$f(Z) = Z^{2p} + XZ^p + Y \in K[Z].$$

   Show that L/K is inseparable yet does not contain any purely inseparable elements over K. (Suggestion: First show f is irreducible and say $\exists\, \beta \in L, \beta^p \in K, \beta \notin K$. Then prove f becomes reducible in $K(\beta)[Z]$ and that then $X^{1/p}$ and $Y^{1/p}$ would lie in L. Prove then that $[L : K] \geq p^2$.)

2. Find the Galois group $\mathfrak{g}(\Omega/K)$ where Ω is a normal closure of L/K.

3. Now just assume $\mathrm{char}(k) \neq 2$, write $K = k(X)$ in this case. Let σ, τ be the 2-torsion k-automorphisms of K given by $\sigma(X) = -X$; $\tau(X) = 1 - X$ (i.e., $\sigma\big(f(X)\big) = f(-X)$, etc.). Show the fixed field of σ is $k(X^2)$; that of τ is $k(X^2 - X)$. If $\mathrm{char}(k) = 0$, show that $\mathrm{Gp}\{\sigma, \tau\}$ is an infinite group and prove that $k = k(X^2) \cap k(X^2 - X)$.

4. Now assume again $\mathrm{char}(k) = p > 2$. Show in this case $k(X^2) \cap k(X^2 - X)$ is strictly bigger than k—determine it explicitly and find the degree

$$\big[k(X) : (k(X^2) \cap k(X^2 - X))\big].$$

5. What is the situation in (3) and (4) if $\mathrm{char}(k) = 2$?

Problem 131 (Various Galois groups). Determine the Galois groups of the following polynomials over the given fields:

1. $(X^2 - p_1) \cdots (X^2 - p_t)$ over $\mathbb{Q}$, where $p_1, \dots, p_t$ are distinct prime numbers.

2. $X^4 - t$ over $\mathbb{R}(t)$.

3. $X^p - m$ over $\mathbb{Q}$, where p is a prime number and m is a square free integer. (Hint: Here, $\mathfrak{g}$ fits into a split exact sequence of groups

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathfrak{g} \underset{\longleftarrow}{\longrightarrow} ? \longrightarrow 0.)$$

4. $X^8 - 2$ over $\mathbb{Q}(\sqrt{2})$, over $\mathbb{Q}(i)$, over $\mathbb{Q}$. (Cf. Problem 128)

Problem 132 Show that $x^7 - 7x + 3$ has a simple group of order 168 as its Galois group over $\mathbb{Q}$. Can you be more precise as to which group this is?

Problem 133

1. Here K/k is a finite extension of fields. Show the following are equivalent:
   (a) K/k is separable
   (b) $K \otimes_k L$ is a product of fields (product in the category of rings) for *any* field L over k
   (c) $K \otimes_k \overline{k}$ is a product of fields
   (d) $K \otimes_k K$ is a product of fields.
2. Now assume K/k is also a normal extension, and let
$$K_{\mathrm{pi}} = \{\alpha \in K \mid \alpha \text{ is purely inseparable over } k\}.$$
For the map
$$\theta : K_{\mathrm{pi}} \otimes_k K_{\mathrm{pi}} \to K_{\mathrm{pi}} \textit{ via } \theta(\xi \otimes \eta) = \xi\eta,$$
show that the kernel of θ is exactly the nilradical of $K_{\mathrm{pi}} \otimes_k K_{\mathrm{pi}}$.
3. Prove: If K/k is a finite normal extension, then $K \otimes_k K$ is an Artin ring with exactly $[K : k]_{\mathrm{s}}$ prime ideals. The residue fields of all its localizations at these prime ideals are each the same field, K. A necessary and sufficient condition that K/k be purely inseparable is that $K \otimes_k K$ be a local ring. (Hints: $K = K_{\mathrm{s}} \otimes_k K_{\mathrm{pi}}$ and the normal basis theorem.)

Problem 134 Throughout this problem, G is a finite group, k is a field, and $R = k[G]$. We further assume that $(\#(G), \mathrm{char}(k)) = 1$.

(1) If S is a k-algebra (not necessarily commutative) write $\mathrm{Fcn}(G, S)$ for the k-module of all functions from G to S under pointwise addition and k-multiplication.

For $f \in \mathrm{Fcn}(G, S)$, we set
$$\int_G f(\sigma)d\sigma = \frac{1}{\#(G)} \sum_{\sigma \in G} f(\sigma).$$
Further, write $f_\tau(\sigma) = f(\tau\sigma)$ and show that
$$\int_G f_\tau(\sigma)d\sigma = \int_G f(\tau\sigma)d\sigma = \int_G f(\sigma)d\sigma$$
as well as
$$\int_G 1 d\sigma = 1.$$
(We can write this as $d(\tau\sigma) = d\sigma$ and refer to the above as the "left invariance of the integral". Of course, the integral is also right invariant as well as "inverse invariant" (i.e., $d(\sigma^{-1}) = d\sigma$.) The integral is also called a "mean" on G as it averages the values of the function f.

(2) If M is an R-module (i.e., a G-module which is also a k-vector space) and N is a sub-R-module of M, write π for any k-projection of M onto N. (So then, $M = \mathrm{Ker}\ \pi \amalg N$ *as k-spaces*.) Now $\pi \in \mathrm{End}_k(M) (= S)$, so we can form
$$T = \int_G (\sigma^{-1}\pi\sigma)d\sigma.$$

Prove that T is a G-invariant projection from M onto N and that

$$M = \text{Ker } T \amalg N, \quad \textit{as } R\textit{-modules.}$$

Deduce

Maschke's Theorem (1898) *If G, R and k are as above with $(\#(G), \text{char}(k)) = 1$, then R is semi-simple as k-algebra.*

(3) If M is a simple R-module, prove that M is finite-dimensional as a k-vector space. (R-modules are called (linear) *representation spaces for* G and the map $G \longrightarrow \text{Aut}(M)$, making M a G-module, is called *a representation of G with space M*. The dimension of M (as k-space) is called the *degree* of the representation.) It is a known theorem of Wederburn that a simple k-algebra with the D.C.C. (on left ideals) is isomorphic (as k-algebra) to the $r \times r$ matrices over a division ring, D. If k is algebraically closed, prove that D is k itself. Now prove that

(a) For each finite group, G, and algebraically closed field, k, with $(\#(G), \text{char}(k)) = 1$, the number of non-isomorphic simple $k[G]$-modules is finite,

and

(b) We have $g = f_1^2 + \cdots + f_t^2$, where f_j is the degree of the j^{th} simple R-module and $g = \#(G)$.

Problem 135 Say R is a not necessarily commutative ring but that R is noetherian (on the left).

(1) Given a f.g. R-module, M, show that $\text{projdim}_R(M) \leq d$ if and only if for all **finitely generated** R-modules, N, we have

$$\text{Ext}_R^{d+1}(M, N) = (0).$$

(2) Does the same criterion work for non f.g. R-modules M?

Problem 136 (Yoneda) Here, R is a ring and M', M'' are R-modules.

(1) Consider exact sequences of the form

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow X_2 \longrightarrow M'' \longrightarrow 0 \qquad (E_2)$$

where the X_i are R-modules. Call such "2-fold extensions of M'' by M'" and, on the model of ordinary extensions, define an equivalence relation on the 2-fold extensions. Prove that the equivalence classes so defined are in 1-1 correspondence with $\text{Ext}_R^2(M'', M')$.

(2) Generalize part (1) to "n-fold extensions":

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_n \longrightarrow M'' \longrightarrow 0 \qquad (E_n)$$

including the 1-1 correspondence of the equivalence classes with $\text{Ext}_R^n(M'', M')$.

(3) We know $\text{Ext}_R^n(A, B)$ is a co-functor in A and a functor in the variable B. If $M' \longrightarrow \widetilde{M}'$ and if $\xi \in \text{Ext}_R^n(M'', M')$ is represented by

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_n \longrightarrow M'' \longrightarrow 0,$$

describe explicitly an n-fold extension representing the image of ξ in $\text{Ext}_R^n(M'', \widetilde{M}')$. Same question but for a morphism $M'' \longrightarrow \widetilde{M}''$ and an element $\widetilde{\xi} \in \text{Ext}_R^n(\widetilde{M}'', M')$.

(4) $\text{Ext}_R^n(-, -)$ is an abelian group, as we know. Start with $n = 1$ and describe, in terms of representing extensions,

$$0 \longrightarrow M' \longrightarrow X \longrightarrow M'' \longrightarrow 0,$$

the abelian group structure on $\mathrm{Ext}^n_R(M'', M')$. (Of course, you must show your explicit construction of the equivalence class of a sum of two extensions

$$0 \longrightarrow M' \longrightarrow X \longrightarrow M'' \longrightarrow 0 \qquad (a)$$
$$0 \longrightarrow M' \longrightarrow Y \longrightarrow M'' \longrightarrow 0 \qquad (b)$$

is independent of the choice of the representatives (a) and (b).) Continue with the general case of n-fold extensions.

(5) Say

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_r \longrightarrow Z \longrightarrow 0$$

and

$$0 \longrightarrow Z \longrightarrow Y_1 \longrightarrow \cdots \longrightarrow Y_s \longrightarrow M'' \longrightarrow 0$$

are an r-fold (resp. s-fold) extension of Z by M' (resp. of M'' by Z). We can splice these to obtain an $r+s$-fold extension of M'' by M':

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_r \longrightarrow Y_1 \longrightarrow \cdots \longrightarrow Y_s \longrightarrow M'' \longrightarrow 0.$$

Prove that this process respects the equivalence relation on extensions and therefore yields a map

$$\theta\colon \mathrm{Ext}^s_R(M'', Z) \prod \mathrm{Ext}^r_R(Z, M') \longrightarrow \mathrm{Ext}^{r+s}_R(M'', M').$$

Show that from an r-fold extension

$$0 \longrightarrow M' \longrightarrow X_1 \longrightarrow \cdots \longrightarrow X_r \longrightarrow Z \longrightarrow 0 \qquad (E_r)$$

we obtain an "iterated connecting homomorphism"

$$\delta_r\colon \mathrm{Hom}_R(M', A) \longrightarrow \mathrm{Ext}^r_R(Z, A)$$

for any R-module, A. If we take $A = M'$ and compute $\delta_r(\mathrm{id}_{M'})$, we get an element $\chi(E_r)$ in $\mathrm{Ext}^r_R(Z, M')$. Prove that $\chi(E_r)$ depends only on the equivalence class of E_r and gives the 1-1 correspondence of part (2). Discuss the pairing θ in terms of these "characteristic classes", $\chi(E_r)$, of extensions.

(6) Show that θ is actually bi-additive, hence it is $\mathbb{Z}$-bilinear and therefore we get a map

$$\mathrm{Ext}^s_R(M'', Z) \otimes_{\mathbb{Z}} \mathrm{Ext}^r_R(Z, M') \longrightarrow \mathrm{Ext}^{r+s}_R(M'', M').$$

Take $M = Z = M''$, call the common value M. Then we can compute $\theta(\alpha, \beta)$ and $\theta(\beta, \alpha)$ for $\alpha \in \mathrm{Ext}^r_R(M, M)$ and $\beta \in \mathrm{Ext}^s_R(M, M)$. Is θ commutative? Is θ graded commutative $(\theta(\alpha, \beta) = (-1)^{rs}\theta(\beta, \alpha))$? Neither?

Problem 137 We take G to be a group and write R for $\mathbb{Z}[G]$.

(1) Recall from Chapter 5, Section 5.3, that there is an isomorphism

$$H^p(G, M) \cong \mathrm{Ext}^p_R(\mathbb{Z}, M)$$

for every $p \geq 0$. Here, M is a G-module (so, an R-module). When $p = 2$, the left hand group classifies group extensions

$$0 \longrightarrow M \longrightarrow \mathfrak{G} \longrightarrow G \longrightarrow 1 \qquad (E)$$

up to equivalence, while the right hand side classifies 2-extensions (of R-modules)

$$0 \longrightarrow M \longrightarrow X_1 \longrightarrow X_2 \longrightarrow \mathbb{Z} \longrightarrow 0, \qquad (\mathcal{E})$$

again up to equivalence.

In terms of exact sequences and natural operations with them describe the 1-1 correspondence between sequences (E) and $(\mathcal{E})$.

(2) Again, with the G-action on M fixed, extensions (E) can be classified by equivalence classes of 2-cocycles of G with values in M. Given such a 2-cocycle, show how to construct, explicitly, a 2-extension $(\mathcal{E})$. Carry through the verification that cohomologous 2-cocycles yield equivalent 2-extensions.

(3) Transfer the Yoneda addition of 2-extensions from Problem 136 to the addition of group extensions—the so called Baer addition.

Problem 138

1. Let $A = k[X_1, \ldots, X_n]/\big(f(X_1, \ldots, X_n)\big)$, where k is a field. Assume, for each maximal ideal, $\mathfrak{p}$, of A, we have $(\operatorname{grad} f)(\mathfrak{p}) \neq 0$ (i.e., $(\forall\, \mathfrak{p})(\exists$ component of $\operatorname{grad} f$ not in $\mathfrak{p})$). Show that $\operatorname{Der}_k(A, A)$ is a projective A-module.

2. Suppose now $A = k[X, Y]/(Y^2 - X^3)$, $\operatorname{char}(k) \neq 2, \neq 3$. Consider the linear map $A \amalg A \to A$ given by the matrix (X^2, Y); find generators for the kernel of this map.

3. In the situation of (2), show that $\operatorname{Der}_k(A, A)$ is *not* projective over A.

Problem 139 Suppose in a ring R (assumed commutative for simplicity) we have elements $f_1, \ldots, f_r$. We let $\overrightarrow{f} = (f_1, \ldots, f_r)$; prove that

$$K_\bullet(\overrightarrow{f}) \cong K_\bullet(\overrightarrow{f_1}) \otimes_R \cdots \otimes_R K_\bullet(\overrightarrow{f_r}),$$

where on the right hand side we mean the total complex.

Problem 140 For G a group and M a right G-module, let M be considered as a "trivial" (left) $\mathbb{Z}[G]$-module and consider the bar complex as in Section 5.3, Chapter 5 of the text with boundary map

$$\partial_n(m \otimes \sigma_1 \otimes \cdots \otimes \sigma_n) = m\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n + \sum_{i=1}^{n-1} (-1)^i m \otimes \sigma_1 \otimes \cdots \otimes \sigma_i\sigma_{i+1} \otimes \cdots \otimes \sigma_n + (-1)^{n+1} m \otimes \sigma_1 \otimes \cdots \otimes \sigma_{n-1}.$$

Define

$$\widetilde{H}_n(G, M) = \operatorname{Ker} \partial_n / \operatorname{Im} \partial_{n+1}$$

and prove that $M \rightsquigarrow \{\widetilde{H}_\bullet(G, M)\}$ is a universal ∂-functor as stated in the text. Thus, complete, by elementary methods, the identification of group homology for (right) G-modules, M, and Hochschild homology for the ring $\mathbb{Z}[G]$ and the modules $\epsilon_* M$ (definition on page 339, top).

Problem 141 Suppose that G is a profinite group and that H is a closed subgroup of G.

(1) Show that $\operatorname{c.d}(H) \leq \operatorname{c.d}(G)$.

(2) If H is open in G (and hence automatically closed in G), can you strengthen the inequality of (1)?

(3) Suppose G is a *finite* group. Prove that

$$\operatorname{c.d}(G) = \begin{cases} 0 \\ \infty \end{cases}$$

and $\operatorname{c.d}(G) = 0$ when and only when $G = \{1\}$.

Problem 142 For simplicity, assume in this problem that A is a commutative ring. If $\overrightarrow{f} = (f_1, \ldots, f_r)$ and $\overrightarrow{g} = (g_1, \ldots, g_r)$ are two ordered sequences of elements of A, write $\overrightarrow{fg}$ for the sequence $(f_1 g_1, \ldots, f_r g_r)$. Now, we have a map

$$\varphi_{\overrightarrow{g}} \colon K_\bullet(\overrightarrow{fg}) \longrightarrow K_\bullet(\overrightarrow{f})$$

induced by

$$\varphi_{\overrightarrow{g}}(\xi_1, \ldots, \xi_r) = (g_1\xi_1, \ldots, g_r\xi_r).$$

(1) Show that this map is a chain map.

(2) Write $\overrightarrow{f^p} = (f_1^p, \ldots, f_r^p)$, then, for $0 < s < t$, we get a map

$$\varphi_{\overrightarrow{f^{t-s}}} \colon K_\bullet(\overrightarrow{f^t}) \longrightarrow K_\bullet(\overrightarrow{f^s})$$

and hence

$$\varphi^\bullet_{\overrightarrow{f^{t-s}}}(M) \colon K^\bullet(\overrightarrow{f^s}, M) \longrightarrow K^\bullet(\overrightarrow{f^t}, M).$$

We set

$$C^\bullet((\overrightarrow{f}), M) = \varinjlim K^\bullet(\overrightarrow{f^t}, M)$$

(with respect to these maps) and further set

$$H^\bullet((\overrightarrow{f}), M) = H^\bullet(C^\bullet((\overrightarrow{f}), M)).$$

Prove that

$$H^\bullet((\overrightarrow{f}), M) = \varinjlim H^\bullet(\overrightarrow{f^t}, M).$$

(3) Now, fix $\overrightarrow{f}$ and for the given $\overrightarrow{g}$, define

$$E_g \colon K_\bullet(\overrightarrow{f}) \longrightarrow K_\bullet(\overrightarrow{f})$$

by the equation

$$(E_g)_\bullet(z) = \left(\sum_{j=1}^{r} g_j e_j\right) \wedge z; \quad \text{the } e_j \text{ are a base for } A^r.$$

Prove that

$$d \circ E_g + E_g \circ d = \left(\sum_{i=1}^{r} g_i f_i\right) \mathrm{id} \quad \text{on } K_t(\overrightarrow{f}), \text{ all } t \geq 0.$$

Deduce the

Proposition *Suppose $f_1, \ldots, f_r$ generate the unit ideal of A, then for all A-modules, M, the complexes*

$$K_\bullet(\overrightarrow{f^t});\ K_\bullet(\overrightarrow{f^t}, M);\ K^\bullet(\overrightarrow{f^t}, M);\ C^\bullet((\overrightarrow{f^t}), M)$$

have trivial (co)homology in **all** *dimensions.*

(4) The homology and cohomology modules $H_0(\overrightarrow{f}, M)$, $H_r(\overrightarrow{f}, M)$, $H^0(\overrightarrow{f}, M)$, $H^r(\overrightarrow{f}, M)$ depend only on the ideal, $\mathfrak{A}$, generated by $f_1, \ldots, f_r$. Is it true that $H^\bullet((\overrightarrow{f}), M)$ depends only on $\mathfrak{A}$ as (3) suggests?

Problem 143 Give the proof of "Lemma C" (= Lemma 5.51 of the text) following the methods used for "Lemmas A & B".

Problem 144 If A is a P.I.D., prove that $\mathrm{gldim}(A) \leq 1$. Under what conditions does the strict inequality hold? You may wish to investigate first the relations between $\mathrm{gldim}(A)$ and $\mathrm{gldim}(A_{\mathfrak{p}})$ for a commutative (noetherian?) ring, A, and all its prime ideals, $\mathfrak{p}$. Is the inequality $\mathrm{gldim}(A) \leq 1$ still valid if A is just a principal ideal ring (not a domain)? If A is a Dedekind ring, what is $\mathrm{gldim}(A)$?

Problem 145

1. Prove the six conditions of Proposition 5.70 are indeed equivalent.
2. Prove that the ten conditions listed in Proposition 5.71 are equivalent.

Problem 146 Here, A is a commutative ring, $\mathfrak{A}$ is an ideal of A and M is an A-module.

1. Prove that the number of elements in a maximal M-regular sequence from $\mathfrak{A}$ is independent of the choice of these elements (from $\mathfrak{A}$). Thus, $\mathrm{depth}_{\mathfrak{A}} M$ is well-defined.
2. Reformulate Koszul's Proposition (our 5.66) in terms of $\mathfrak{A}$-depth.
3. If A and M are graded and $(f_1, \ldots, f_t) = \overrightarrow{f}$ is an M -regular sequence of *homogeneous* elements then any permutation of $(f_1, \ldots, f_t)$ is still an M-regular sequence.

Problem 147 (R. Brauer) Here, G is a group and T is a finite subgroup of order m. For $\sigma, \tau \in G$, we define

$$\sigma \sim \tau \Longleftrightarrow (\exists t \in T)(\sigma^{-i} t \tau^i \in T, \text{ all } i \in \mathbb{Z}).$$

1. Show that $\sim$ is an equivalence relation and that each equivalence class has m elements.
2. Say $\sigma \sim \tau$, prove there is an $x \in T$ so that $\tau^m = x^{-1}\sigma^m x$.
3. Let S be a subset of $Z(G)$; pick a suitable T as above and show: Given $n \in \mathbb{Z}$, either
$$\#(\{z \in G \mid z^n \in S\}) = \infty$$
or this cardinality is divisible by $\mathrm{g.c.d}(n, m)$.
4. When $\#(G) = g < \infty$, show that the cardinality of the set in (3) is divisible by $\mathrm{g.c.d}(g, n)$.

Problem 148 If $F(r)$ is the free group of rank r, and if $\Gamma_n(F(r))$ is the n^{th} term in the lower central series for $F(r)$, prove that the group $G = F(r)/\Gamma_n(F(r))$ is torsion-free.

Problem 149 Suppose A is a commutative ring, write $\mathrm{GL}(A)$ for the group $\bigcup_{n=1}^{\infty} \mathrm{GL}(n, A)$ in which $\mathrm{GL}(n, A)$ is a subgroup of $\mathrm{GL}(n+1, A)$ by the map

$$\xi \mapsto \left(\begin{array}{c|c} \xi & 0 \\ \hline 0 & 1 \end{array}\right)$$

1. When $A = \mathbb{Z}$, consider elements of $\mathrm{GL}(n+1, \mathbb{Z})$ of the form
$$\left.\begin{array}{c} \left(\begin{array}{ccc|c} & & & * \\ & I & & \vdots \\ & & & * \\ \hline 0 & \cdots & 0 & * \end{array}\right) \\ \underbrace{\qquad\qquad}_{n} \end{array}\right\} n$$
and their transposes. Show these matrices generate $\mathrm{GL}(n+1, \mathbb{Z})$ (as a group).

2. Prove that for any $\alpha \in \mathrm{GL}(n, A)$, there exist elements $x, \beta \in \mathrm{GL}(A)$ with β of the form

$$\beta = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & * \end{array}\right) \begin{array}{l} \} n \\ \} r \end{array}$$
$$\underbrace{}_{n} \quad \underbrace{}_{r}$$

and $\alpha = x\beta x^{-1}$.

Problem 150 Let k be a field, $\mathrm{ch}(k) \neq 2$ and write F for any overfield of k. Denote by $V_n(F)$ the set of all *symmetric, nilpotent* $n \times n$ matrices, A, with *entries in* F and $\mathrm{rank}(A) = n - 1$.

1. In the ring of all $n \times n$ matrices over F, show that if a matrix commutes with A it must be a polynomial (coefficients in F) in A.

2. When $n = 2$ and $F = \mathbb{F}_p$, prove that $V_2(F)$ is non-empty when and only when $p \equiv 1 \pmod 4$.

3. If $n = 3$ and $p \equiv 1 \pmod 4$ then $V_3(\mathbb{F}_p) \neq \emptyset$. Show, moreover, that $V_3(\mathbb{F}_3) \neq \emptyset$.

4. Let $\mathbb{Z}_p$ denote the ring of p-adic integers with $p \neq 2$. Prove there is an $n \times n$ symmetric matrix, B, with entries in $\mathbb{Z}_p$ so that $B^n = pC$ iff $V_n(\mathbb{F}_p) \neq \emptyset$. (Here, C is an *invertible* $n \times n$ matrix with entries in $\mathbb{Z}_p$.)

5. As usual, write $\overline{F}$ for the algebraic closure of F and $O_n(\overline{F})$ for the group of orthogonal matrices for the standard diagonal form (entries in $\overline{F}$). If $D \in \mathrm{GL}(n, \overline{F})$, write $\mathrm{Cay}(D) = D^\top D$ (this is the *Cayley transform of* D) and show the map
$$D \mapsto \mathrm{Cay}(D)$$
is an isomorphism of the coset space $O_n(\overline{F})\backslash GL(n, \overline{F})$ with the set, $S_n(\overline{F})$, consisting of symmetric, invertible $n \times n$ matrices from $\overline{F}$. Is this true when F replaces $\overline{F}$?

6. Write N for the nilpotent matrix $(n \times n)$
$$N = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$
If S is a symmetric $n \times n$ matrix prove that $SN = N^\top S$ iff S has the form
$$S = \begin{pmatrix} s_n & s_{n-1} & \cdots & s_2 & s_1 \\ s_{n-1} & s_{n-2} & \cdots & s_1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ s_2 & s_1 & \cdots & 0 & 0 \\ s_1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$
and show further that S is invertible iff s_1 is a unit.

7. Say $p \neq 2$, prove that $V_n(\overline{\mathbb{F}_p}) \neq \emptyset$. Using only (5) and (6) above, determine how big an extension, K, of $\mathbb{F}_p$ you need to guarantee $V_n(K) \neq \emptyset$.

Problem 151 (Continuation of Problem 150) Here, $\mathrm{ch}(F) \neq 2$.

1. Prove $O_n(\overline{F})$ acts transitively on $V_n(\overline{F})$.

2. Show $V_n(\overline{F})$ is a principal homogeneous space (= a *torsor*) for the group $PO_n(\overline{F})$, which, by definition, is $O_n(\overline{F})/(\pm I)$.

3. If n is odd, show $V_n(\overline{F})$ is a torsor for $SO_n(\overline{F})$; while if n is even, prove $V_n(\overline{F})$ has two components.

Problem 152 (Sierpinski) Write $\pi(x)$ for the nunmber of prime integers less than or equal to the positive real number x. The Prime Number Theorem asserts that $\lim_{x\mapsto\infty} \pi(x)\Big/\left(\frac{x}{\log x}\right) = 1$. Call a rational number *special* if it has the form $\frac{p}{q}$ where p and q are prime integers. Prove that the special rational numbers are dense in the positive reals.

Problem 153 Suppose $(B_\alpha, \varphi_\alpha^\beta)$ is a right mapping system of Artinian rings. Write B for $\varinjlim B_\alpha$, and assume B is noetherian. Prove that B is Artinian. That is, B is Artinian iff it is noetherian.

Problem 154 Fix a commutative ring, R, and an R-module, E. Suppose A and B are submodules of E so that B is free (of rank r) and is a direct summand of E. Prove that for an integer $q \geq 0$, the following are equivalent:

(a) The map $\bigwedge^q A \longrightarrow \bigwedge^q(E/B)$ is zero.

(b) The map $\bigwedge^q((A+B)/B) \longrightarrow \bigwedge^q(E/B)$ is zero.

(c) The map $\bigwedge^{q+r}(A+B) \longrightarrow \bigwedge^{q+r} E$ is zero.

Problem 155 Throughout this problem A, B, C are three subgroups of a group, G, and we assume $AB = BA$, $AC = CA$ and $C \subseteq B$.

1. Prove that $(B\colon C) = (AB\colon AC)/(A\cap B\colon A\cap C)$.

2. Suppose φ maps B onto a group B^* and write C^* for the image of C under φ. Prove that
$$(B\colon C) = (B^*\colon C^*)(\operatorname{Ker}\varphi\colon \operatorname{Ker}(\varphi \restriction C)).$$

3. Here, let φ and ψ be in $\operatorname{End}(G)$; assume $\varphi\psi$ and $\psi\varphi$ are each the trivial homomorphism. Let H be any subgroup of G stable under both φ and ψ. Show that
$$(G\colon H)(\operatorname{Ker}(\varphi \restriction H)\colon \operatorname{Im}(\psi \restriction H)) = (\varphi(G)\colon \varphi(H))(\psi(G)\colon \psi(H))(\operatorname{Ker}\varphi\colon \operatorname{Im}\psi).$$

4. Under the hypotheses of (3), if $(G\colon H) < \infty$, deduce *Herbrand's Lemma*:
$$(\operatorname{Ker}\varphi\colon \operatorname{Im}\psi)(\operatorname{Ker}(\psi \restriction H)\colon \varphi(H)) = (\operatorname{Ker}\psi\colon \operatorname{Im}\varphi)(\operatorname{Ker}(\varphi \restriction H)\colon \psi(H)).$$

Problem 156 Suppose A is a (commutative) local or semi-local ring. Recall that the (*strict*) *Henselization of* A, denoted A^h, is the right limit, $\varinjlim C$, in which C runs over the family of finitely presented *étale* A-algebras.

1. If B is a semi-local A-algebra (A also being semi-local) and if B is integral over A, prove that $B\otimes_A A^h$ is both semi-local and isomorphic to B^h.

2. Suppose A is local and Henselian (*i.e.* $A = A^h$), show that for every $\mathfrak{p} \in \operatorname{Spec} A$ the integral closure of $A/\mathfrak{p}$ in $\operatorname{Frac}(A/\mathfrak{p})$ is again a local ring.

Problem 157 (Eilenberg) Let R be the non-commutative polynomial ring in n variables, $T_1, \ldots, T_n$, over the field k; so, $R = k\langle T_1, \ldots, T_n\rangle$. If M is a two-sided R-module, then a *crossed homomorphism* from R to M is an R-module map $R \longrightarrow M$ so that
$$f(\xi\eta) = \xi f(\eta) + f(\xi)\eta.$$
(Also called a derivation).

1. Given elements $m_1, \ldots, m_n$ from M, show that the assigment $T_j \mapsto m_j$ gives rise to a unique crossed homomorphism $R \longrightarrow M$. Here, there is no restriction on the m_j.

2. As in Section 5.3 of the text, consider the augmentation ideal, $\mathfrak{J}$, for the map $\partial_0 \colon R^e \to R$. Prove that $\mathfrak{J}$ is a free R^e-module on the base $T_j \otimes 1 - 1 \otimes T_j^{\mathrm{op}}$, $j = 1, 2, \ldots, n$.

3. Deduce from (2) that $\dim_{R^e}(R) = 1$ $(n > 0)$ in contradistinction to the commutative case.

Problem 158 (Serre) Here, G is a group and it acts on a set, S.

1. Suppose G is finite and S is finite. Write χ for the function on G to $\mathbb{C}$ given by

$$\chi(\sigma) = \#\text{ of fixed points of } \sigma \text{ on } S.$$

Prove *Burnside's Lemma*: The number of orbits of G acting on S equals $\int \chi(\sigma) d\sigma$ (cf. Problem 134 for notation). (Suggestions. Show it suffices to give the proof when S *is* an orbit. In this case write

$$\int \chi(\sigma) d\sigma = \int \Big(\sum_{x \in S^\sigma} 1 \Big) d\sigma = \sum_{s \in S} \int_{G_x} 1 d\sigma,$$

where $G_x = \{\sigma \in G \mid \sigma x = x\}$.)

2. Apply part (1) to the set $S \coprod S$ with its G-action to see that $\chi^2(\sigma)$ counts the fixed points of σ on $S \coprod S$. Prove: $\int \chi^2(\sigma) d\sigma \geq 2$.

3. Write $G_0 = \{\sigma \in G \mid \chi(\sigma) = 0\}$ = the σ's of G having no fixed points. Set $n = \#(S)$ and prove

$$\int_{G - G_0} (\chi(\sigma) - 1)(\chi(\sigma) - n) d\sigma \leq 0.$$

Next assume $n \geq 2$ and G acts transitively on S. Prove that

$$\int_G (\chi(\sigma) - 1)(\chi(\sigma) - n) d\sigma \geq 1$$

and evaluate $\int_{G_0} (\chi(\sigma) - 1)(\chi(\sigma) - n) d\sigma$. Put all together to prove the

Cameron-Cohen Inequality: If $n \geq 2$ and S is a G-orbit then

$$\frac{\#(G_0)}{\#(G)} \geq \frac{1}{n}.$$

Deduce *Jordan's Theorem*: If G acts on S transitively and $\#(S) \geq 2$, then there is a $\sigma \in G$ having no fixed point on S.

Problem 159 (Kaplansky) R is a ring and we are interested in "big" R-modules, i.e., those generated by more than $\aleph_0$ generators. For this reason, modules finitely or countably generated will be called "atoms" and we use the locution "finite atom" for a f.g. module.

1. Suppose M is an R-module that is a coproduct of (an arbitrary number of) atoms, say $M = \coprod M_i$. Suppose further P is a direct summand of M; that is,

$$M = P \amalg Q \qquad (\text{some } Q)$$

Prove there exists a well-ordered increasing family $\{S_\alpha\}_{\alpha \text{ an ordinal}}$ of submodules of M having the following properties:

(a) Each S_α is a coproduct of some of the M_i

(b) Each S_α splits as $(S_\alpha \cap P) \coprod (S_\alpha \cap Q)$

(c) If α is a limit ordinal, then $S_\alpha = \bigcup_{\beta<\alpha} S_\beta$

(d) $S_{\alpha+1}/S_\alpha$ is an atom.

(Hints: We use transfinite induction. By (c) we know how to proceed at a limit ordinal, check properties (a) and (b). The only point is to construct $S_{\alpha+1}$ from S_α. One of the M_i is not contained in S_α, call it M^*. Write the generators of the atom M^* as

$$x_{11}\, x_{12}\, x_{13}\, x_{14}\, \cdots$$

Begin with x_{11} and split it into its P and Q components giving us two new elements of M. Show only finitely many M_i's appear in the coproduct decomposition of these new elements; so, if we take $\coprod\{M_i \mid M_i \text{ appears}\}$ we get an atom. Write its generators as a second row of the infinite matrix being constructed. Repeat for x_{12} and get the third row $x_{31}\, x_{32}\, \cdots$. Now just as in the counting of $\mathbb{Q}$ take the elements in "diagonal order": $x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \cdots$ and keep repeating. Show that

$$S_{\alpha+1} = \text{module generated by } S_\alpha \text{ and all } x_{ij}$$

has (a) and (b) ((d) is obvious).)

2. Write $P_\alpha = P \cap S_\alpha$, show P_α is a direct summand of $P_{\alpha+1}$, that $P_\alpha = \bigcup_{\beta<\alpha} P_\beta$ (when α is a limit ordinal) and that $P_{\alpha+1}/P_\alpha$ is an atom. Finally, deduce P is a coproduct of atoms and so prove

Kaplansky's Theorem. Every direct summand of a module which is a coproduct of atoms is itself a coproduct of atoms. Every projective R-module is a coproduct of atoms.

Chapter 1

Group Theory

1.1 Introduction

Groups are probably the most useful of the structures of algebra; they appear throughout mathematics, physics[1] and chemistry. They almost always occur as "groups of transformations" and that is the way we will use them at first. This allows of tremendous freedom, constrained only by the imagination in finding objects on which to let groups act, or, what is the same, in finding homomorphisms from the group to the "automorphisms" of some object or structure. Then we will look into groups *qua* groups, and here there is a sharp distinction between the finite case and the infinite case. In the finite case, there is a subtle interplay (not yet fully understood) between the order of a group and its structure, whereas in the infinite case"geometric" arguments and applications are more the norm.

1.2 Group Actions and First Applications; The Three Sylow Theorems

We begin by reviewing the notion of group action.

Definition 1.1 Let G be a group and S be a set. We say that G *acts on* S *(on the left)* (or that *there is a (left)* G*-action on* S) iff there is a map

$$\begin{array}{ccc} G \prod S & \longrightarrow & S \\ (\sigma,\, s) & \mapsto & \sigma \cdot s \end{array}$$

called the *action*, satisfying the two rules:

(1) $(\forall s \in S)(1 \cdot s = s)$

(2) $(\forall \sigma, \tau \in G)(\forall s \in S)(\sigma \cdot (\tau \cdot s) = (\sigma\tau) \cdot s)$.

Remarks:

(1) For every $\sigma \in G$, the map $s \mapsto \sigma \cdot s$ is a bijection of S to itself. Its inverse is the map $s \mapsto \sigma^{-1} \cdot s$. We let $\mathrm{Aut}(S)$ denote the set of all set theoretic bijections of S.

[1]The word group even occurs in Einstein's first paper [12] on special relativity; it is the only place to my knowledge where that word appears in Einstein's corpus of scientific work.

(2) Write $\theta(\sigma)$ for the element of $\mathrm{Aut}(S)$ given by remark (1), *i.e.*,

$$\theta(\sigma)(s) = \sigma \cdot s.$$

Then, the map $\theta\colon G \to \mathrm{Aut}(S)$ is a homomorphism of groups (where $\mathrm{Aut}(S)$ is a group under composition).

(3) Conversely, a n.a.s.c. that G act on S is that there is a *homomorphism* $\theta\colon G \to \mathrm{Aut}(S)$. (The action gives θ by remarks (1) and (2), and given θ, define the corresponding action by $\sigma \cdot s = \theta(\sigma)(s)$. Check that this is an action (DX).)

Say G acts on S, and for any given s consider

$$\mathrm{St}(s) = \{\sigma \in G \mid \sigma \cdot s = s\},$$

the *stabilizer* of s. It is always a subgroup of G. The set

$$\{t \in S \mid (\exists \sigma \in G)(\sigma \cdot s = t)\}$$

is the *orbit* of s under the action, and it is denoted $\mathrm{O}_G(s)$.

(4) There is a one-to-one correspondence between the elements of the orbit of s and the left cosets of $\mathrm{St}(s)$ in G. Namely, if $H = \mathrm{St}(s)$, there are maps

$$\begin{aligned} \sigma H &\mapsto \sigma \cdot s \\ \sigma \cdot s &\mapsto \sigma H, \end{aligned}$$

for any left coset, σH. The first map is well-defined because if $\sigma H = \tau H$, then $\tau = \sigma h$ for some $h \in H$, and

$$\tau \cdot s = (\sigma h) \cdot s = \sigma \cdot (h \cdot s) = \sigma \cdot s$$

as $h \in \mathrm{St}(s)$. The reader should check that the second map is well-defined (DX).

If G is finite or $(G : \mathrm{St}(s))$ is finite (here, $(G : H)$ denotes the index of the subgroup H in G, *i.e.*, the number of (left) cosets of H in G), then $\mathrm{O}_G(s)$ is a finite set and when G is finite, $\#(\mathrm{O}_G(s))$ divides $\#(G)$.

(5) Say $t \in \mathrm{O}_G(s)$ and $H = \mathrm{St}(s)$. Write $t = \sigma \cdot s$. What is $\mathrm{St}(t)$?

We have $\tau \in \mathrm{St}(t)$ iff $\tau \cdot t = t$ iff $\tau \cdot (\sigma \cdot s) = \sigma \cdot s$ iff $(\sigma^{-1}\tau\sigma) \cdot s = s$ iff $\sigma^{-1}\tau\sigma \in H$ iff $\tau \in \sigma H \sigma^{-1}$. In conclusion, we see that $\mathrm{St}(\sigma \cdot s) = \sigma \mathrm{St}(s) \sigma^{-1}$, a conjugate subgroup of $\mathrm{St}(s)$.

(6) The reader can check that the relation $\sim$ on the set S defined by

$$s \sim t \quad \text{iff} \quad t = \sigma \cdot s \quad \text{for some } \sigma \in G$$

is an equivalence relation on S, and that the equivalence classes of this relation are exactly the distinct orbits $\mathrm{O}_G(s)$. Thus, given two orbits, $\mathrm{O}_G(s)$ and $\mathrm{O}_G(t)$, either $\mathrm{O}_G(s) \cap \mathrm{O}_G(t) = \emptyset$ or $\mathrm{O}_G(s) = \mathrm{O}_G(t)$. As a conclusion,

$$S = \bigcup_{\text{distinct orbits}}{\!\!\cdot}\ \mathrm{O}_G(s).$$

The *orbit space*, $G \setminus S$, is the quotient set $S/\sim$, *i.e.*, the collection of orbits, each considered as a distinct entity.

Obviously, we can define the notion of right action using a map $S \prod G \longrightarrow G$. It is obvious how to modify conditions (1) and (2) in Definition 1.1.

We now give some examples of group actions.

Example 1.1

(1) *Trivial action*. Let G be any group and S be any set. The action is

$$\sigma \cdot s = s,$$

that is, it leaves every element of S fixed.

(2) Let G be a group and H be a subgroup of G. Consider G as a set, H as a group, and the action $H \prod G \longrightarrow G$ given by

$$(\tau, s) \mapsto \tau \cdot s = \tau s \in G.$$

This action is called *translation*. Observe that

$$\mathrm{St}(s) = \{\tau \in H \mid \tau s = s\} = \{1\},$$

and

$$\begin{aligned} \mathrm{O}_H(s) &= \{t \in G \mid (\exists \sigma \in H)(\sigma \cdot s = t)\} \\ &= \{t \in G \mid (\exists \sigma \in H)(\sigma s = t)\} \\ &= Hs = \text{a right coset of } s. \end{aligned}$$

(3) Let G be a group and H be a subgroup of G. Consider G as a set, H as a group, and the action $H \prod G \longrightarrow G$ given by

$$(\tau, s) \mapsto \tau \cdot s = \tau s \tau^{-1} \in G.$$

This action is called *conjugation*. Note that

$$\begin{aligned} \mathrm{St}(s) &= \{\tau \in H \mid \tau s \tau^{-1} = s\} \\ &= \{\tau \in H \mid \tau s = s\tau\}, \end{aligned}$$

the collection of τ's in H which commute with s. When $H = G$, we see that $\mathrm{St}(s)$ is the *centralizer* of s in G, denoted $Z_G(s)$. For an arbitrary subgroup H of G, we get $\mathrm{St}(s) = Z_G(s) \cap H$. We also have

$$\mathrm{O}_H(s) = \{t \in G \mid (\exists \sigma \in H)(\sigma s \sigma^{-1} = t)\},$$

the *H-conjugacy class* of s, denoted $\mathrm{Cl}_H(s)$. When $H = G$, we get the *conjugacy class* of s, denoted $\mathrm{Cl}(s)$.

(4) Suppose the set S has some structure. Two very important special cases are:

(a) The set S is a vector space over a field. Then, we require $\theta\colon G \to \mathrm{Aut}(S)$ to land in the *linear* automorphisms of S, *i.e.*, in the invertible linear maps. In this case, our action is called a *(linear) representation* of G.

(b) The set S is an abelian group under addition, $+$. Then, we require $\theta\colon G \to \mathrm{Aut}(S)$ to land in the group of group automorphisms of S. Our action makes S into a *G-module*. Observe that in addition to the axioms (1) and (2) of Definition 1.1, a G-module action also satisfies the axiom

$$\sigma \cdot (a + b) = (\sigma \cdot a) + (\sigma \cdot b), \quad \text{for all } \sigma \in G \text{ and all } a, b \in S.$$

Now, assume that G is finite. Observe that the converse of Lagrange's theorem is false; namely, if G has order n and h divides n, then there isn't necessarily a subgroup of order h. Indeed, the group, A_4, of even permutations on four elements, has order 12 and $6 \mid 12$, yet A_4 has *no* subgroup of order 6. In 1872, Sylow (pronounce "Zŏloff") discovered the Sylow existence theorem and the classification theorem, known now as Sylow theorems I & II.

Theorem 1.1 *(Sylow, I) If G is a finite group of order g and p is a given prime number, then whenever $p^\alpha \mid g$ (with $\alpha \geq 0$), there exists a subgroup, H, of G of exact order p^α.*

To prove Theorem 1.1, we need an easy counting lemma. If m is an integer, write $\mathrm{ord}_p(m)$ for the maximal exponent to which p divides m (*i.e.*, $\mathrm{ord}_p(m) = \beta$ for the largest β such that $p^\beta \mid m$). The following simple properties hold (DX):

(1) $\mathrm{ord}_p(mn) = \mathrm{ord}_p(m) + \mathrm{ord}_p(n)$.

(2) $\mathrm{ord}_p(m \pm n) \geq \min\{\mathrm{ord}_p(m), \mathrm{ord}_p(n)\}$,
with equality if $\mathrm{ord}_p(m) = \mathrm{ord}_p(n)$.

(3) By convention, $\mathrm{ord}_p(0) = \infty$.

Lemma 1.2 *(Counting lemma) Let p be a prime, α, m positive integers. Then,*

$$\mathrm{ord}_p\binom{p^\alpha m}{p^\alpha} = \mathrm{ord}_p(m).$$

Proof. We know that

$$\binom{p^\alpha m}{p^\alpha} = \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - (p^\alpha - 1))}{p^\alpha(p^\alpha - 1)\cdots 2 \cdot 1}.$$

Observe that for $0 < i < p^\alpha$, we have (DX)

$$\mathrm{ord}_p(p^\alpha m - i) = \mathrm{ord}_p(p^\alpha - i).$$

Thus,

$$\binom{p^\alpha m}{p^\alpha} = mK, \quad \text{where } K \text{ is prime to } p.$$

Therefore,

$$\mathrm{ord}_p\binom{p^\alpha m}{p^\alpha} = \mathrm{ord}_p(m),$$

as contended. □

Proof of Sylow I. (Wielandt, 1959) If S is any subset of G, let

$$\sigma \cdot S = \{\sigma t \mid t \in S\},$$

and note that $\sigma \cdot S$ is a subset of the same cardinality of that of S. Let

$$\mathcal{S} = \{S \subseteq G \mid \#(S) = p^\alpha\}.$$

Note that in the above definition, S is *any* subset of G, and not necessarily a subgroup of G. Of course,

$$\#(\mathcal{S}) = \binom{p^\alpha m}{p^\alpha}.$$

The group G acts on $\mathcal{S}$ by translation, *i.e., via*, $S \mapsto \sigma \cdot S$.

Claim. There is some $S \in \mathcal{S}$ so that

$$\mathrm{ord}_p(\#(\mathrm{O}_G(S))) \leq \mathrm{ord}_p(m).$$

If not, then for all $S \in \mathcal{S}$, we have $\mathrm{ord}_p(\#(\mathrm{O}_G(S))) > \mathrm{ord}_p(m)$. But we know that $\mathcal{S}$ can be written as a disjoint union of G-orbits,

$$\mathcal{S} = \bigcup_{\text{distinct orbits}} \mathrm{O}_G(S).$$

So,

$$\#(\mathcal{S}) = \sum_{\text{distinct orbits}} \#(\mathrm{O}_G(S)).$$

Consequently,

$$\mathrm{ord}_p(\#(\mathcal{S})) \geq \min\{\mathrm{ord}_p(\#(\mathrm{O}_G(S)))\} > \mathrm{ord}_p(m).$$

But

$$\mathrm{ord}_p(\#(\mathcal{S})) = \mathrm{ord}_p\binom{p^\alpha m}{p^\alpha},$$

contradicting Lemma 1.2. This proves the claim.

Now, pick some $S \in \mathcal{S}$ so that $\mathrm{ord}_p(\#(\mathrm{O}_G(S))) \leq \mathrm{ord}_p(m)$. Let H be the stabilizer of S. We know that

(a) $\#(\mathrm{O}_G(S)) = (G : \mathrm{St}(S)) = (G : H)$.

(b) $p^\alpha m = \#(G) = \#(H)\#(\mathrm{O}_G(S))$.

From (b), applying the ord function, we get

$$\alpha + \mathrm{ord}_p(m) = \mathrm{ord}_p(\#(H)) + \mathrm{ord}_p(\#(\mathrm{O}_G(S))) \leq \mathrm{ord}_p(\#(H)) + \mathrm{ord}_p(m).$$

So, $\alpha \leq \mathrm{ord}_p(\#(H))$ and then, p^α divides $\#(H)$, and thus, $\#(H) \geq p^\alpha$. Now, H takes S elementwise to itself by translation, and for every $s \in S$,

$$\mathrm{St}(s) = \{\sigma \in H \mid \sigma s = s\} = \{1\}.$$

Therefore, $\#(H) = \#(\mathrm{O}_H(s))$ for every $s \in S$, and yet every orbit is contained in S. Thus,

$$\#(\mathrm{O}_H(s)) \leq \#(S) = p^\alpha,$$

from which we deduce that $\#(H) \leq p^\alpha$. We conclude that $\#(H) = p^\alpha$, and H is the required subgroup. □

Corollary 1.3 *(Original Sylow I) If p^β is the maximal power of p to divide $\#(G)$ and p is a prime number, then G possesses a subgroup of order p^β.*

The subgroups of maximal p-power order arising in Corollary 1.3 are called the *p-Sylow subgroups of G* (there can be more than one).

Corollary 1.4 *(Cauchy, 1840) Say G is a finite group and $p \mid \#(G)$, where p is a prime number. Then, there is some σ of order p in G.*

Nomenclature: A *p-group* is a finite group whose order is a power of the prime number p.

Corollary 1.5 *Say G is a p-group, with $\#(G) = p^r$. Then G possesses a descending chain*

$$G = G_0 > G_1 \cdots > G_{r-1} > G_r = \{1\},$$

so that $(G_i : G_{i+1}) = p$ for all i with $0 \leq i \leq r-1$. Hence, $\#(G_i) = p^{r-i}$.

Proof. By Sylow I, a subgroup G_1 of order p^{r-1} exists. An induction finishes the proof. □

Remark: It is not clear that G_{i+1} is normal in G_i. In fact, this is true, but it takes more work (see Proposition 1.10).

To prove Sylow II, we need the local embedding lemma. In order to state this lemma, we need to recall the concept of a normalizer. If $\mathcal{S}$ denotes the collection of all *subsets* of G, then G acts on $\mathcal{S}$ by conjugation: $S \mapsto \sigma S \sigma^{-1}$. This action preserves cardinality. For every $S \in \mathcal{S}$, we have

$$\mathrm{St}(S) = \{\sigma \in G \mid \sigma S \sigma^{-1} = S\}.$$

The group $\mathrm{St}(S)$ is called the *normalizer* of S in G, and it is denoted $N_G(S)$. If S is a subgroup of G, then S is normal in $N_G(S)$ (denoted $S \lhd N_G(S)$), and $N_G(S)$ is the biggest subgroup in which S is normal (DX).

The "philosophy" behind the local embedding lemma is that if P is any subgroup of a group G, then $N_G(P)$ is a "local neighborhood" of P in which P perhaps behaves nicely. We recall the following proposition which is used for proving Lemma 1.7.

Proposition 1.6 *Given a group G, for any two subgroups S and P, if $S \subseteq N_G(P)$, then $PS = SP$ is the subgroup of $N_G(P)$ generated by $S \cup P$, the subgroup P is normal in SP and $(SP)/P \cong S/(S \cap P)$.*

Proof. Since $S \subseteq N_G(P)$, we have $\sigma P \sigma^{-1} = P$ for all $\sigma \in S$, and thus, it clear that $SP = PS$. We have $\sigma\tau\sigma^{-1} \in P$ for all $\sigma \in S$ and all $\tau \in P$, and thus, for all $a, c \in S$ and all $b, d \in P$, we have

$$\begin{aligned} (ab)(cd) &= (ac)(c^{-1}bc)d \\ b^{-1}a^{-1} &= a^{-1}(ab^{-1}a^{-1}). \end{aligned}$$

The above identities prove that SP is a group. Since S and P contain the identity, this group contains S and P, and clearly any subgroup containing S and P contains SP. Therefore, SP is indeed the subgroup of $N_G(P)$ generated by $S \cup P$ and it is clear that P is normal in SP. Now, look at the composition φ of the injection $S \longrightarrow SP$ with the quotient map $SP \longrightarrow (SP)/P$. It is surjective, and $\varphi(\sigma) = \sigma P$ for every $\sigma \in S$. Thus, $\sigma \in \mathrm{Ker}\ \varphi$ iff $\sigma \in S \cap P$, and so $\mathrm{Ker}\ \varphi = S \cap P$, and the first isomorphism theorem yields
$(SP)/P \cong S/(S \cap P)$. □

After this short digression, we return to the main stream of the lecture.

Lemma 1.7 *(Local embedding lemma) Suppose that P is a p-Sylow subgroup of G. Then for every $\sigma \in N_G(P)$, if σ has p-power order then $\sigma \in P$. In particular, if H is a p-subgroup of $N_G(P)$, then $H \subseteq P$ and P is unique in $N_G(P)$.*

Proof. Let S be any p-subgroup of $N_G(P)$. Look at the group, H, generated by S and P in $N_G(P)$, denoted $\mathrm{Gp}\{S, P\}$. Since P is normal in $N_G(P)$, from Proposition 1.6, we have $H = SP = PS$, and $H/P = (SP)/P \cong S/(S \cap P)$. Thus,

$$(H : P) = (S : S \cap P),$$

and $(S : S \cap P)$ is a p-power, since S is a p-group. On the other hand, $(S : S \cap P)$ is prime to p, as $(G : P) = (G : H)(H : P)$ and $(G : P)$ is prime to p by definition of P. So, we must have $(H : P) = (S : S \cap P) = 1$, which implies that $H = P$. Thus, $S = S \cap P$, and $S \subseteq P$. We finish the proof by letting S be the cyclic p-group generated by σ. □

Theorem 1.8 *(Sylow II) If G is a finite group, write $\mathcal{S}\mathrm{yl}_p(G)$ for the collection of all p-Sylow subgroups of G, and $\mathcal{P}$ for the collection of* **all** *the p-subgroups of G, where p is a prime number. Then, the following hold:*

(1) $\mathrm{syl}_p(G) = \#(\mathcal{S}\mathrm{yl}_p(G)) \equiv 1 \,(mod\, p)$.

(2) For all $S \in \mathcal{P}(G)$ and all $P \in \mathcal{S}\mathrm{yl}_p(G)$, there is some $\sigma \in G$ so that $S \subseteq \sigma P \sigma^{-1}$. In particular, any two p-Sylow subgroups of G are conjugate in G.

(3) $\mathrm{syl}_p(G)$ divides $\#(G)$; in fact, $\mathrm{syl}_p(G)$ divides the prime to p part of $\#(G)$.

Proof. (1) The group G acts by conjugation on $\mathcal{S}\mathrm{yl}(G)$ (drop the subscript p in the course of this proof). So

$$\mathcal{S}\mathrm{yl}(G) = \bigcup_{\text{distinct orbits}}\!\!\!\cdot\ \ \mathrm{O}_G(P).$$

Any $S \in \mathcal{P}(G)$ also acts by conjugation on $\mathcal{S}\mathrm{yl}(G)$, and so

$$\mathcal{S}\mathrm{yl}(G) = \bigcup_{\text{distinct orbits}}\!\!\!\cdot\ \ \mathrm{O}_S(P).$$

What is $\mathrm{St}(P)$? We have

$$\mathrm{St}(P) = \{\sigma \in S \mid \sigma P \sigma^{-1} = P\} = S \cap N_G(P).$$

But S has p-power order, so $S \cap N_G(P)$ is a p-subgroup of $N_G(P)$. The embedding lemma implies that $S \cap N_G(P) \subseteq P$, from which we deduce that $S \cap N_G(P) = S \cap P$. So,

$$\#(\mathrm{O}_S(P)) = (S : S \cap P).$$

Now, take for S one of the p-Sylow subgroups, say P. Then, $\#(\mathrm{O}_P(Q)) = (P : P \cap Q)$. If $Q \neq P$, then $P \cap Q < P$, and so, $(P : P \cap Q)$ is a nontrivial p-power (*i.e*, not equal to 1). If $P = Q$, then $(P : P \cap Q) = 1$. Therefore, in the orbit decomposition

$$\mathcal{S}\mathrm{yl}(G) = \bigcup_{\substack{\text{distinct orbits} \\ Q \in \mathcal{S}\mathrm{yl}(G)}}\!\!\!\cdot\ \ \mathrm{O}_P(Q),$$

one orbit has cardinality 1, the rest having nontrivial p-power cardinalities. We conclude that

$$\#(\mathcal{S}\mathrm{yl}(G)) = 1 + \sum p\text{-powers},$$

and $\mathrm{syl}_p(G) = \#(\mathcal{S}\mathrm{yl}_p(G)) \equiv 1 \pmod{p}$, as claimed.

(2) Let $S \in \mathcal{P}(G)$ and look at $\mathrm{O}_G(P)$ where $P \in \mathcal{S}\mathrm{yl}(G)$. The subgroup S acts by conjugation on $\mathrm{O}_G(P)$. So, we have

$$\mathrm{O}_G(P) = \bigcup_{\substack{\text{distinct orbits} \\ Q \in \mathrm{O}_G(P)}}\!\!\!\cdot\ \ \mathrm{O}_S(Q). \tag{$*$}$$

If $Q \in \mathrm{O}_G(P)$, then consider the stabilizer of Q *in* S,

$$\mathrm{St}(Q) = \{\sigma \in S \mid \sigma Q \sigma^{-1} = Q\} = S \cap N_G(Q).$$

As before, by the embedding lemma, $S \cap N_G(Q) = S \cap Q$. Then, $\#(\mathrm{O}_S(Q)) = (S : S \cap Q)$. Take $S = P$ itself. If $Q = P$, then $(P : P \cap P) = 1$ and $\#(\mathrm{O}_P(P)) = 1$. On the other hand, if $P \neq Q$, then $(P : P \cap Q)$ is a nontrivial p-power. Thus, as before, using $(*)$, we deduce that

$$\#(\mathrm{O}_G(P)) \equiv 1 \pmod{p}.$$

Assume that (2) is false. Then, there exist some S and some P such that $S \not\subseteq \sigma P \sigma^{-1}$ for *any* $\sigma \in G$. Let this S act on $\mathrm{O}_G(P)$, for this P. But we have

$$\#(\mathrm{O}_G(P)) = \sum_{\substack{\text{distinct orbits} \\ Q \in \mathrm{O}_G(P)}} \#(\mathrm{O}_S(Q)), \tag{$**$}$$

and $\#(\mathrm{O}_S(Q)) = (S\colon S \cap Q)$ where Q is a conjugate of P, so that $S \not\subseteq Q$, and therefore $(S : S \cap Q)$ is a nontrivial p-power. Then, $(**)$ implies

$$\#(\mathrm{O}_G(P)) \equiv 0 \,(\mathrm{mod}\, p),$$

a contradiction. Thus, neither S nor P exist and (2) holds.

(3) By (2), $\mathcal{S}\mathrm{yl}(G) = \mathrm{O}_G(P)$, for some fixed P. But the size of an orbit divides the order of the group. The rest is clear. □

Theorem 1.9 *(Sylow III) If G is a finite group and P is a p-Sylow subgroup of G, then $N_G(N_G(P)) = N_G(P)$.*

Proof. Let $T = N_G(N_G(P))$ and $S = N_G(P)$, so that $T = N_G(S)$ and $S \lhd T$.

Claim. For every $\sigma \in T$, if σ has p-power order then $\sigma \in P$.

The order of T/S is $(T : S)$. But

$$(G : P) = (G : T)(T : S)(S : P)$$

and $(G : P)$ is prime to p by definition of P. So, $(T : S)$ is prime to p. Consider $\overline{\sigma}$, the image of σ in T/S. The element $\overline{\sigma}$ has p-power order, yet $\#(T/S)$ is prime to p. Thus, $\overline{\sigma} = 1$, and so, $\sigma \in S$. The local embedding lemma yields $\sigma \in P$. Therefore, if H is a p-subgroup of T, we have $H \subseteq P$. Thus, any p-Sylow subgroup, H, of T is contained in P; but since H has maximal p-size, $H = P$. This implies that T has a single p-Sylow subgroup, namely P. By Sylow II, the group P is normal in T and so $T \subseteq N_G(P) = S$. Yet, $S \subseteq T$, trivially, and $S = T$. □

Remark: A p-Sylow subgroup is unique iff it is normal in G.

Definition 1.2 A group, G, is *simple* if and only if it possesses no nontrivial normal subgroups ($\{1\}$ and G itself are the two trivial normal subgroups).

Example 1.2

(1) Assume that G is a group of order pq, with p and q prime and $p < q$. Look at the q-Sylow subgroups. Write $\mathrm{syl}(q)$ for the number of q-Sylow subgroups of G. We know that

$$\mathrm{syl}(q) \equiv 1 \,(\mathrm{mod}\, q) \quad \text{and} \quad \mathrm{syl}(q) \mid p.$$

This implies that $\mathrm{syl}(q) = 1, p$. But $p < q$, so that $p \equiv p \,(\mathrm{mod}\, q)$, and the only possibility is $\mathrm{syl}(q) = 1$. Therefore, the unique q-Sylow subgroup is normal, and G is *not* simple.

(2) Assume that G is a group of order pqr, with p, q, r prime and $p < q < r$. Look at the r-Sylow subgroups. We must have

$$\mathrm{syl}(r) \equiv 1 \,(\mathrm{mod}\, r) \quad \text{and} \quad \mathrm{syl}(r) \mid pq.$$

This implies that $\mathrm{syl}(r) = 1, p, q, pq$. Since $p < r$ and $q < r$, as above, p and q are ruled out, and $\mathrm{syl}(r) = 1, pq$.

Suppose that $\mathrm{syl}(r) = pq$. We see immediately that $r < pq$. Now, each r-Sylow subgroup is isomorphic to $\mathbb{Z}/r\mathbb{Z}$ (cyclic of prime order), and any two distinct such subgroups intersect in the identity (since, otherwise, they would coincide). Hence, there are $pq(r-1)$ elements of order r. We shall now show that if $\mathrm{syl}(r) = pq$, then $\mathrm{syl}(q) = 1$. Assume that $\mathrm{syl}(r) = pq$ and look at the q-Sylow subgroups of G. We have

$$\mathrm{syl}(q) \equiv 1 \,(\mathrm{mod}\, q) \quad \text{and} \quad \mathrm{syl}(q) \mid pr.$$

This implies that $\mathrm{syl}(q) = 1, p, r, pr$ and, as before, p is ruled out since $p < q$. So, $\mathrm{syl}(q) = 1, r, pr$. Suppose that $\mathrm{syl}(q) = r$ or $\mathrm{syl}(q) = pr$, and call it x. Reasoning as before but now on the q-Sylow subgroups, we see

that there are $x(q-1)$ elements of order q. Now, $q-1 \geq p$ and $x \geq r$. Thus, there are at least rp elements of order q. But $r > q$, so there are more than pq elements of order q. Now, since there are $pq(r-1)$ elements of order r and more than pq elements of order q, there are more than

$$pq(r-1) + pq = pqr - pq + pq = pqr$$

elements in G, a contradiction. So, either the r-Sylow subgroup is normal in G (which is the case when $r > pq$) or the q-Sylow subgroup is normal in G. In either case, G is *not* simple.

Cases (1) and (2) have the following generalizations:

(a) Frobenius (1890's) showed that if $\#(G) = p_1 p_2 \cdots p_t$, a product of *distinct* primes, then G is *not* simple. The proof uses group representations and characters.

(b) Burnside (1901) proved the "$p^a q^b$-theorem": If $\#(G) = p^a q^b$, where p, q are distinct primes and $a, b \in \mathbb{N}$, then G is *not* simple. There are three known proofs, all hard, and all but one use group representations.

Obvious generalizations of (a) and (b) are *false*. The easiest case is $\#(G) = 2^2 \cdot 3 \cdot 5 = 60$. Indeed, the alternating group, A_5, is simple. After proving (b), Burnside conjectured (*circa* 1902) that every nonabelian group of odd order is *not* simple. This conjecture was proved in 1961 by W. Feit and J. Thompson. The proof is **very** hard, and very long (over 200 pages).

A piece of the proof of (a) and (b) is the following proposition:

Proposition 1.10 *If G is a finite group and p is the smallest prime number which divides the order of G, then any subgroup, H, of index p is automatically normal in G.*

Proof. Take H so that $(G : H) = p$. Consider the set $\mathcal{S} = \{H_1 = H, H_2, \ldots, H_p\}$ of cosets of H in G. The group G acts on $\mathcal{S}$ by translation,

$$\sigma \cdot H_j = \sigma H_j = H_l, \quad \text{for some } l, \text{ with } 1 \leq l \leq p.$$

This action is nontrivial, that is, we get a nontrivial homomorphism $\theta\colon G \to \mathfrak{S}_p$ (where $\mathfrak{S}_p \cong \mathrm{Aut}(\mathcal{S})$ is the group of permutations on p elements), and $\mathrm{Im}\ \theta \neq \{1\}$. We shall prove that $H = \mathrm{Ker}\ \theta$, which yields $H \lhd G$.

Observe that $\#(G) = \#(\mathrm{Ker}\ \theta) \cdot \#(\mathrm{Im}\ \theta)$. We must have

(1) $\#(\mathrm{Im}\ \theta) \mid p!$

(2) $\#(\mathrm{Im}\ \theta) \mid \#(G)$.

But $\#(G) = p^\alpha K$, where K contains primes greater than p. Therefore, $\#(\mathrm{Im}\ \theta) = p^a J$, where $J = 1$ or J contains primes greater than p. If $J \neq 1$, then J contains some prime $q > p$, and since $p^\alpha J$ divides $p! = p(p-1)\cdots 2 \cdot 1$, the prime q must divide $p!$. Since q is prime, q must divide one of the terms in $p!$, which is impossible, since $q > p$. We conclude that $J = 1$. Now, $a \geq 1$ since $\mathrm{Im}\ \theta$ is nontrivial. If $a \geq 2$, since $p^{a-1} \mid (p-1)\cdots 2 \cdot 1$, the prime p should divide $p - j$, for some j with $1 \leq j \leq p-1$. However, this is impossible, and so, $a = 1$. Therefore, $\#(\mathrm{Im}\ \theta) = p$ and $(G : \mathrm{Ker}\ \theta) = p$. Note that $\sigma \in \mathrm{Ker}\ \theta$ iff σ acts trivially on $\mathcal{S}$ iff $\sigma\tau H = \tau H$ iff $\tau^{-1} H \tau = H$ iff $\tau^{-1}\sigma\tau \in H$ for all τ iff $\sigma \in \tau H \tau^{-1}$ for all $\tau \notin H$ iff

$$\sigma \in \bigcap_{\tau \in G} \tau H \tau^{-1}.$$

We deduce that

$$\mathrm{Ker}\ \theta = \bigcap_{\tau \in G} \tau H \tau^{-1} \subseteq H.$$

As $(G : \text{Ker } \theta) = p = (G : H)$ and $\text{Ker } \theta \subseteq H$, we get $H = \text{Ker } \theta$, and H is indeed normal in G. $\square$

Note that we can now improve Corollary 1.5 as follows: If G is a p-group with $\#(G) = p^r$, then there is a descending chain of subgroups

$$G = G_0 > G_1 > \cdots > G_r = \{1\},$$

where each G_{j+1} is normal in G_j and each quotient G_{j+1}/G_j is simple; so, $G_{j+1}/G_j = \mathbb{Z}/p\mathbb{Z}$, a cyclic group of order p.

Definition 1.3 A *composition series* for a group G is a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_t = \{1\}$$

in which each subgroup G_{j+1} is maximal, normal in G_j. The factor groups G/G_1, $G_1/G_2, \ldots, G_{t-1}/G_t = G_{t-1}$ are called the *composition factors* of the given composition series and each one is a simple group.

Remark: Every finite group possesses a composition series (DX).

Not every group possesses maximal subgroups, even maximal normal subgroups (such groups must be infinite).

However, finitely generated groups do possess maximal subgroups, but because such groups can be infinite, the proof requires a form of transfinite induction known as Zorn's lemma. Since this lemma is an important tool, we briefly digress to state the lemma and illustrate how it is used.

Recall that a *partially ordered set* or *poset* is a pair, $(S, \leq)$, where S is a set and $\leq$ is a *partial order* on S, which means that $\leq$ is a binary relation on S satisfying the properties: For all $a, b, c \in S$, we have:

(1) $a \leq a$ (reflexivity)

(2) If $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity)

(3) If $a \leq b$ and $b \leq a$, then $a = b$. (antisymmetry)

Observe that given $a, b \in S$, it may happen that neither $a \leq b$ nor $b \leq a$. A *chain*, C, in S is a linearly ordered subset of S (which means that for all $a, b \in C$, either $a \leq b$ or $b \leq a$). The empty set is considered a chain. An element, $b \in S$, is an *upper bound* of C (resp. a *lower bound* of C) if $a \leq b$ for all $a \in C$ (resp. $b \leq a$ for all $a \in C$). Note that an upper bound of C (resp. a lower bound of C) *need not* belong to C. We say that $C \subseteq S$ is *bounded above* if it possesses some upper bound (in S) (resp. *bounded below* if it possesses some lower bound (in S)). The notion of least upper bound (resp. greatest lower bound) of a chain is clear as is the notion of least or greatest element of a chain. These need not exist. A set, S, which is a chain, is *well ordered* iff every nonempty subset of S has a least element.

Remark: Obviously, the notions of upper bound (resp. lower bound), maximal (resp. minimal) element, greatest (resp. smallest) element, all make sense for arbitrary subsets of a poset, and not just for chains. Some books define a well ordered set to be a poset so that every nonempty subset of S has a least element. Thus, it is not required that S be a chain, but it is required that *every* nonempty subset have a least element, not just chains. It follows that a well ordered set (under this new definition) is necessarily a chain. Indeed, for any two elements $a, b \in S$, the subset $\{a, b\}$ must have a smallest element, so, either $a \leq b$ or $b \leq a$.

Hausdorff maximal principle: Every nonempty poset possesses a maximal chain.

From set theory, it is known that Hausdorff's maximal principle is equivalent to the axiom of choice, which is also equivalent to Zermelo's well ordering principle (every nonempty subset can be well ordered).

We say that a poset is *inductive* iff every nonempty chain possesses a least upper bound.

Zorn's lemma: Each inductive poset possesses a maximal element.

Proof. By Hausdorff. □

Remark: Some books define a poset to be inductive iff every nonempty chain is bounded above. Zorn's lemma still holds under this slightly weaker assumption. In practice, this makes little difference, because when proving that a chain is bounded above, one usually shows that this chain has a least upper bound.

Here are two illustrations of the use of Zorn's lemma.

Theorem 1.11 *Every finitely generated group, G, possesses a maximal subgroup.*

Proof. Consider the set, $\mathcal{S}$, of all proper subgroups, H, of G. Partially order $\mathcal{S}$ by inclusion (i.e., $H \leq K$ iff $H \subseteq K$). Let $\{H_\alpha\}$ be a chain in $\mathcal{S}$. If $H = \bigcup_\alpha H_\alpha$, we see that H is a group and that it is the least upper bound of $\{H_\alpha\}$. We must show that $H \neq G$. If $H = G$, then as G is finitely generated, $H = G = \mathrm{Gp}\{\sigma_1, \ldots, \sigma_t\}$, with $\sigma_i \in H$ for $i = 1, \ldots, t$. This means that, for each i, there is some α_i so that $\sigma_i \in H_{\alpha_i}$. Since $\{H_\alpha\}$ is a chain, there is some s so that $H_{\alpha_j} \subseteq H_{\alpha_s}$ for $j = 1, \ldots, t$. Thus, $\sigma_1, \ldots, \sigma_t \in H_{\alpha_s}$, and so, $H_{\alpha_s} = G$, contradicting the fact that $H_{\alpha_s} \neq G$. Therefore, $\mathcal{S}$ is inductive, and consequently, by Zorn's lemma, it possesses a maximal element. Such an element is a maximal subgroup of G. □

As a second illustration of Zorn's lemma, we prove that every vector space has a Hamel basis. Given a vector space, V, over a field, k, a *Hamel basis* of V is a family, $\{e_\alpha\}_{\alpha \in \Lambda}$, so that:

(1) For every $v \in V$, there exists a finite subset of Λ, say I, and some elements of k for these α's in I, say c_α, so that
$$v = \sum_{\alpha \in I} c_\alpha e_\alpha.$$

(2) The e_α's are linearly independent, *i.e.*, given any finite subset I of Λ, if $\sum_{\alpha \in I} c_\alpha e_\alpha = 0$, then $c_\alpha = 0$, for all $\alpha \in I$.

Theorem 1.12 *Every vector space, V, possesses a Hamel basis.*

Proof. Let $\mathcal{S}^*$ be the collection of all subspaces, W, of V which possess a Hamel basis, together with a choice of a basis. Write $(W, \{e_\alpha\})$ for any element of $\mathcal{S}^*$. The collection, $\mathcal{S}^*$, is nonempty, since finitely dimensional vector spaces have bases. Partially order $\mathcal{S}^*$ by $(W, \{e_\alpha\}) \leq (\widetilde{W}, \{f_\beta\})$ iff

(a) $W \subseteq \widetilde{W}$ and

(b) $\{e_\alpha\} \subseteq \{f_\beta\}$, which means that the basis $\{f_\beta\}$ extends the basis $\{e_\alpha\}$.

We claim that $\mathcal{S}^*$ is inductive.

Given a chain, $\{W^{(\lambda)}, \{e_\alpha^{(\lambda)}\})$, in $\mathcal{S}^*$, take
$$W = \bigcup_\lambda W^{(\lambda)} \quad \text{and} \quad \{e_\gamma\} = \bigcup_\lambda \{e_\alpha^{(\lambda)}\} \subseteq W.$$

The reader should check that $\{e_\gamma\}$ is a basis for W (DX); therefore, $(W, \{e_\gamma\})$ is the least upper bound of our chain. By Zorn's lemma, there exists a maximal element of $\mathcal{S}^*$, call it $(W_0, \{e_\gamma\})$. We need to show that $W_0 = V$. If not, there is some $v \in V$ with $v \notin W_0$. Consider the subspace
$$Z = W_0 \amalg kv = \{w + \xi v \mid w \in W_0, \xi \in k\}.$$

The subspace, Z, strictly contains W_0 and $\{e_\gamma\} \cup \{v\}$ is a Hamel basis for Z (DX). However, this contradicts the maximality of W_0. Therefore, $W_0 = V$. □

Corollary 1.13 *If W is a subspace of V and $\{e_\alpha\}$ is a Hamel basis for W, then there exists a Hamel basis of V extending $\{e_\alpha\}$.*

Application: The field, $\mathbb{R}$, is a vector space over $\mathbb{Q}$, and $1 \in \mathbb{Q}$ is a Hamel basis for $\mathbb{Q}$. We can extend this basis of $\mathbb{Q}$ to a Hamel basis for $\mathbb{R}$ (over $\mathbb{Q}$), call it $\{e_\alpha\}_{\alpha\in\Lambda}$, and say, $e_0 = 1$; then, $\mathbb{R}/\mathbb{Q}$ is a vector space (over $\mathbb{Q}$) spanned by the e_α other than e_0. So, we have

$$\mathbb{R}/\mathbb{Q} \cong \coprod_{\alpha\in\Lambda,\alpha\neq 0} \mathbb{Q}.$$

1.3 Elementary Theory of p-Groups

Recall that for a group G, the *center* of G, denoted $Z(G)$, is given by

$$Z(G) = \{\sigma \in G \mid (\forall \tau \in G)(\sigma\tau = \tau\sigma)\}.$$

We write $[\sigma, \tau]$ for the element $\sigma\tau\sigma^{-1}\tau^{-1}$, called the *commutator of* σ *and* τ. Observe that $[\tau, \sigma] = [\sigma, \tau]^{-1}$. Also,

$$Z(G) = \{\sigma \in G \mid (\forall \tau \in G)([\sigma, \tau] = 1)\}$$

and $Z(G)$ is the centralizer of G under conjugation.

Let G act on itself by conjugation. When do we have $\mathrm{O}_G(\sigma) = \{\sigma\}$? This happens when

$$(\forall \tau \in G)(\tau\sigma\tau^{-1} = \sigma) \quad \text{i.e.} \quad (\forall \tau \in G)(\tau\sigma\tau^{-1}\sigma^{-1} = [\tau, \sigma] = 1).$$

Thus, $\sigma \in Z(G)$ iff $\mathrm{O}_G(\sigma) = \{\sigma\}$.

Remark: Obviously,

$$Z(G) = \bigcap_{\sigma \in G} Z_G(\sigma).$$

Moreover, it is obvious that $\sigma \in Z_G(\sigma)$ for every $\sigma \in G$. Thus, for every $\sigma \notin Z(G)$, we have $Z(G) < Z_G(\sigma)$ (obviously, $Z_G(\sigma) = G$ if $\sigma \in Z(G)$.) Therefore, if G is nonabelian, then $Z(G) < Z_G(\sigma)$ for all $\sigma \in G$.

Proposition 1.14 *The center, $Z(G)$, of a p-group, G, is nontrivial.*

Proof. If we let G act on itself by conjugation, we know that G is the disjoint union of distinct orbits, and since $\mathrm{O}_G(\sigma)$ is the conjugacy class of σ and $\sigma \in Z(G)$ iff $\mathrm{O}_G(\sigma) = \{\sigma\}$, we get

$$G = Z(G) \cup \bigcup_{\substack{\text{distinct orbits} \\ \tau \notin Z(G)}} \mathrm{O}_G(\tau).$$

Consequently, using the fact that $\#(\mathrm{O}_G(\tau)) = (G : \mathrm{St}(\tau))$, we get

$$\#(G) = \#(Z(G)) + \sum_{\substack{\text{distinct orbits} \\ \tau \notin Z(G)}} (G : \mathrm{St}(\tau)). \tag{$*$}$$

But $\#(G) = p^r$, so that each term $(G : \mathrm{St}(\tau))$ for $\tau \notin Z(G)$ is a nontrivial p-power. So, in $(*)$, all terms must be divisible by p. Therefore, $p \mid \#(Z(G))$. $\square$

Note that $Z(G)$ is normal in G. Thus, $G/Z(G)$ is a p-group of strictly smaller order, providing a basis for induction proofs.

We make the following provisional definition (due to E. Galois, 1832). A finite group, G, is *solvable* iff it possesses a composition series all of whose factors are abelian, or equivalently iff it possesses a composition series all of whose factors are cyclic of prime order.

We have shown that a p-group is solvable.

Remark: The above definition is provisional because it only works for finite group (c.f. Definition 1.7), but the concept of a solvable group can be defined for an arbitrary group.

Corollary 1.15 *Every p-group of order less than or equal to p^2 is abelian.*

Proof. Since $\#(G) = 1, p, p^2$ and G is obviously abelian in the first two cases, we may assume that $\#(G) = p^2$. We know that $Z(G)$ is non-trivial and we must prove that $Z(G) = G$. If $Z(G) < G$, then there is some $\sigma \in G$ so that $\sigma \notin Z(G)$. Clearly, $Z(G) \subseteq Z_G(\sigma)$ (where $Z_G(\sigma)$ denotes the centralizer of σ in G). But $\sigma \in Z_G(\sigma)$ implies that $(Z_G(\sigma) : Z(G)) \geq p$ and since $Z(G)$ is nontrivial, we must have $Z_G(\sigma) = G$. So, $\sigma \in Z(G)$, a contradiction. □

We now consider a nice property possessed by p-groups called *property (N)*. If G is any group, G *has property (N)* iff for every proper subgroup, H, of G, the group H is a proper subgroup of $N_G(H)$.

Remark: An abelian group has (N). Indeed, every subgroup of an abelian group is normal, and so, $N_G(H) = G$.

Proposition 1.16 *Every p-group has (N).*

Proof. We proceed by induction on $\#(G) = p^r$. Corollary 1.15 takes care of the base case of the induction. Next, let $\#(G) = p^{r+1}$ and assume that the induction hypothesis holds up to r. We know that $Z(G)$ is nontrivial, and so $\#(G/Z(G)) \leq p^r$. Thus, $G/Z(G)$ has (N). Pick H, any proper subgroup of G. Of course, $Z(G) \subseteq N_G(H)$, and we may assume that $Z(G) \subseteq H$ (since, otherwise, it is clear that $H < N_G(H)$). By the second homomorphism theorem, the question: $H < N_G(H)$? is reduced to the question: $\overline{H} < \overline{N_G(H)}$?, where the bar means pass to $G/Z(G)$. But in this case, as $Z(G) \subseteq H$, we see that (DX)

$$\overline{N_G(H)} = N_{\overline{G}}(\overline{H}),$$

and we just remarked that $\overline{G} = G/Z(G)$ has (N). Therefore, $N_{\overline{G}}(\overline{H}) > \overline{H}$, and so, $\overline{N_G(H)} > \overline{H}$, as desired. □

Groups that have property (N) tend to have good properties. Here are a few of them.

Proposition 1.17 *Say G is a finite group having (N), then each of its p-Sylow subgroups is unique and normal in G. Every maximal subgroup of G is also normal and has prime index.*

Proof. Look at P, a p-Sylow subgroup of G. Now, if $N_G(P) \neq G$, then by (N), we have $N_G(N_G(P)) > N_G(P)$, a contradiction to Sylow III. Thus, $N_G(P) = G$ and so, $P \lhd G$. Next, let H be a maximal subgroup. By (N), we have $N_G(H) > H$, yet H is maximal, so $N_G(H) = G$, and $H \lhd G$. It follows that G/H is a group with no nontrivial subgroup. But then, G/H is cyclic of prime order. □

Proposition 1.18 *Say G is a finite group and suppose that*

(a) $g = \#(G) = p_1^{a_1} \cdots p_t^{a_t}$ (where the p_i's are distinct primes)

(b) G has (N).

Write P_j for the p_j-Sylow subgroup of G. Then, the map

$$P_1 \prod \cdots \prod P_t \xrightarrow{\varphi} G$$

via $\varphi(\sigma_1, \ldots, \sigma_t) = \sigma_1 \cdots \sigma_t$ is an isomorphism of groups. Hence, G is isomorphic to a product of p-groups.

The proof depends on the following lemma:

Lemma 1.19 *Let G be a group and let H and K be normal subgroups of G. If $H \cap K = \{1\}$, then every element of H commutes with every element of K. Suppose that σ and τ are commuting elements in G, with orders r and s respectively. If r and s are relatively prime then the order of $\sigma\tau$ is rs.*

Proof. Look at $[\sigma, \tau]$, where $\sigma \in H$ and $\tau \in K$. We have

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}).$$

Now, $\sigma\tau\sigma^{-1} \in K$, since $K \lhd G$. Thus, $(\sigma\tau\sigma^{-1})\tau^{-1} \in K$. Similarly, $\sigma(\tau\sigma^{-1}\tau^{-1}) \in H$. But $H \cap K = \{1\}$, and since we just proved that $[\sigma, \tau] \in H \cap K$, we have $[\sigma, \tau] = 1$. The second part of the lemma is left to the reader (DX). □

Proof of Proposition 1.18. By Proposition 1.17, each p_j-Sylow subgroup P_j is normal in G. First, we claim that the map $P_1 \prod \cdots \prod P_t \xrightarrow{\varphi} G$ is a group homomorphism. Now, because the orders of P_i and P_j are relatively prime if $i \neq j$, we have $P_i \cap P_j = \{1\}$. Since

$$\varphi((\sigma_1, \ldots, \sigma_t)(\tau_1, \ldots, \tau_t)) = \sigma_1\tau_1 \cdots \sigma_t\tau_t,$$

using Lemma 1.19, we can push each τ_j past $\sigma_{j+1} \cdots \sigma_t$, and we get

$$\varphi((\sigma_1, \ldots, \sigma_t)(\tau_1, \ldots, \tau_t)) = \sigma_1 \cdots \sigma_t\tau_1 \cdots \tau_t = \varphi(\sigma_1, \ldots, \sigma_t)\varphi(\tau_1, \ldots, \tau_t),$$

proving that φ is a homomorphism. The kernel of φ consists of those $\sigma = (\sigma_1, \ldots, \sigma_t)$ so that $\sigma_1 \cdots \sigma_t = 1$, or equivalently, $\sigma_t^{-1} = \sigma_1 \cdots \sigma_{t-1}$. Using Lemma 1.19 and an obvious induction, the order on the righthand side is $p_1^{l_1} \cdots p_{t-1}^{l_{t-1}}$ and the order on the left hand side in $p_t^{l_t}$, which implies that $l_1 = \cdots = l_t$, and thus, all $\sigma_j = 1$. Therefore, Ker $\varphi = \{1\}$ and φ is injective. One more application of Lemma 1.19 yields $\#(P_1 \prod \cdots \prod P_t) = g$. Since φ is injective, it is an isomorphism. □

Remark: The proof of Proposition 1.18 only uses the fact that every p-Sylow subgroup is normal in G.

Definition 1.4 Let G be any group, then the *Frattini subgroup* of G, denoted $\Phi(G)$, is the intersection of all the maximal proper subgroups of G. In case G has no maximal proper subgroup, we set $\Phi(G) = G$.

Remark: The additive abelian group $(\mathbb{Q}, +)$ has no maximal proper subgroup.

Definition 1.5 In a group, G, an element σ is a *non-generator* iff for every subset, A, if $G = \mathrm{Gp}\{A, \sigma\}$, then $G = \mathrm{Gp}\{A\}$ (where $\mathrm{Gp}\{A\}$ denotes the subgroup of G generated by A).

As an example, assume that G is a cyclic group of order p^r. Then, $\Phi(G)$ is the cyclic subgroup of order p^{r-1}.

Proposition 1.20 *The Frattini subgroup of G is a characteristic subgroup of G, i.e., for every automorphism, $\varphi \in \mathrm{Aut}(G)$, we have $\varphi(\Phi(G)) = \Phi(G)$. In particular, $\Phi(G)$ is normal in G. Furthermore, if G is finite, then*

$$\Phi(G) = \{\sigma \in G \mid \sigma \textit{ is a non-generator}\}.$$

Proof. Every automorphism permutes the collection of maximal subgroups of G. Therefore, $\Phi(G)$ is characteristic. Now assume G is finite, or, at least, that every proper subgroup is contained in a maximal subgroup.

Claim: If $\mathrm{Gp}\{A, \Phi(G)\} = G$, then $\mathrm{Gp}\{A\} = G$.

If not, $\mathrm{Gp}\{A\} \neq G$, and so, there exists a maximal subgroup, M, containing $\mathrm{Gp}\{A\}$. Now, $\Phi(G) \subseteq M$, therefore, $\mathrm{Gp}\{A, \Phi(G)\} \subseteq M \neq G$, a contradiction. This proves that $\Phi(G)$ is contained in the set of non-generators.

Conversely, assume that σ is a non-generator. Were $\sigma \notin \Phi(G)$, we would have a maximal subgroup, M, with $\sigma \notin M$. Take $M = A$ in the definition of a non-generator. Look at $\mathrm{Gp}\{M, \sigma\}$. Of course, $M \subseteq \mathrm{Gp}\{M, \sigma\}$ and $\sigma \in \mathrm{Gp}\{M, \sigma\}$, so $M < \mathrm{Gp}\{M, \sigma\}$. But M is maximal, and so, $\mathrm{Gp}\{M, \sigma\} = G$. By definition (since σ is a non-generator), $G = \mathrm{Gp}\{M\}$, and thus, $G = M$, a contradiction. □

Definition 1.6 A group G is an *elementary abelian p-group* iff

(1) It is abelian, and

(2) For every $\sigma \in G$, we have $\sigma^p = 1$.

Remark: Any elementary abelian p-group is, in a natural way, a vector space over $\mathbb{F}_p$. Conversely, for any vector space over the finite field $\mathbb{F}_p$, its additive group is an elementary abelian p-group. Under this correspondence, an endomorphism of G goes over to a linear map and an automorphism of G goes to an invertible linear map. The group G is finite iff the corresponding vector space is finite dimensional.

(Given G, write the group operation additively. Thus, we have

$$p \cdot \sigma = \underbrace{\sigma + \cdots + \sigma}_{p} = 0.$$

The finite field $\mathbb{F}_p$ acts on G as follows: If $\lambda \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, *i.e.*, $\lambda \equiv 0, 1, \ldots, p-1 \pmod p$, we set

$$\lambda \cdot \sigma = \underbrace{\sigma + \cdots + \sigma}_{\lambda \pmod p \text{ times}}.$$

The reader should check that scalar multiplication is indeed well defined and that the facts asserted in the previous remark are true (DX).)

Proposition 1.21 *For any p-group, G, the quotient group, $G/\Phi(G)$, is an elementary abelian p-group.*

Proof. Say H is a maximal subgroup of G. Since G has (N), the group, H, is normal in G and $(G : H) = p$. Therefore, G/H is cyclic of order p. Write $\overline{\sigma}$ for the image of σ in G/H. We know that $(\overline{\sigma})^p = 1$. So, $\overline{\sigma^p} = 1$, *i.e.*, $\sigma^p \in H$. But H is arbitrary, and so,

$$\sigma^p \in \bigcap_{H \text{ maximal}} H = \Phi(G).$$

Now, G/H is abelian since $G/H = \mathbb{Z}/p\mathbb{Z}$. This implies that $[G, G] \subseteq H$ (here $[G, G]$ is the subgroup of G generated by the commutators, called the *commutator group of* G; it is the smallest normal subgroup, K, of G such that G/K is abelian). Since H is arbitrary, we get

$$[G, G] \subseteq \bigcap_{H \text{ maximal}} H = \Phi(G).$$

This shows that $G/\Phi(G)$ is abelian. As $\sigma^p \in \Phi(G)$, we get $(\overline{\overline{\sigma}})^p = 1$ in $G/\Phi(G)$, where $\overline{\overline{\sigma}}$ is the image of σ in $G/\Phi(G)$. □

We now come to a famous theorem of Burnside.

Theorem 1.22 *(Burnside Basis Theorem) Say G is a p-group and let d be the minimal number of elements found among all minimal generating sets for G. The following properties hold:*

(1) Given any set of d elements in G, say $\sigma_1, \ldots, \sigma_d$, they generate G iff $\overline{\sigma_1}, \ldots, \overline{\sigma_d}$ are a basis of $G/\Phi(G)$.

(2) More generally, any set of t elements $\sigma_1, \ldots, \sigma_t$ in G generates G iff $\{\overline{\sigma_1}, \ldots, \overline{\sigma_t}\}$ spans $G/\Phi(G)$. Hence, any set of generators of G possesses a subset of exactly d elements which generates G. The number d is the dimension of $G/\Phi(G)$ over $\mathbb{F}_p$.

Proof. Everything follows from the statement: $\sigma_1, \ldots, \sigma_t$ generate G iff $\overline{\sigma_1}, \ldots, \overline{\sigma_t}$ generate $\overline{G} = G/\Phi(G)$ (DX).

The implication ($\Longrightarrow$) is trivial and always true. Conversely, if $\overline{\sigma_1}, \ldots, \overline{\sigma_t}$ generate $\overline{G}$, then

$$G = \mathrm{Gp}\{\sigma_1, \ldots, \sigma_t, \Phi(G)\}.$$

But then, as $\Phi(G)$ is the set of nongenerators, we have

$$G = \mathrm{Gp}\{\sigma_1, \ldots, \sigma_t, \Phi(G)\} = \mathrm{Gp}\{\sigma_1, \ldots, \sigma_t\},$$

as desired. □

Let G be a group (possibly infinite). We set $\Delta^{(0)}(G) = G$, and $\Delta^{(1)}(G) = [G, G]$ and, more generally

$$\Delta^{(j+1)}(G) = [\Delta^{(j)}(G), \Delta^{(j)}(G)] = \Delta^{(1)}(\Delta^{(j)}(G)).$$

Observe that $\Delta^{(1)}(G) = [G, G]$ is the commutator group of G, and recall that for any normal subgroup, H, of G, we have $\Delta^{(1)}(G) \subseteq H$ iff G/H is abelian. Moreover, for a simple nonabelian group, $[G, G] = G$.

Proposition 1.23 *Suppose G is a group, then each $\Delta^{(j)}(G)$ is a characteristic subgroup of G and each group $\Delta^{(j)}(G)/\Delta^{(j+1)}(G)$ is abelian ($j \geq 0$). If G has property (N), then $\Delta^{(1)}(G) \subseteq \Phi(G) < G$ (provided maximal subgroups exist). If G is a p-group, then the chain*

$$G \supseteq \Delta^{(1)}(G) \supseteq \Delta^{(2)}(G) \supseteq \cdots \supseteq \Delta^{(t)}(G) \supseteq \cdots$$

is strictly descending and reaches $\{1\}$ after finitely many steps.

Proof. The group $\Delta^{(1)}(G)$ consists of products of the form

$$[\sigma_1, \tau_1] \cdots [\sigma_l, \tau_l], \quad l \geq 1.$$

If $\varphi \in \mathrm{Aut}(G)$, then

$$\varphi([\sigma_1, \tau_1] \cdots [\sigma_l, \tau_l]) = \varphi([\sigma_1, \tau_1]) \cdots \varphi([\sigma_l, \tau_l]),$$

and $\varphi([\sigma, \tau]) = [\varphi(\sigma), \varphi(\tau)]$, so $\Delta^{(1)}(G)$ is characteristic. We prove that $\Delta^{(j)}(G)$ is characteristic by induction on j. The base case $j = 1$ has just been established. Look at $\Delta^{(j+1)}(G)$. By the induction hypothesis, we have $\varphi(\Delta^{(j)}(G)) = \Delta^{(j)}(G)$. Therefore, φ is an automorphism of $\Delta^{(j)}(G)$. Yet, $\Delta^{(j+1)}(G) = \Delta^{(1)}(\Delta^{(j)}(G))$, and we proved that $\Delta^{(1)}(H)$ is characteristic for any group H (case $j = 1$). Now, $G/\Delta^{(1)}(G)$ is abelian for any group G, so $\Delta^{(j)}(G)/\Delta^{(j+1)}(G) = \Delta^{(j)}(G)/\Delta^{(1)}(\Delta^{(j)}(G))$ is abelian.

Say G has (N) and possesses maximal subgroups. If H is a maximal subgroup of G we know that $H \lhd G$ and H has prime index. So, G/H is abelian, and thus, $\Delta^{(1)}(G) \subseteq H$. Since H is arbitrary, we deduce that

$$\Delta^{(1)}(G) \subseteq \bigcap_{H \text{ maximal}} H = \Phi(G).$$

Now, assume that G is a p-group. Then, G has (N), and thus, $\Delta^{(1)}(G) \subseteq \Phi(G) < G$. But $\Delta^{(1)}(G)$ in turn is a p-group, so we can apply the argument to $\Delta^{(1)}(G)$ and we get $\Delta^{(2)}(G) < \Delta^{(1)}(G)$, etc. □

Nomenclature.

(1) The group $\Delta^{(1)}(G)$ is called the *first derived group* of G (or *commutator group* of G).

(2) The group $\Delta^{(j)}(G)$ is the *j-th derived group* of G.

(3) The sequence
$$G = \Delta^{(0)}(G) \supseteq \Delta^{(1)}(G) \supseteq \Delta^{(2)}(G) \supseteq \cdots \supseteq \Delta^{(t)}(G) \supseteq \cdots$$
is the *derived series* of G.

(4) The smallest $t \geq 0$ for which $\Delta^{(t)}(G) = \{1\}$ is the *derived length* of G and if $\Delta^{(t)}(G)$ is never $\{1\}$ (e.g., in a nonabelian simple group) then the derived length is infinite. Write $\delta(G)$ for the derived length of G.

Look at the derived series of G:
$$G = \Delta^{(0)}(G) \supseteq \Delta^{(1)}(G) \supseteq \Delta^{(2)}(G) \supseteq \cdots \supseteq \Delta^{(t)}(G) \supseteq \cdots .$$
Each quotient $\Delta^{(j)}(G)/\Delta^{(j+1)}(G)$ is abelian. Suppose G is finite, then $\Delta^{(j)}(G)/\Delta^{(j+1)}(G)$ is finite abelian. Interpolate between $\Delta^{(j)}(G)$ and $\Delta^{(j+1)}(G)$ a sequence of subgroups, necessarily normal, each maximal in the previous one. If $\delta(G) < \infty$, we get a composition series all of whose factors are cyclic of prime order. This proves half of the

Proposition 1.24 *A necessary and sufficient condition that a finite group be solvable (in the sense of Galois) is that $\delta(G) < \infty$.*

Proof. We need only prove: If G is (Galois) solvable, then $\delta(G) < \infty$. Say
$$G = G_0 > G_1 > G_2 > \cdots > G_t = \{1\}$$
is a composition series with abelian factors. We have $G_1 < G$ and G/G_1 is abelian. Therefore, by a previous remark, $\Delta^{(1)}(G) \subseteq G_1$. Each quotient G_j/G_{j+1} is abelian, so $\Delta^{(1)}(G_j) \subseteq G_{j+1}$ for all j. Now, $\Delta^{(1)}(G) \subseteq G_1$ implies that $\Delta^{(1)}(\Delta^{(1)}(G)) \subseteq \Delta^{(1)}(G_1)$, and so,
$$\Delta^{(2)}(G) \subseteq \Delta^{(1)}(G_1) \subseteq G_2.$$
An easy induction yields $\Delta^{(r)}(G) \subseteq G_r$ (DX). Therefore, $\Delta^{(t)}(G) \subseteq \{1\}$, *i.e.*, $\delta(G) \leq t$. □

Observe that we actually proved more: The derived length, $\delta(G)$, of a solvable finite group is less than or equal to the length of any composition series for G.

Definition 1.7 An arbitrary group, G, is *solvable* iff $\delta(G) < \infty$.

Proposition 1.25 *Say G is a p-group of order at least p^2. Then, $(G : \Delta^{(1)}(G)) \geq p^2$.*

Proof. We may assume that G is nonabelian, else $\Delta^{(1)}(G) = \{1\}$ and so, $(G : \Delta^{(1)}(G)) = \#(G) \geq p^2$. As G is a p-group, if $(G : \Delta^{(1)}(G)) < p^2$, then $(G : \Delta^{(1)}(G)) = p$. We know that $\Delta^{(1)}(G) \subseteq \Phi(G)$. Therefore, $(G : \Phi(G)) = p$ and the Burnside dimension of G (*i.e.* $\dim_{\mathbb{F}_p} G/\Phi(G)$) is equal to 1. By the Burnside basis theorem, G is cyclic, so abelian, a contradiction. □

1.4 Group Extensions

Let G be a finite group and let

$$G = G_0 > G_1 > G_2 > \cdots > G_t = \{1\}$$

be a composition series. We have the groups $G_j/G_{j+1} = \overline{G}_j$, the composition factors of the composition series.

Problem: Given the (ordered) sequence $\overline{G_0}, \overline{G}_1, \overline{G}_2, \ldots, \overline{G}_{t-1}$, try to reconstruct G.

Say H and K are two groups, $\mathcal{G}$ is a "big" group and $H \lhd \mathcal{G}$ with $\mathcal{G}/H \xrightarrow{\sim} K$. Note, this is exactly the case at the small end of a composition series. We have
$G_{t-1} = \overline{G}_{t-1} = G_{t-1}/G_t$. We also have $G_{t-1} \lhd G_{t-2}$, and the quotient is $\overline{G}_{t-2}$, so we are in the above situation with $H = G_{t-1} = \overline{G}_{t-1}$, $K = \overline{G}_{t-2}$, $\mathcal{G} = G_{t-2}$, and $\mathcal{G}/H \xrightarrow{\sim} K$.

The above situation is a special case of an *exact sequence*. A diagram of groups and homomorphisms

$$0 \longrightarrow H \xrightarrow{\varphi} \mathcal{G} \xrightarrow{\psi} K \longrightarrow 0,$$

where the map $0 \longrightarrow H$ is the inclusion of $\{1\}$ into H and the map $K \longrightarrow 0$ is the surjection sending every element of K to 1 in the trivial group $\{1\}$, is called a *short exact sequence* iff the kernel of every homomorphism is equal to the image of the previous homomorphism on its left. This means that

(1) $\operatorname{Ker} \varphi = \{1\}$, so φ is injective, and we identify H with a subgroup of $\mathcal{G}$.

(2) $H = \operatorname{Im} \varphi = \operatorname{Ker} \psi$, so H is normal in $\mathcal{G}$.

(3) $\operatorname{Im} \psi = K$, so ψ is surjective. By the first homomorphism theorem, $\mathcal{G}/H \xrightarrow{\sim} K$.

(4) Properties (1), (2), (3) are equivalent to $0 \longrightarrow H \longrightarrow \mathcal{G} \longrightarrow K \longrightarrow 0$ is exact.

Going back to composition series, we have $G_{j+1} \lhd G_j$ and $\overline{G}_j = G_j/G_{j+1}$. So, a composition series is equivalent with a collection of short exact sequences

$$\begin{aligned}
&0 \longrightarrow G_{t-1} \longrightarrow G_{t-2} \longrightarrow \overline{G}_{t-2} \longrightarrow 0\\
&0 \longrightarrow G_{t-2} \longrightarrow G_{t-3} \longrightarrow \overline{G}_{t-3} \longrightarrow 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&0 \longrightarrow G_1 \longrightarrow G \longrightarrow \overline{G}_0 \longrightarrow 0.
\end{aligned}$$

So our problem reduces to the problem of *group extensions*: Given H and K, groups, find (classify) all groups, $\mathcal{G}$, which can possibly fit into an exact sequence

$$0 \longrightarrow H \longrightarrow \mathcal{G} \longrightarrow K \longrightarrow 0.$$

The problem is very hard when H is nonabelian.

Definition 1.8 If A, G are groups, a group, $\mathcal{G}$, is an *extension of G by A* iff $\mathcal{G}$ fits into an exact sequence

$$(E) \qquad 0 \longrightarrow A \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 0.$$

Two such extensions (E), (E') are *equivalent* iff there exists a commutative diagram

$$\begin{array}{cccccccc}
(E) & 0 & \longrightarrow & A & \longrightarrow & \mathcal{G} & \longrightarrow & G & \longrightarrow & 0\\
 & & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\
(E') & 0 & \longrightarrow & A & \longrightarrow & \mathcal{G}' & \longrightarrow & G & \longrightarrow & 0.
\end{array}$$

Remarks:

(1) The homomorphism, ψ, in the above diagram is an isomorphism of groups. So, the notion of equivalence is indeed an equivalence relation (DX).

(2) Equivalence of group extensions is stronger than isomorphism of $\mathcal{G}$ with $\mathcal{G}'$.

(3) The group $\mathcal{G}$ in (E) should be considered a "fibre space" whose base is G and whose "fibre" is A.

As we remarked before, the theory is good only when A is abelian. *From now on, we assume A is an abelian group.*

Proposition 1.26 *Say*

$$(E) \qquad 0 \longrightarrow A \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 0$$

is a group extension and A is abelian. Then, there exists a natural action of G on A; so, A is a G-module. Equivalent extensions give rise to the same action.

Proof. Denote the surjective homomorphism $\mathcal{G} \longrightarrow G$ in (E) by bar (-). Pick $\xi \in G$ and any $a \in A$. There exists $x \in \mathcal{G}$ with $\overline{x} = \xi$. Consider xax^{-1}. Since $A \lhd \mathcal{G}$, we have $xax^{-1} \in A$. If $y \in \mathcal{G}$ and if $\overline{y} = \overline{x} = \xi$, then $x = y\alpha$ for some $\alpha \in A$. Then,

$$xax^{-1} = y\alpha a\alpha^{-1}y^{-1} = yay^{-1},$$

as A is abelian. Therefore, if we set

$$\xi \cdot a = xax^{-1},$$

this is a well-defined map. The reader should check that it is an action (DX). Assume we have an equivalence of extensions between (E) and (E'):

$$\begin{array}{lccccccc} (E) & 0 \longrightarrow & A & \longrightarrow & \mathcal{G} & \longrightarrow & G & \longrightarrow 0 \\ & & \| & & \downarrow{\scriptstyle \psi} & & \| & \\ (E') & 0 \longrightarrow & A & \longrightarrow & \mathcal{G}' & \longrightarrow & G & \longrightarrow 0. \end{array}$$

Pick $\xi \in G$ and any $a \in A$. Denote the E-action by $\cdot$ and the E'-action by $\cdot\cdot$. Observe that

$$\xi \cdot a = \psi(\xi \cdot a) = \psi(xax^{-1}) = \psi(x)\psi(a)\psi(x)^{-1} = \psi(x)a\psi(x)^{-1},$$

since the left vertical arrow is the identity in the diagram, yet $\psi(x)$ lifts ξ in $\mathcal{G}'$, as the right vertical arrow is the identity in the diagram. However, by definition,

$$\xi \cdot\cdot a = \psi(x)a\psi(x)^{-1},$$

so, $\xi \cdot\cdot a = \xi \cdot a$ for all $a \in A$. □

The *type* of (E) is the structure of A as G-module, i.e., the action of G on A. We get a first invariant of a *group extension*, its action (of G on A).

Fix the action of (E). Can we classify the extensions up to equivalence? Say we are given an extension

$$(E) \qquad 0 \longrightarrow A \longrightarrow \mathcal{G} \xrightarrow{\pi} G \longrightarrow 0.$$

There is always a set-theoretic section $s\colon G \to \mathcal{G}$, i.e., a set map, s, so that $\pi(s(\sigma)) = \sigma$ for all $\sigma \in G$. Write u_σ for the s-lift of σ, i.e., $s(\sigma) = u_\sigma$. So, $\pi(u_\sigma) = \overline{u_\sigma} = \sigma$. As s is **not** necessarily a group homomorphism, what is the obstruction? Consider

$$u_\sigma u_\tau (u_{\sigma\tau})^{-1} = f(\sigma, \tau). \qquad (*)$$

Note that $f(\sigma,\tau) = 1$ iff $s\colon \sigma \mapsto u_\sigma$ is a group homomorphism. If we apply the homomorphism bar to $(*)$, we get $\overline{f(\sigma,\tau)} = 1$, and so, $f(\sigma,\tau) \in A$. Observe that f is a function $f\colon G \prod G \to A$. Given $x \in \mathcal{G}$, look at $\overline{x}$. We know that $\overline{x} = \sigma \in G$. If we apply bar to xu_σ^{-1}, we get 1, because $\overline{u_\sigma^{-1}} = \sigma^{-1}$ and $\overline{x} = \sigma$. So, we have $xu_\sigma^{-1} \in A$, which yields $x = au_\sigma$, for some $a \in A$.

Observe that:

(1) Each x determines *uniquely* a representation $x = au_\sigma$, with $a \in A$ and $\sigma \in G$.

(2) The map $A \prod G \longrightarrow \mathcal{G}$ (where $A \prod G$ is the product of A and G *as sets*) *via*

$$(a, \sigma) \mapsto au_\sigma$$

is a bijection of sets (an isomorphism in the category of sets).

(3) $\mathcal{G}$ (as a set) is just $A \prod G$ (product in the category of sets).[2]

Can we recover the group multiplication of $\mathcal{G}$? We have

$$\begin{aligned}(au_\sigma)(bu_\tau) &= a(u_\sigma b)u_\tau \\ &= a(u_\sigma b u_\sigma^{-1})u_\sigma u_\tau \\ &= a(\sigma \cdot b)u_\sigma u_\tau \\ &= a(\sigma \cdot b)f(\sigma,\tau)u_{\sigma\tau} \\ &= cu_{\sigma\tau},\end{aligned}$$

where $c = a(\sigma \cdot b)f(\sigma,\tau)$, and $c \in A$. Therefore, knowledge of the action and $f(\sigma,\tau)$ gives us knowledge of the group multiplication.

Thus, it is natural to try to go backwards and make $\mathcal{G}$ from the groups A and G, the action of G on A, and f. It is customary to use an additive notation for the group operation in A, since A is abelian. The underlying set of the group $\mathcal{G}$ is

$$A \prod G = \{\langle a, \sigma\rangle \mid a \in A,\ \sigma \in G\}.$$

Multiplication is given by

$$\langle a, \sigma\rangle\langle b, \tau\rangle = \langle a + \sigma \cdot b + f(\sigma,\tau), \sigma\tau\rangle. \tag{$\dagger$}$$

However, the multiplication defined by $(\dagger)$ is supposed to make $\mathcal{G}$ into a group, and this imposes certain conditions on f. First, we deal with associativity. For this, we go back to the original $\mathcal{G}$ where we have the associative law:

$$(au_\sigma)((bu_\tau)(cu_\rho)) = ((au_\sigma)(bu_\tau))(cu_\rho).$$

Expanding the left hand side, we get

$$\begin{aligned}(au_\sigma)((bu_\tau)(cu_\rho)) &= (au_\sigma)(b(\tau \cdot c)f(\tau,\rho)u_{\tau\rho}) \\ &= (a\sigma \cdot (b(\tau \cdot c)f(\tau,\rho))f(\sigma,\tau\rho)u_{\sigma(\tau\rho)} \\ &= a(\sigma \cdot b)(\sigma\tau \cdot c)(\sigma \cdot f(\tau,\rho))f(\sigma,\tau\rho)u_{\sigma(\tau\rho)}.\end{aligned}$$

Expanding the righthand side, we get

$$\begin{aligned}((au_\sigma)(bu_\tau))(cu_\rho) &= a(\sigma \cdot b)f(\sigma,\tau)u_{\sigma\tau})(cu_\rho) \\ &= a(\sigma \cdot b)f(\sigma,\tau)(\sigma\tau \cdot c)f(\sigma\tau,\rho)u_{(\sigma\tau)\rho}.\end{aligned}$$

[2] In (2) and (3) we give a foretaste of the language of categories to be introduced in Section 1.7.

Thus, the associative law becomes (writing RHS = LHS)

$$f(\sigma,\tau)(\sigma\tau\cdot c)f(\sigma\tau,\rho) = (\sigma\tau\cdot c)(\sigma\cdot f(\tau,\rho))f(\sigma,\tau\rho).$$

Now, all the above terms are in A, and since A is abelian, we can permute terms and perform cancellations, and we get

$$f(\sigma,\tau)f(\sigma\tau,\rho) = (\sigma\cdot f(\tau,\rho))f(\sigma,\tau\rho). \tag{††}$$

This identity is equivalent to the associativity law in $\mathcal{G}$.

Nomenclature: A function from $G\prod G$ to A is called a 2-*cochain on* G *with values in* A. Any 2-cochain satisfying (††) is called a 2-*cocycle with coefficients in* A.

Therefore, (†) is an associative multiplication in $A\prod G$ iff f is a 2-cocycle with values in A.

Does $A\prod G$ with multiplication (†) have an identity?

The original group, $\mathcal{G}$, has identity 1 and we have $1 = u_1^{-1}u_1$, where $u_1 \in A$, and so, $u_1^{-1} \in A$. For all $b \in A$ and all $\tau \in G$, we have

$$(u_1^{-1}u_1)(bu_\tau) = bu_\tau,$$

which yields

$$u_1^{-1}(1\cdot b)f(1,\tau)u_\tau = u_1^{-1}bf(1,\tau)u_\tau = bu_\tau.$$

Since A is abelian, we get

$$f(1,\tau) = u_1,$$

which shows that $f(1,\tau)$ is independent of τ. In particular, $u_1 = f(1,1)$.

Question: Is (††) sufficient to imply that $f(1,\tau) = f(1,1)$ for all $\tau \in G$?

In (††), take $\sigma = 1$. We get

$$f(1,\tau)f(\tau,\rho) = f(\tau,\rho)f(1,\tau\rho).$$

Again, since A is abelian, we deduce that $f(1,\tau) = f(1,\tau\rho)$. If we take $\tau = 1$, we get $f(1,1) = f(1,\rho)$, for all ρ.

Therefore, (††) is sufficient and $A\prod G$ has an identity $\mathbf{1} = \langle f(1,1)^{-1}, 1\rangle$, or in additive notation (since A is abelian),

$$\mathbf{1} = \langle -f(1,1), 1\rangle. \tag{$*$}$$

Finally, what about inverses? Once again, go back to our original $\mathcal{G}$.

We have $(au_\sigma)^{-1} = u_\sigma^{-1}a^{-1}$. Now,

$$\overline{u_\sigma^{-1}} = (\overline{u_\sigma})^{-1} = \sigma^{-1} = \overline{u_{\sigma^{-1}}}.$$

Therefore, there is some $\alpha \in A$ so that $u_\sigma^{-1} = \alpha u_{\sigma^{-1}}$. By multiplying on the right by u_σ, we get

$$1 = \alpha u_{\sigma^{-1}}u_\sigma = \alpha f(\sigma^{-1},\sigma)u_{\sigma\sigma^{-1}} = \alpha f(\sigma^{-1},\sigma)u_1 = \alpha f(\sigma^{-1},\sigma)f(1,1),$$

since $u_1 = f(1,1)$. So, $\alpha = f(1,1)^{-1}f(\sigma^{-1},\sigma)^{-1}$. Consequently, we get

$$\begin{aligned}
(au_\sigma)^{-1} &= u_\sigma^{-1}a^{-1}\\
&= \alpha u_{\sigma^{-1}}a^{-1}\\
&= \alpha(u_{\sigma^{-1}}a^{-1}u_{\sigma^{-1}}^{-1})u_{\sigma^{-1}}\\
&= \alpha(\sigma^{-1}\cdot a^{-1})u_{\sigma^{-1}}\\
&= f(1,1)^{-1}f(\sigma^{-1},\sigma)^{-1}(\sigma^{-1}\cdot a^{-1})u_{\sigma^{-1}}\\
&= f(1,1)^{-1}f(\sigma^{-1},\sigma)^{-1}(\sigma^{-1}\cdot a)^{-1}u_{\sigma^{-1}}\\
&= ((\sigma^{-1}\cdot a)f(\sigma^{-1},\sigma)f(1,1))^{-1}u_{\sigma^{-1}}.
\end{aligned}$$

Therefore, in $A \prod G$ (switching to additive notation since A is abelian), inverses are given by

$$\langle a, \sigma\rangle^{-1} = \langle -\sigma^{-1} \cdot a - f(\sigma^{-1}, \sigma) - f(1,1),\ \sigma^{-1}\rangle. \tag{$**$}$$

We find that $A \prod G$ can be made into a group *via* (†), provided $f(\sigma, \tau)$ satisfies (††). The formulae ($*$) and ($**$) give the unit element and inverses, respectively. For temporary notation, let us write $(A \prod G; f)$ for this group. Also, since A is abelian, let us rewrite (††) in additive notation, since this will be more convenient later on:

$$\sigma \cdot f(\tau, \rho) + f(\sigma, \tau\rho) = f(\sigma\tau, \rho) + f(\sigma, \tau). \tag{††}$$

Go back to the original group, $\mathcal{G}$, and its set-theoretic section $s\colon G \to \mathcal{G}$ (with $s(\sigma) = u_\sigma$). We might have chosen another set-theoretic section, $t\colon G \to \mathcal{G}$, namely, $t(\sigma) = v_\sigma$. We get a 2-cocycle $g(\sigma, \tau) = v_\sigma v_\tau (v_{\sigma\tau})^{-1}$, i.e., $v_\sigma v_\tau = g(\sigma, \tau) v_{\sigma\tau}$.

What is the relation between f and g?

We know that $\overline{v_\sigma} = \sigma = \overline{u_\sigma}$, which implies that there is some $k(\sigma) \in A$ with $v_\sigma = k(\sigma) u_\sigma$. Then, we have

$$v_\sigma v_\tau = g(\sigma, \tau) v_{\sigma\tau} = g(\sigma, \tau) k(\sigma\tau) u_{\sigma\tau},$$

and also

$$v_\sigma v_\tau = k(\sigma) u_\sigma k(\tau) u_\tau = k(\sigma)(\sigma \cdot k(\tau)) u_\sigma u_\tau = k(\sigma)(\sigma \cdot k(\tau)) f(\sigma, \tau) u_{\sigma\tau}.$$

By equating these expressions, we get

$$g(\sigma, \tau) k(\sigma\tau) = k(\sigma)(\sigma \cdot k(\tau)) f(\sigma, \tau).$$

But A is abelian, so we can write the above

$$g(\sigma, \tau) - f(\sigma, \tau) = \sigma \cdot k(\tau) - k(\sigma\tau) + k(\sigma). \tag{$*$}$$

Observe that $k\colon G \to A$ is a function of one variable on G. We call k a 1-*cochain on G with values in A*. For a 1-cochain, define a corresponding 2-cochain, called its *coboundary*, δk, by

$$(\delta k)(\sigma, \tau) = \sigma \cdot k(\tau) - k(\sigma\tau) + k(\sigma).$$

Remarks:

(1) Every coboundary of a 1-cochain is automatically a 2-cocycle (DX).

(2) Cocycles form a group under addition of functions denoted by $Z^2(G, A)$. The special 2-cocycles which are coboundaries (of 1-cochains) form a group (DX) denoted by $B^2(G, A)$. Item (1) says that $B^2(G, A)$ is a subgroup of $Z^2(G, A)$.

(3) The quotient group, $Z^2(G, A)/B^2(G, A)$, denoted $H^2(G, A)$, is the *second cohomology group of G with coefficients in A*.

(4) Equation ($*$) above says: If we change the choice of section from s to t, the corresponding cocycles, f and g, are *cohomologous*, i.e., $g - f = \delta k$, i.e., the image of f in $H^2(G, A)$ is the same as the image of g in $H^2(G, A)$. Thus, it is the cohomology class of f which is determined by (E).

Now, make $(A \prod G; f)$. Then, we can map A into $(A \prod G; f)$ *via*

$$a \mapsto \langle a - f(1,1), 1\rangle.$$

Claim. The set $\{\langle a - f(1,1), 1\rangle \mid a \in A\}$ is a subgroup of $(A \prod G; f)$. In fact, it is a normal subgroup and the quotient is G.

Proof. We have

$$\langle a - f(1,1), 1\rangle\langle b - f(1,1), 1\rangle = \langle a - f(1,1) + b - f(1,1) + f(1,1), 1\rangle = \langle a + b - f(1,1), 1\rangle,$$

and thus, the map $\lambda\colon a \mapsto \langle a - f(1,1), 1\rangle$ is a group homomorphism. We leave the rest as a (DX). □

Say $f - g = \delta k$, i.e., f and g are cohomologous, and make $(A \prod G; f)$ and $(A \prod G; g)$. Consider the map $\theta\colon (A \prod G; f) \to (A \prod G; g)$ given by

$$\theta\colon \langle a, \sigma\rangle \mapsto \langle a + k(\sigma), \sigma\rangle.$$

We claim that θ is a homomorphism. Since

$$\langle a, \sigma\rangle\langle b, \tau\rangle = \langle a + \sigma \cdot b + f(\sigma, \tau), \sigma\tau\rangle,$$

we have

$$\theta(\langle a, \sigma\rangle\langle b, \tau\rangle) = \langle a + \sigma \cdot b + f(\sigma, \tau) + k(\sigma\tau), \sigma\tau\rangle.$$

We also have

$$\begin{aligned} \theta(\langle a, \sigma\rangle)\theta(\langle b, \tau\rangle) &= \langle a + k(\sigma), \sigma\rangle\langle b + k(\tau), \tau\rangle) \\ &= \langle a + k(\sigma) + \sigma \cdot b + \sigma \cdot k(\tau) + g(\sigma, \tau), \sigma\tau\rangle). \end{aligned}$$

In order for θ to be a homomorphism, we need

$$k(\sigma) + \sigma \cdot k(\tau) + g(\sigma, \tau) = f(\sigma, \tau) + k(\sigma\tau),$$

that is, $f - g = \delta k$. Consequently, θ is a homomorphism, in fact, an isomorphism. Moreover, $(A \prod G; f)$ and $(A \prod G; g)$ fit into two extensions and we have the following diagram:

$$\begin{array}{lccccccc} (E)_f & 0 & \longrightarrow & A & \longrightarrow & (A \prod G; f) & \longrightarrow & G \longrightarrow 0 \\ & & & \| & & \downarrow{\scriptstyle \theta} & & \| \\ (E')_g & 0 & \longrightarrow & A & \longrightarrow & (A \prod G; g) & \longrightarrow & G \longrightarrow 0. \end{array}$$

The rightmost rectangle commutes, but we need to check that the leftmost rectangle commutes. Going over horizontally and down from $(A \prod G; f)$, for any $a \in A$, we have

$$a \mapsto \langle a - f(1,1), 1\rangle \mapsto \langle a - f(1,1) + k(1), 1\rangle,$$

and going horizontally from the lower A, we have

$$a \mapsto \langle a - g(1,1), 1\rangle.$$

For the rectangle to commute, we need: $g(1,1) = f(1,1) - k(1)$. However,
$f(\sigma, \tau) = g(\sigma, \tau) + \delta k(\sigma, \tau)$ and $\delta k(\sigma, \tau) = \sigma \cdot k(\tau) - k(\sigma\tau) + k(\sigma)$. If we set $\sigma = \tau = 1$, we get

$$\delta k(1,1) = k(1) - k(1) + k(1) = k(1),$$

and it follows that $g(1,1) = f(1,1) - k(1)$, as desired.

Hence, cohomologous 2-cocycles give rise to *equivalent* group extensions (the action is fixed). Conversely, we now show that equivalent group extensions give rise to cohomologous 2-cocycles. Say

$$\begin{array}{lccccccc} (E) & 0 & \longrightarrow & A & \longrightarrow & \mathcal{G} & \longrightarrow & G & \longrightarrow & 0 \\ & & & \| & & \downarrow{\scriptstyle \psi} & & \| & & \\ (E') & 0 & \longrightarrow & A & \longrightarrow & \mathcal{G}' & \longrightarrow & G & \longrightarrow & 0. \end{array}$$

is an equivalence of extensions (i.e., the diagram commutes). We know, up to the notion of being cohomologous, that we may adjust both cocycles f and g associated with (E) and (E') by choice of sections. In both cases, take $u_1 = 0$ (since we are using additive notation). Therefore, $f(1,1) = g(1,1) = 0$. From the commutativity of the diagram, ψ must be of the form

$$\psi\langle a, \sigma\rangle = \langle \varphi(a, \sigma), \sigma\rangle$$

for some function $\varphi\colon A \coprod G \to A$. By the above choice, the maps $A \longrightarrow \mathcal{G}$ and $A \longrightarrow \mathcal{G}'$ are given by $a \mapsto \langle a, 1\rangle$ in both cases. Therefore,
$\psi(a,1) = \langle \varphi(a,1), 1\rangle = (a,1)$, and so,

$$\varphi(a,1) = a, \quad \text{for all } a \in A.$$

Since ψ is a homomorphism, we have

$$\psi(\langle a,\sigma\rangle\langle b,\tau\rangle) = \psi(\langle a,\sigma\rangle)\psi(\langle b,\tau\rangle),$$

and this yields an identity relating f, g and φ. The left hand side of the above equation is equal to

$$\psi(\langle a + \sigma\cdot b + f(\sigma,\tau), \sigma\tau\rangle) = \langle \varphi(a + \sigma\cdot b + f(\sigma,\tau), \sigma\tau\rangle), \sigma\tau\rangle,$$

and the righthand side is equal to

$$\langle \varphi(a,\sigma),\sigma\rangle\langle\varphi(b,\tau),\tau\rangle = \langle \varphi(a,\sigma) + \sigma\cdot\varphi(b,\tau) + g(\sigma,\tau), \sigma\tau\rangle,$$

and by equating them, we get

$$\varphi(a + \sigma\cdot b + f(\sigma,\tau), \sigma\tau\rangle) = \varphi(a,\sigma) + \sigma\cdot\varphi(b,\tau) + g(\sigma,\tau). \tag{$\dagger\dagger\dagger$}$$

By taking $\tau = 1$ (using the fact that $\varphi(b,1) = b$), we get

$$\varphi(a + \sigma\cdot b + f(\sigma,1), \sigma\rangle) = \varphi(a,\sigma) + \sigma\cdot b + g(\sigma,1). \tag{$***$}$$

Now, $(\dagger\dagger)$ can be written as

$$\sigma\cdot f(\tau,\rho) - f(\sigma\tau,\rho) + f(\sigma,\tau\rho) - f(\sigma,\tau) = 0.$$

If we take $\rho = 1$, we get

$$\sigma\cdot f(\tau,1) - f(\sigma\tau,1) + f(\sigma,\tau) - f(\sigma,\tau) = 0.$$

which yields

$$\sigma\cdot f(\tau,1) = f(\sigma\tau,1).$$

If we take $\tau = 1$, we get $\sigma\cdot f(1,1) = f(\sigma,1)$, but $f(1,1) = 0$, and so,

$$f(\sigma,1) = 0.$$

Consequently, $(***)$ yields

$$\varphi(a + \sigma\cdot b, \sigma) = \varphi(a,\sigma) + \sigma\cdot b.$$

Writing $b = \sigma^{-1} \cdot c$, we get

$$\varphi(a + c, \sigma) = \varphi(a, \sigma) + c, \quad \text{for all } a, c \in A.$$

In particular, when $a = 0$, we get $\varphi(c, \sigma) = \varphi(0, \sigma)+c$. Let $\varphi(0, \sigma) = k(\sigma)$. Now, if we use $\varphi(a, \sigma) = \varphi(0, \sigma)+a$ in (†††), we get

$$a + \sigma \cdot b + f(\sigma, \tau) + k(\sigma\tau) = a + k(\sigma) + \sigma \cdot (b + k(\tau)) + g(\sigma, \tau),$$

which yields

$$f(\sigma, \tau) + k(\sigma\tau) = g(\sigma, \tau) + k(\sigma) + \sigma \cdot k(\tau),$$

that is, $f - g = \delta k$. Hence, we have proved almost all of the following fundamental theorem:

Theorem 1.27 *If G and A are groups and A is abelian, then each group extension*

$$(E) \qquad 0 \longrightarrow A \longrightarrow \mathcal{G} \xrightarrow{\pi} G \longrightarrow 0$$

makes A into a G-module; the G-module structure is the type of (E) and equivalent extensions have the same type. For a given type, the equivalence classes of extensions of G by A are in one-to-one correspondence with $H^2(G, A)$, the second cohomology group of G with coefficients in A. Hence, the distinct extensions of G by A (up to equivalence) are classified by the pairs $(\text{type}(E), \chi(E))$, where $\chi(E)$ is the cohomology class in $H^2(G, A)$ corresponding to (E). In this correspondence, central extensions correspond to G-modules, A, with trivial action ((E) is central iff $A \subseteq Z(\mathcal{G})$). An extension of any type splits iff $\chi(E) = 0$ in $H^2(G, A)$. ((E) is split iff there is a group homomorphism $s\colon G \to \mathcal{G}$ so that $\pi \circ s = \text{id}$).

Proof. We just have to prove the last two facts. Note that the type of extension is trivial iff

$$(\forall \sigma \in G)(\forall a \in A)(\sigma \cdot a = a)$$

iff

$$(\forall x \in \mathcal{G})(\forall a \in A)(x^{-1}ax = a)$$

iff

$$(\forall x \in \mathcal{G})(\forall a \in A)([x, a] = 1)$$

iff $A \subseteq Z(\mathcal{G})$.

Finally, the cohomology is trivial iff every cocycle is a coboundary iff every cocycle is cohomologous to 0 iff in (E) there is a map $\sigma \mapsto u_\sigma$ with $f(\sigma, \tau) = 0$. Such a map is a homomorphism. Thus, $\chi(E) = 0$ in $H^2(G, A)$ iff (E) has a splitting. □

Examples. (I) Find all extensions

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{G} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

There are several cases to consider depending on the type and the cohomology class of the extension.

(a) Trivial type (the action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}$ is trivial).

($a1$) Split extension. We get $\mathcal{G} \cong \mathbb{Z} \prod (\mathbb{Z}/2\mathbb{Z})$.

($a2$) Nonsplit extensions. In this case, we have to compute $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$ (trivial action). We know from previous work that (up to cohomology) we can restrict ourselves to *normalized cochains*, $f(\sigma, \tau)$, i.e., cochains such that

$$f(\sigma, 1) = f(1, \sigma) = 0.$$

Elements in $\mathbb{Z}/2\mathbb{Z}$ are ± 1. We need to know what $f(-1, -1)$ is. The reader should check that the cocycle condition, $\delta f = 0$, gives no condition on the integer $f(-1, -1)$, and thus, we have an isomorphism $Z^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$.

What about coboundaries: $f = \delta k$? Such k's are also normalized, and so, $k(1) = 0$. We have $k(-1) = b$, for any $b \in \mathbb{Z}$. Since

$$\delta k(\sigma, \tau) = \sigma \cdot k(\tau) - k(\sigma\tau) + k(\sigma),$$

using the fact that the action is trivial and that $k(1) = 0$, we get

$$\delta k(-1, -1) = (-1) \cdot k(-1) - k(1) + k(-1) = k(-1) + k(-1) = 2b.$$

So, we can adjust f, up to parity by coboundaries, and $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Consequently, we have exactly one nonsplit, trivial-type extension

$$\mathcal{G} = \{(n, \pm 1) \mid n \in \mathbb{Z}\}.$$

The group operation is given by

$$\begin{aligned} (n, \pm 1)(m, 1) &= (n + m, \pm 1) \\ (n, 1)(m, \pm 1) &= (n + m, \pm 1) \\ (n, -1)(m, -1) &= (n + m + 1, 1), \end{aligned}$$

where in this last equation, we assumed without loss of generality that $f(-1, -1) = 1$.

(b) Nontrivial type. We need a nontrivial map $\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z})$. Since $\mathbb{Z}$ is generated by 1 and -1, there is only one nontrivial action:

$$(-1) \cdot n = -n.$$

(Recall that $1 \cdot n = n$, always).

(b1) The split, nontrivial type extension. In this case

$$\mathcal{G} = \{(n, \sigma) \mid n \in \mathbb{Z},\ \sigma \in \mathbb{Z}/2\mathbb{Z}\},$$

with multiplication given by

$$(n, \sigma)(m, \tau) = (n + \sigma \cdot m, \sigma\tau).$$

Now, consider the map

$$(n, \sigma) \mapsto \begin{pmatrix} \sigma & n \\ 0 & 1 \end{pmatrix}.$$

Observe that matrix multiplication yields

$$\begin{pmatrix} \sigma & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \tau & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \sigma\tau & n + \sigma \cdot m \\ 0 & 1 \end{pmatrix}.$$

Therefore, $\mathcal{G}$ is isomorphic to the group of matrices

$$\begin{pmatrix} \sigma & n \\ 0 & 1 \end{pmatrix}$$

under matrix product. This is a nonabelian group, it is infinite and we claim that $\mathcal{G}$ is solvable with $\delta(\mathcal{G}) = 2$.

Indeed, we have $\mathcal{G}/\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$, an abelian group, and so $\Delta^{(1)}(\mathcal{G}) \subseteq \mathbb{Z}$. So,
$\Delta^{(2)}(\mathcal{G}) \subseteq \Delta^{(1)}(\mathbb{Z}) = \{0\}$, and we conclude that $\delta(\mathcal{G}) = 2$.

(b2) Nonsplit, nontrivial type extension. We need to figure out what the cocycles are in order to compute $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$. By the same reasoning as before, we need to know what is $f(-1, -1)$. We know that $\delta f(\sigma, \tau) = 0$. So, we have

$$\sigma \cdot f(\tau, \rho) - f(\sigma\tau, \rho) + f(\sigma, \tau\rho) - f(\sigma, \tau) = 0.$$

Let $\tau = \rho = -1$ in the above equation. We get

$$\sigma \cdot f(-1,-1) - f(-\sigma,-1) + f(\sigma,1) - f(\sigma,-1) = \sigma \cdot f(-1,-1) - f(-\sigma,-1) - f(\sigma,-1) = 0,$$

since $f(\sigma,1) = 0$. If we let $\sigma = -1$, since $f(1,-1) = 0$, we get

$$-f(-1,-1) - f(-1,-1) = 0,$$

and so, $2f(-1,-1) = 0$. Since $f(-1,-1) \in \mathbb{Z}$, we get $f(-1,-1) = 0$. Therefore, $f \equiv 0$ and the cohomology is trivial: $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = (0)$ (for nontrivial action).

As a conclusion, there exist three extension classes and three distinct groups, two of them abelian, the third solvable and faithfully representable by matrices.

(II) Let V be a finite dimensional vector space and consider V^+ as additive group. Let $G = \mathrm{GL}(V)$ and let the action of G on V be the natural one (i.e, for any $\varphi \in \mathrm{GL}(V)$ and any $v \in V$, $\varphi \cdot v = \varphi(v)$). We have the split extension

$$0 \to V \to \mathcal{G} \rightleftarrows \mathrm{GL}(V) \to 0.$$

The group, $\mathcal{G}$, in the above exact sequence is the *affine group* of V.

(III) Again, we restrict ourselves to split extensions. Let A be any abelian group and let $n \in \mathbb{N}$. The group

$$\underbrace{A \prod A \prod \cdots \prod A}_{n}$$

is acted on by the symmetric group, $\mathfrak{S}_n$, simply by permuting the factors. We have a split extension

$$0 \to \underbrace{A \prod A \prod \cdots \prod A}_{n} \to \mathcal{G} \rightleftarrows \mathfrak{S}_n \to 0.$$

The group, $\mathcal{G}$, is called the *wreath product* of A by $\mathfrak{S}_n$ and is denoted $A \wr \mathfrak{S}_n$. We denote the split extension of a given type of G by A by $A \lll G$ (note that this notation does not refer to the action).

Here are some useful facts on cohomology:

(1) If G is arbitrary and A is n-torsion, which means that $nA = 0$, then $H^2(G, A)$ is n-torsion.

(2) If G is a finite group, say $\#(G) = g$ and A is arbitrary, then $H^2(G, A)$ is g-torsion (this is not trivial to prove!).

(3) Suppose that A is n-torsion and G is finite, with $\#(G) = g$, and suppose that $(g, n) = 1$. Then, $H^2(G, A) = (0)$. (This is a clear consequence of (1) and (2).)

(4) Suppose that G is finite. We can define a homomorphism (of G-modules) $A \longrightarrow A$, called the *G-norm* and denoted $\mathcal{N}_G$ (we will usually drop the subscript G), defined by

$$\mathcal{N}_G(a) = \sum_{\sigma \in G} \sigma \cdot a.$$

Moreover, assume that G is a *finite cyclic group*. Then, for any A, there is an isomorphism

$$A^G / \mathcal{N} A \cong H^2(G, A),$$

where

$$A^G = \{a \in A \mid \sigma \cdot a = a, \quad \text{for all } \sigma \in G\}.$$

Here is an example of how to use the above facts.

(IV) Find all the groups of order pq (with p, q prime and $0 < p < q$).

We know that the q-Sylow subgroup is normal, namely, it is $\mathbb{Z}/q\mathbb{Z} = A \lhd \mathcal{G}$, and $G = \mathcal{G}/A = \mathbb{Z}/p\mathbb{Z}$. Therefore, whatever $\mathcal{G}$ is, it fits in the group extension

$$0 \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathcal{G} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

By (3), since $(p, q) = 1$, we have $H^2(G, A) = (0)$. So, we only have split extensions. What is $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$? Clearly, it is $\mathbb{Z}/(q-1)\mathbb{Z}$. So, we have to consider the homomorphisms

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) = \mathbb{Z}/(q-1)\mathbb{Z}. \qquad (*)$$

If $(*)$ is non-trivial, then $p \mid (q-1)$, i.e., $q \equiv 1 \pmod{p}$. So, if $q \not\equiv 1 \pmod{p}$, then we have trivial action and we find that

$$\mathcal{G} \cong (\mathbb{Z}/q\mathbb{Z}) \prod (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}.$$

If $q \equiv 1 \pmod{p}$, we also can have trivial action, and we get $\mathbb{Z}/pq\mathbb{Z}$, again. So, we now consider nontrivial actions. The unique cyclic group of order p in $\mathbb{Z}/(q-1)\mathbb{Z}$ is generated by $\lambda^{\frac{q-1}{p}}$, where $\lambda = 1, 2, \ldots, p-1$. If we send $1 \in \mathbb{Z}/p\mathbb{Z}$ to $\lambda^{\frac{q-1}{p}}$, the corresponding action is

$$n \mapsto n\lambda \frac{q-1}{p} \pmod{q}.$$

Thus, there are $p-1$ nontrivial (split) group extensions, (E_λ), with central groups

$$\mathcal{G}_\lambda = \{(n, \zeta^m) \mid 0 \leq m \leq p-1\}$$

(here the elements of $\mathbb{Z}/p\mathbb{Z}$ are $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$) and multiplication given by

$$(n, \zeta^m)(r, \zeta^s) = \left((n + rm\lambda \frac{q-1}{p}, \zeta^{m+s} \right).$$

Consider the map $\mathcal{G}_\lambda \longrightarrow \mathcal{G}_1$ given by

$$(n, \zeta^m) \mapsto (m, \zeta^{\lambda m}).$$

This is a group isomorphism. So, here we have all *inequivalent extensions*, (E_λ), with $p-1$ different actions, yet the groups $\mathcal{G}_\lambda$ are mutually isomorphic. Thus, $\mathcal{G}_1$ and $\mathbb{Z}/pq\mathbb{Z}$ are the two groups of order pq when $q \equiv 1 \pmod{p}$.

The second cohomology group, $H^2(G, A)$, has appeared naturally in the solution to the group extension problem. Consequently, it is natural at this stage to define cohomology groups in general.

The set up is: We have a group, G, and a G-action, $G \prod A \longrightarrow A$, where A is an abelian group. For every $n \in \mathbb{N}$, we define

$$C^n(G, A) = \{f \colon \underbrace{G \prod \cdots \prod G}_{n} \to A\},$$

where $\underbrace{G \prod \cdots \prod G}_{n}$ is the product of G with itself n times (in the category of sets). By convention, when $n = 0$, this set product is the one point set, $\{*\}$. The set $C^n(G, A)$ is an abelian group under addition of functions (*e.g*, $f + g$ is the function defined by $(f + g)(x) = f(x) + g(x)$ for all $x \in G$). The group

$C^n(G,A)$ is called the group of *n-cochains of G with coefficients in A*. We define the *coboundary map*, $\delta_n\colon C^n(G,A) \to C^{n+1}(G,A)$, for every $n \geq 0$, by the formula:

$$\begin{aligned}(\delta_n f)(\sigma_1,\ldots,\sigma_{n+1}) &= \sigma_1 \cdot f(\sigma_2,\ldots,\sigma_{n+1}) + \sum_{j=1}^{n}(-1)^j f(\sigma_1,\ldots,\sigma_{j-1},\sigma_j\sigma_{j+1},\sigma_{j+2},\ldots,\sigma_{n+1}) \\ &\quad + (-1)^{n+1} f(\sigma_1,\ldots,\sigma_n),\end{aligned}$$

for all $f \in C^n(G,A)$ and all $\sigma_1,\ldots,\sigma_{n+1} \in G$.

(1) Check (DX): For all $n \geq 0$,

$$\delta_n(\delta_{n-1}f) \equiv 0.$$

(By convention, $\delta_{-1} = 0$).

(2) Set $Z^n(G,A) = \operatorname{Ker}\delta_n$, a subgroup of $C^n(G,A)$, the group of *n-cocycles of G with coefficients in A*. We also let $B^n(G,A) = \operatorname{Im}\delta_{n-1}$, a subgroup of $C^n(G,A)$, the group of *n-coboundaries of G with coefficients in A*. Observe that since $\delta_{-1} = 0$, we have $B^0(G,A) = (0)$. Furthermore, (1) implies that $B^n(G,A) \subseteq Z^n(G,A)$, for all $n \geq 0$.

(3) Set $H^n(G,A) = Z^n(G,A)/B^n(G,A)$; this is the *nth cohomology group of G with coefficients in A*.

Examples. (i) Case $n = 0$: Then, $B^0 = (0)$. The functions, f, in $C^0(G,A)$ are in one-to-one correspondence with the elements $f(*)$ of A, and so, $C^0(G,A) = A$. Note that for any $\sigma \in G$, if $f \in C^0(G,A)$ corresponds to the element a in A, we have

$$(\delta_0 f)(\sigma) = \sigma \cdot f(*) - f(*) = \sigma \cdot a - a.$$

Thus,

$$Z^0(G,A) = \{a \in A \mid \delta_0(a) = 0\} = \{a \in A \mid \sigma \cdot a = a, \text{ for all } \sigma \in G\} = A^G.$$

So, we also have $H^0(G,A) = A^G$.

(ii) Case $n = 1$: Then, $C^1(G,A)$ is the set of all functions $f\colon G \to A$. For any $f \in C^1(G,A)$, we have

$$(\delta_1 f)(\sigma,\tau) = \sigma \cdot f(\tau) - f(\sigma\tau) + f(\sigma).$$

It follows that

$$Z^1(G,A) = \{f \in C^1(G,A) \mid \delta_1 f = 0\} = \{f \in C^1(G,A) \mid f(\sigma\tau) = \sigma \cdot f(\tau) + f(\sigma)\}.$$

This is the set of *crossed* (or *twisted*) *homomorphisms* from G to A.

Remark: If A has trivial G-action, then $Z^1(G,A) = \operatorname{Hom}_{\mathcal{G}r}(G,A)$.

We have $B^1(G,A) = \operatorname{Im}\delta_0 =$ all functions, g, so that $g(\sigma) = (\delta_0(a))(\sigma) = \sigma \cdot a - a$, for some $a \in A$. Such objects are twisted homomorphisms, called *principal* (or *inner*) *twisted homomorphisms*.

Remark: If A has trivial G-action, then $B^1(G,A) = (0)$. So, $H^1(G,A)$ is the quotient of the twisted homomorphisms modulo the principal twisted homomorphisms if the action is nontrivial, and $H^1(G,A) = \operatorname{Hom}_{\mathcal{G}r}(G,A)$ if the action is trivial.

(iii) Case $n = 2$: We have already encountered this case in dealing with group extensions. We content ourselves with computing δ_2. Since $C^2(G,A) = \{f\colon G \coprod G \to A\}$, we have

$$(\delta_2 f)(\sigma,\tau,\rho) = \sigma \cdot f(\tau,\rho) - f(\sigma\tau,\rho) + f(\sigma,\tau\rho) - f(\sigma,\tau).$$

We note that $Z^2(G, A)$ gives us back the group of "old" 2-cocycles, $B^2(G, A)$ gives us back the group of "old" 2-coboundaries, and $H^2(G, A)$ is in one-to-one correspondence with the equivalence classes of group extensions of a fixed type.

Remark: Given a group, G, Eilenberg and Mac Lane (1940's) constructed a topological space, $K(G, 1)$, unique up to homotopy type, with the following properties:

$$\pi_n(K(G,1)) = \begin{cases} G & \text{if } n = 1 \\ (0) & \text{if } n \neq 1. \end{cases}$$

Fact: If we compute the integral cohomology of $K(G, 1)$, denoted $H^n(K(G, 1), \mathbb{Z})$, we get

$$H^n(K(G,1), \mathbb{Z}) \cong H^n(G, \mathbb{Z}).$$

Here, the G-action on $\mathbb{Z}$ is trivial.

1.5 Solvable and Nilpotent Groups

Given a group, G, its derived series,

$$G = \Delta^{(0)}(G) \supseteq \Delta^{(1)}(G) \supseteq \Delta^{(2)}(G) \supseteq \cdots \supseteq \Delta^{(t)}(G) \supseteq \cdots,$$

may decrease very quickly, and even though the solvable groups (those for which the derived series reaches $\{1\}$ after finitely many steps, i.e., those for which $\delta(G)$ is finite) are not as "wild" as groups for which $\delta(G) = \infty$, it desirable to delineate families of groups with an even "nicer" behavior. One way of doing so is to define descending (or ascending) chains that do not decrease (or increase) too quickly and then to investigate groups whose chains are finite. The collection of nilpotent groups is such a family of groups, and, moreover, nilpotent groups tend to show up as fundamental groups of spaces arising naturally in geometry. Every nilpotent group is solvable and solvability is inherited by subgroups and quotient groups, as shown in the following proposition:

Proposition 1.28 *If G is a group and G is solvable, then for every subgroup, H, of G, the group, H, is solvable. Moreover, if H is normal in G, then G/H is solvable. In fact, for both groups, $\delta(\text{either}) \leq \delta(G)$. Conversely, say G possesses a normal subgroup, H, so that both H and G/H are solvable. Then, G is solvable. In fact, $\delta(G) \leq \delta(H) + \delta(G/H)$.*

Proof. Let G be solvable. Then, $H \subseteq G$ implies $\Delta^{(1)}(H) \subseteq \Delta^{(1)}(G)$; therefore (by induction),

$$\Delta^{(j)}(H) \subseteq \Delta^{(j)}(G),$$

and we deduce that $\delta(H) \leq \delta(G)$. Consider $\overline{G} = G/H$ when $H \lhd G$. Then, $\overline{[x,y]} = [\overline{x}, \overline{y}]$ and this implies $\overline{\Delta^{(1)}(G)} = \Delta^{(1)}(\overline{G})$. Hence (by induction),

$$\overline{\Delta^{(j)}(G)} = \Delta^{(j)}(\overline{G}).$$

Therefore, $\delta(\overline{G}) \leq \delta(G)$.

Conversely, assume that H and G/H are solvable (with $H \lhd G$). We have $\overline{\Delta^{(j)}(G)} = \Delta^{(j)}(\overline{G})$ and if $j \geq \delta(\overline{G})$, then $\overline{\Delta^{(j)}(G)} = \{1\}$, which implies that $\Delta^{(j)}(G) \subseteq H$. So, $\Delta^{(k+j)}(G) \subseteq \Delta^{(k)}(H)$, and the latter is $\{1\}$ if $k = \delta(H)$. Therefore,

$$\Delta^{(\delta(\overline{G})+\delta(H))}(G) = \{1\},$$

and so, $\delta(G) \leq \delta(H) + \delta(G/H)$. □

Proposition 1.29 *Let (P) be some property of finite groups. Assume that (P) satisfies:*

(a) The trivial group has (P), every cyclic group of prime order has (P).

(b) Suppose G has (P), then $H \lhd G$ implies H and G/H have (P).

(c) If G has (P) (with $G \neq \{1\}$), then G is not simple unless G is cyclic of prime order.

Then, when G has (P), the group G is solvable.

Proof. We proceed by induction on $\#(G)$. The case $G = \{1\}$ is trivial, by (a) (nothing to check). Assume that the proposition holds for all G with $\#(G) \leq n$, and assume $\#(G) = n + 1$. If $n + 1$ is prime, then G is cyclic of prime order, which implies that it is solvable. Thus, we may assume that $n + 1$ is not prime and that G has (P). By (c), the group G has some nontrivial normal subgroup, H. By (b), both H and G/H have (P), and the induction hypothesis implies that both H and G/H are solvable. Proposition 1.28 implies that G is solvable. □

Corollary 1.30 *(Burnside, Feit & Thompson) Every group G, of order $p^a q^b$ or odd order is solvable.*

Remark: Corollary 1.30 is not really proved. It depends on establishing (c) for the two properties: p^aq^b, odd order. As remarked just before Proposition 1.10, this is not easy.

Definition 1.9 Let G be any group. The *lower central series (LCS)* of G is the descending chain of subgroups

$$G = \Gamma_0 \supseteq \Gamma_1 \supseteq \cdots \supseteq \Gamma_d \supseteq \cdots,$$

where $\Gamma_{j+1} = [G, \Gamma_j]$. The *upper central series (UCS)* of G is the ascending chain of subgroups

$$\{1\} = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots \subseteq Z_d \subseteq \cdots,$$

where $Z_j =$ the inverse image in G of $Z(G/Z_{j-1})$.

Remarks:

(1) $\Gamma_1(G) = [G, \Gamma_0] = [G, G] = \Delta^{(1)}(G)$, and

$$\Gamma_2(G) = [G, \Gamma_1] = [G, \Delta^{(1)}(G)] \supseteq [\Delta^{(1)}(G), \Delta^{(1)}(G)] = \Delta^{(2)}(G),$$

and so, $\Gamma_2(G) \supseteq \Delta^{(2)}(G)$. The reader should check (DX) that $\Gamma_d(G) \supseteq \Delta^{(d)}(G)$, for all $d \geq 0$.

(2) $Z_1(G) =$ inverse image in G of $Z(G/Z_0) =$ inverse image of $Z(G)$, so $Z_1(G) = Z(G)$.

(3) If for some j, the equality $\Gamma_j(G) = \Gamma_{j+1}(G)$ holds, then $\Gamma_j(G) = \Gamma_d(G)$, for all $d \geq j$. The lower central series strictly descends until the first repetition.

(4) Similarly, if for some j, the equality $Z_j(G) = Z_{j+1}(G)$ holds, then $Z_j(G) = Z_d(G)$, for all $d \geq j$. The upper central series strictly ascends until the first repetition.

Proposition 1.31 *Suppose the lower central series of G reaches $\{1\}$ after r steps. Then, for every $j \leq r$, we have $\Gamma_{r-j} \subseteq Z_j$. Consequently, the upper central series reaches G after r steps. Conversely, suppose that the upper central series reaches G after r steps. Then, for every $j \leq r$, we have $\Gamma_j \subseteq Z_{r-j}$. Consequently, the lower central series reaches $\{1\}$ after r steps.*

Proof. By induction on j. For $j = 0$, we have $\Gamma_r = \Gamma_{r-0}$, and by hypothesis, $\Gamma_r = \{1\}$ and $Z_0 = \{1\}$, so the basis of the induction holds. Before we do the induction step, let us also consider the case $j = 1$. We need to show that $\Gamma_{r-1} \subseteq Z_1 = Z(G)$. But $\Gamma_r = \{1\}$, yet $\Gamma_r = [G, \Gamma_{r-1}]$. This means that for all $\sigma \in G$ and all $\tau \in \Gamma_{n-1}$, we have $[\sigma, \tau] \in \Gamma_r = \{1\}$. Thus, τ commutes with all $\sigma \in G$, and so, $\tau \in Z(G) = Z_1$. Let us now assume our statement, $\Gamma_{r-j} \subseteq Z_j$, for some j, and look at the case $j + 1$. Now, $\Gamma_{r-j} = [G, \Gamma_{r-j-1}]$. By the induction hypothesis,

$$[G, \Gamma_{r-j-1}] \subseteq Z_j.$$

Consider the map $G \longrightarrow G/Z_j = \overline{G}$. Then,

$$[\overline{G}, \overline{\Gamma}_{r-j-1}] = \{1\} \quad \text{in } \overline{G}.$$

Therefore, Γ_{r-j-1} is contained in the inverse image of $Z(\overline{G}) = Z(G/Z_j) = Z_{j+1}$, concluding the induction step.

For the converse, again, use induction on j. When $j = 0$, we have $\Gamma_0 = G$ and $Z_r = Z_{r-0} = G$, by hypothesis, and the basis of the induction holds. Assume that $\Gamma_j \subseteq Z_{r-j}$ for some j, and consider the case $j + 1$. We have

$$\Gamma_{j+1} = [G, \Gamma_j] \subseteq [G, Z_{r-j}],$$

by the induction hypothesis. Look at the map $G \longrightarrow G/Z_{r-j-1} = \overline{G}$. We have

$$\overline{\Gamma}_{j+1} \subseteq [\overline{G}, \overline{Z}_{r-j}].$$

But, by definition, $\overline{Z}_{r-j} = Z(\overline{G})$. Thus, $[\overline{G}, \overline{Z}_{r-j}] = \{1\}$ in $\overline{G}$. Therefore,
$\Gamma_{j+1} \subseteq \text{Ker } (G \longrightarrow \overline{G}) = Z_{r-j-1}$. $\square$

Definition 1.10 A group, G, is *nilpotent* if and only if the lower central series reaches $\{1\}$ after finitely many steps. The smallest number of steps, say c, is the *nilpotence class* of G. We write $G \in \mathcal{N}\text{ilp}(c)$. (We let $c = \infty$ if the LCS does not reach $\{1\}$ in finitely many steps.)

Remarks:

(1) $\mathcal{N}\text{ilp}(0)$ = the class consisting only of the trivial group.
$\mathcal{N}\text{ilp}(1)$ = the collection of abelian, nontrivial groups. If we let $\overline{\mathcal{N}\text{ilp}}(c)$ denote the union of the collections $\mathcal{N}\text{ilp}(k)$ for $k = 0, \ldots, c$, then it turns out that we have a strictly ascending chain

$$\mathcal{A}\text{b} = \overline{\mathcal{N}\text{ilp}}(1) < \overline{\mathcal{N}\text{ilp}}(2) < \overline{\mathcal{N}\text{ilp}}(3) < \cdots$$

of "worse and worse behaved" groups.

(2) We have $G \in \mathcal{N}\text{ilp}(c)$ iff the UCS reaches G after c steps and c is minimal with this property.

(3) Each nilpotent group is automatically solvable, but the converse is false, even for finite groups, even for small finite groups. Indeed, we observed earlier that $\Delta^{(r)}(G) \subseteq \Gamma_r(G)$. Therefore, $\delta(G) \leq$ nilpotence class of G. For a counter-example, take $G = \mathfrak{S}_3$. This group has order 6, its center is trivial, and so $Z_1 = Z_0$ and G is *not* nilpotent. Yet, we have an exact sequence

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathfrak{S}_3 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

and the extremes are solvable (even nilpotent, even abelian), so the middle is solvable.

(4) Every p-group is nilpotent. This is because the center of a p-group is nontrivial, so the UCS is strictly ascending and our group is finite; so, this implies that our group is nilpotent.

Remark: The fundamental groups of many spaces arising in geometry tend to be nilpotent groups.

Proposition 1.32 *(Modified Sylow III) Say G is a finite group, P is a p-Sylow subgroup of G and H is some subgroup of G. If $H \supseteq N_G(P)$, then $N_G(H) = H$.*

Proof. (Frattini Argument). Pick $\sigma \in N_G(H)$. Then, $\sigma H \sigma^{-1} = H$ and $\sigma P \sigma^{-1} \subseteq \sigma H \sigma^{-1}$ (since $H \supseteq N_G(P)$). So, P and $\sigma P \sigma^{-1}$ are two p-Sylow subgroups of H, and by Sylow II, there is some $\tau \in H$ so that $\tau P \tau^{-1} = \sigma P \sigma^{-1}$. Thus, $\tau^{-1}\sigma P (\tau^{-1}\sigma)^{-1} = P$, and so, $\tau^{-1}\sigma \in N_G(P) \subseteq H$, by hypothesis. So, $\sigma \in \tau H = H$ (since $\tau \in H$). $\square$

Theorem 1.33 *Let G be a finite group. Then, the following statements are equivalent:*

(1) G is nilpotent.

(2) G has property (N).

(3) Every maximal subgroup of G is normal.

(4) $\Delta^{(1)}(G) \subseteq \Phi(G)$.

(5) Every p-Sylow subgroup of G is normal in G.

(6) G is isomorphic to the product of its p-Sylow subgroups. (We write $G \cong \prod_p G_p$).

Proof. (1) $\Rightarrow$ (2). Let H be a proper subgroup of G, we must prove that $N_G(H) > H$. Now, there is some c with $\Gamma_c = \{1\}$. Obviously, $\Gamma_c \subseteq H$, so pick a smallest d for which $\Gamma_d \subseteq H$, so that $\Gamma_{d-1} \not\subseteq H$.

Claim: $\Gamma_{d-1} \subseteq N_G(H)$.

If the claim holds, then $H < N_G(H)$, *i.e.*, G has property (N). Pick $\xi \in \Gamma_{d-1}$; so,

$$[H, \xi] \subseteq [H, \Gamma_{d-1}] \subseteq [G, \Gamma_{d-1}] = \Gamma_d.$$

Pick $h \in H$ and look at $[h^{-1}, \xi]$. The element $[h^{-1}, \xi]$ is in Γ_d, and so, in H (since $\Gamma_d \subseteq H$). Consequently, $h^{-1}\xi h \xi^{-1} \in H$, from which we deduce $\xi h \xi^{-1} \in H$, and since this is true for all $h \in H$, we have $\xi \in N_G(H)$, as desired.

(2) $\Rightarrow$ (3). This has already been proved (c.f. Proposition 1.17).

(3) $\Rightarrow$ (4). This has already been proved (c.f. Proposition 1.23).

(4) $\Rightarrow$ (5). Let P be a p-Sylow subgroup of G. Look at $N_G(P)$. If $N_G(P) \neq G$, then $N_G(P)$ is contained is some maximal subgroup, M. By modified Sylow III, we get $N_G(M) = M$. Now, $\Delta^{(1)}(G) \subseteq \Phi(G) \subseteq M$, by hypothesis, and the second homomorphism theorem implies that M corresponds to a subgroup of $G/\Delta^{(1)}(G)$ and normal subgroups correspond to normal subgroups. Yet, $G/\Delta^{(1)}(G)$ is abelian, so all its subgroups are normal, which implies that M is normal, a contradiction.

(5) $\Rightarrow$ (6). This has already been proved (c.f. Proposition 1.18).

(6) $\Rightarrow$ (1). Since every p-group is nilpotent, the implication (6) $\Rightarrow$ (1) follows from the following

Proposition 1.34 *Say $G_j \in \mathcal{N}\mathrm{ilp}(c_j)$, for $j = 1, \ldots, t$. Then,*

$$\prod_{j=1}^{t} G_j \in \mathcal{N}\mathrm{ilp}(\max_{1 \leq j \leq t}\{c_j\}).$$

Proof. An obvious induction reduces us to the case $t = 2$. In this case, we use an induction on $\max\{c_1, c_2\}$. The cases $c_1 \leq 1$ and $c_2 \leq 1$ are trivial. Now, we have (DX)

$$Z(G_1 \prod G_2) \cong Z(G_1) \prod Z(G_2).$$

But then, $(G_1 \prod G_2)/Z(G_1 \prod G_2) \cong (G_1/Z(G_1)) \prod (G_2/Z(G_2))$; on the left hand side, the purported nilpotence class is down by 1 and on the righthand side, both are down by 1. We conclude by applying the induction hypothesis. $\square$

This concludes the proof of Theorem 1.33. $\square$

1.6 Ω-Groups and the Jordan-Hölder-Schreier Theorem

Let Ω be some set. If M is a group, we denote the monoid of group endomorphisms of M (under composition) by $\mathrm{End}_{\mathcal{G}\mathrm{r}}(M)$ and the group of (group) automorphisms of M by $\mathrm{Aut}_{\mathcal{G}\mathrm{r}}(M)$.

Definition 1.11 A group, M, is an Ω-*group* iff there exists a set map $\Omega \longrightarrow \mathrm{End}_{\mathcal{G}\mathrm{r}}(M)$. If Ω is itself a group, we demand that our map be a homomorphism (so, the image lies in $\mathrm{Aut}_{\mathcal{G}\mathrm{r}}(M)$). If Ω is a ring, we demand that M be an abelian group and that our map be a ring homomorphism taking $1 \in \Omega$ to the identity endomorphism of M.

Examples.

(1) When Ω is a group, we get an Ω-action on M (at first, as a set) and further, we obtain:

$$\begin{aligned} 1 \cdot m &= m, \\ \xi \cdot (\eta \cdot m) &= (\xi\eta) \cdot m, \\ \xi \cdot (mn) &= (\xi \cdot m)(\eta \cdot n). \end{aligned}$$

In particular, $(\xi \cdot m)^{-1} = \xi \cdot m^{-1}$.

(2) When Ω is a group and M is abelian, we just get an Ω-*module*.

(3) If Ω is a ring, then the nomenclature is Ω-*module* instead of Ω-group.

(4) When Ω is a field, then an Ω-module is a vector space over Ω.

(5) Being an $\mathbb{Z}$-module is equivalent to being an abelian group.

An Ω-*subgroup* of M (resp. Ω-*normal subgroup* of M) is just a subgroup (resp. a normal subgroup), N, of M stable under Ω, *i.e.*, for all $\xi \in \Omega$, for all $n \in N$, we have $\xi \cdot n \in N$.

Blanket Assertion (DX). The three isomorphism theorems of ordinary group theory are true for Ω-groups provided everywhere "subgroup" appears we substitute "Ω-subgroup", *mutatis–mutandis* for "normal subgroups."

Definition 1.12 A *normal flag* (*normal series, normal chain*) is a descending chain of Ω-subgroups of M:

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_r = \{1\}, \tag{$*$}$$

each M_j being normal in the preceding M_{j-1}. A normal flag is *nonrepetitious* if for no j do we have $M_j = M_{j-1}$. Given a second normal flag:

$$M = M_0' \supseteq M_1' \supseteq M_2' \supseteq \cdots \supseteq M_s' = \{1\}, \tag{$**$}$$

the flag $(**)$ *refines* $(*)$ iff for every i the Ω-group M_i occurs as some M_j'. Two normal flags $(*)$ and $(**)$ are isomorphic iff the collection of their successive quotients, M_{i-1}/M_i and M_{j-1}'/M_j' may be rearranged so that, after rearrangement, they become pairwise isomorphic (in their new order). When this happens, the lengths r and s are equal.

Theorem 1.35 *(Schreier refinement theorem, 1928) For an Ω-group, any two normal flags possess isomorphic refinements. If both normal flags are nonrepetitious, so are their isomorphic refinements.*

The main corollary of the Schreier refinement theorem is:

Corollary 1.36 *(Jordan–Hölder theorem) Any two composition series for an Ω-group are isomorphic.*

Proof. A composition series has *no* refinements except itself—apply Schreier's theorem. □

Zassenhaus proved a lemma specifically designed to give the smoothest proof of Schreier's theorem—this is

Lemma 1.37 *(Zassenhaus' butterfly lemma) Say G is an Ω-group and A and C are subgroups. Suppose $B \lhd A$ and $D \lhd C$ are further Ω-subgroups. Then,*

$$(A \cap C)B/(A \cap D)B \cong (C \cap A)D/(C \cap B)D.$$

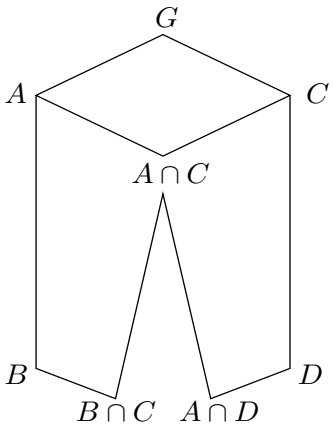


Figure 1.1: The butterfly lemma

Proof. Let $T = A \cap C = C \cap A$, $M = B \cap C$ and $N = A \cap D$. The conclusion of the lemma is

$$TB/NB \cong TD/MD.$$

First of all, there is right-left symmetry in the statement of the lemma and its conclusion ($A \leftrightarrow C$, $B \leftrightarrow D$; under these substitutions, $T \leftrightarrow T$ and $M \leftrightarrow N$). We must prove that $NB \lhd TB$. Pick $t \in G$ and look at $tNBt^{-1} = tNt^{-1}tBt^{-1}$. If $t \in A$, then $tBt^{-1} = B$, since $B \lhd A$. Thus, *if $t \in A$ then $tNBt^{-1} = tNt^{-1}B$*. If $t \in T \subseteq C$, then as $N = D \cap C \cap A = D \cap T$ and $D \lhd C$, we get

$$tNt^{-1} = tDt^{-1} \cap tTt^{-1} = tDt^{-1} \cap T = D \cap T = N.$$

Thus, *if $t \in T$ then $tNBt^{-1} = NB$*.

Say $\xi = tb \in TB$. Since $B \lhd A$ and $N \subseteq A$, we have $BN = NB$. Then, we find

$$\begin{aligned} \xi NB\xi^{-1} &= tbNBb^{-1}t^{-1} \\ &= tbNBt^{-1} \\ &= tbBNt^{-1} \\ &= tBNt^{-1} \\ &= tNBt^{-1} \\ &= NB. \end{aligned}$$

Therefore, $NB \lhd TB$. By symmetry, we get $MD \lhd TD$. Look at $TB/NB = TNB/BN$ (since $N \subseteq T$). By the third isomorphism theorem, we have

$$TB/NB \cong T/T \cap NB.$$

By symmetry,

$$TD/ND \cong T/T \cap MD.$$

If we prove that $T \cap NB = T \cap NM$ (and so, $T \cap MD = T \cap NM$, by symmetry), we will be done. Pick $\xi \in T \cap NB$. We can write $\xi = nb \in NB$, so $b = n^{-1}\xi \in NT = T$ (since $N \subseteq T$). Thus, $b \in B \cap T = B \cap C \cap A \subseteq M$, and so, $b \in M$. Consequently, $\xi = nb \in NM$ and since we also have $\xi \in T$, then $\xi \in T \cap NM$. This proves that $T \cap NB \subseteq T \cap NM$. The reverse inclusion is trivial, since $M \subseteq B$. Therefore, $T \cap NB = T \cap NM$, as claimed. □

Proof of Theorem 1.35. Let

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots M_{i-1} \supseteq M_i \supseteq \cdots \supseteq M_r = \{1\}, \tag{$*$}$$

and

$$M = M'_0 \supseteq M'_1 \supseteq M'_2 \supseteq \cdots M'_{j-1} \supseteq M'_j \supseteq \cdots \supseteq M'_s = \{1\}, \tag{$**$}$$

be two normal nonrepetitious chains. Consider the groups

$$M_{i-1}^{(j)} = (M_{i-1} \cap M'_j)M_i.$$

As j varies, these groups start at M_{i-1} $(= M_{i-1}^{(0)})$ and end at M_i $(= M_{i-1}^{(s)})$ and we get a refinement of $(*)$ if we do this between any pair in $(*)$. Also consider the groups

$$M_{j-1}^{'(i)} = (M'_{j-1} \cap M_i)M'_j,$$

and let i vary. These groups interpolate between M'_{j-1} and M'_j, just as above. Look at the successive quotients

$$M_{i-1}^{(j-1)}/M_{i-1}^{(j)}; \quad M_{j-1}^{'(i-1)}/M_{j-1}^{'(i)}. \tag{$\dagger$}$$

If we let $A = M_{i-1}$, $B = M_i$ $(\lhd A)$, $C = M'_{j-1}$ and $D = M'_j$ $(\lhd C)$, we can write the first quotient group of $(\dagger)$ as

$$M_{i-1}^{(j-1)}/M_{i-1}^{(j)} = (M_{i-1} \cap M'_{j-1})M_i/(M_{i-1} \cap M'_j)M_i = (A \cap C)B/(A \cap D)B,$$

the left hand side of Zassenhaus' lemma. By symmetry, the second quotient group of $(\dagger)$ is the righthand side of Zassenhaus' lemma and we are done. □

1.7 Categories, Functors and Free Groups

Definition 1.13 A *category*, $\mathcal{C}$, is a pair: $\langle \mathcal{O}\mathrm{b}(\mathcal{C}), \mathcal{F}\mathrm{l}(\mathcal{C})\rangle$, in which $\mathcal{O}\mathrm{b}(\mathcal{C})$ and $\mathcal{F}\mathrm{l}(\mathcal{C})$ are classes, called the *objects of* $\mathcal{C}$ and the *morphisms* (or *arrows*) *of* $\mathcal{C}$, respectively. We require the following conditions:

(1) For all $A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$, there is a unique **set**, $\mathrm{Hom}_{\mathcal{C}}(A, B)$, called the collection of *morphisms from* A *to* B, and any two such are either disjoint or equal. Further

$$\mathcal{F}\mathrm{l}(\mathcal{C}) = \bigcup_{A,B} \mathrm{Hom}_{\mathcal{C}}(A, B).$$

For the morphisms, we also require:

(2) For every $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $v \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, there exists a unique morphism $w = v \circ u \in \mathrm{Hom}_{\mathcal{C}}(A, C)$, called the *composition* of v and u.

(3) For every $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$, there is some arrow, $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$, so that for every $B \in \mathcal{O}\mathrm{b}(\mathcal{C})$ and $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, we have

$$\begin{aligned} A \xrightarrow{1_A} A \xrightarrow{u} B &= A \xrightarrow{u} B \\ A \xrightarrow{u} B \xrightarrow{1_B} B &= A \xrightarrow{u} B. \end{aligned}$$

Note: This shows that 1_A is unique for each A (DX).

(4) We have the associativity law

$$u \circ (v \circ w) = (u \circ v) \circ w,$$

whenever the compositions all make sense.

Examples of Categories:

(1) $\mathcal{S}$ets, the category of sets; $\mathcal{O}\mathrm{b}(\mathcal{S}\mathrm{ets})$ = all sets, $\mathcal{F}\mathrm{l}(\mathcal{S}\mathrm{ets})$ = all maps of sets.

(2) $\mathcal{G}$r, the category of groups; $\mathcal{O}\mathrm{b}(\mathcal{G}\mathrm{r})$ = all groups, $\mathcal{F}\mathrm{l}(\mathcal{G}\mathrm{r})$ = all homomorphisms of groups. A special case is $\mathcal{A}$b, the category of abelian groups.

(3) Ω-$\mathcal{G}$r, the category of Ω-groups. Special cases are: The category of G-modules, $\mathcal{M}\mathrm{od}(G)$; the category of R-modules, $\mathcal{M}\mathrm{od}(R)$ (where R is a ring); and the category of vector spaces, $\mathrm{Vect}(k)$ (where k is a field). Also, $\mathcal{A}\mathrm{b} = \mathcal{M}\mathrm{od}(\mathbb{Z})$.

(4) TOP, the category of topological spaces; $\mathcal{O}\mathrm{b}(\mathrm{TOP})$ = all topological spaces, $\mathcal{F}\mathrm{l}(\mathrm{TOP})$ = all continuous maps.

(5) C^k-MAN, the category of C^k-manifolds; $\mathcal{O}\mathrm{b}(C^k\text{-MAN})$ = all (real) C^k-manifolds ($0 \leq k \leq \infty$ or ω), $\mathcal{F}\mathrm{l}(C^k\text{-MAN})$ = all C^k-maps of C^k-manifolds.

(6) HOL, the category of complex analytic manifolds; $\mathcal{O}\mathrm{b}(\mathrm{HOL})$ = all complex analytic manifolds, $\mathcal{F}\mathrm{l}(\mathrm{HOL})$ = all complex analytic maps of holomorphic manifolds.

(7) RNG, the category of all rings; $\mathcal{O}\mathrm{b}(\mathrm{RNG})$ = all rings (with unity), $\mathcal{F}\mathrm{l}(\mathrm{RNG})$ = all homomorphisms of rings. A special case is CR, the category of commutative rings.

A *subcategory*, $\mathcal{D}$, of $\mathcal{C}$ is a category, $\langle \mathcal{O}\mathrm{b}(\mathcal{D}), \mathcal{F}\mathrm{l}(\mathcal{D})\rangle$, so that

(a) $\mathcal{O}\mathrm{b}(\mathcal{D}) \subseteq \mathcal{O}\mathrm{b}(\mathcal{C})$.

(b) $\mathcal{F}\mathrm{l}(\mathcal{D}) \subseteq \mathcal{F}\mathrm{l}(\mathcal{C})$, in such a way that for all $A, B \in \mathcal{O}\mathrm{b}(\mathcal{D})$, we have $\mathrm{Hom}_{\mathcal{D}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A, B)$.

We say that $\mathcal{D}$ is a *full subcategory* of $\mathcal{C}$ iff for all $A, B \in \mathcal{O}\mathrm{b}(\mathcal{D})$, we have $\mathrm{Hom}_{\mathcal{D}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Examples of Subcategories:

(1) The category, $\mathcal{A}\mathrm{b}$, is a full subcategory of $\mathcal{G}\mathrm{r}$; the category, CR, is a full subcategory of RNG.

(2) Recall that $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is an *isomorphism* (in $\mathcal{C}$) iff there is some $v \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ so that

$$\begin{aligned} A \xrightarrow{u} B \xrightarrow{v} A &= A \xrightarrow{1_A} A \\ B \xrightarrow{v} A \xrightarrow{u} B &= B \xrightarrow{1_B} B. \end{aligned}$$

Take $\mathcal{D}$ so that $\mathcal{O}\mathrm{b}(\mathcal{D}) = \mathcal{O}\mathrm{b}(\mathcal{C})$, and morphisms, set $\mathrm{Hom}_{\mathcal{D}}(A, B) = \{u \in \mathrm{Hom}_{\mathcal{C}}(A, B) \mid u \text{ is an isomorphism}\}$ and $\mathcal{F}\mathrm{l}(\mathcal{D}) = \bigcup_{A,B} \mathrm{Hom}_{\mathcal{D}}(A, B)$. (Note that $\mathrm{Hom}_{\mathcal{D}}(A, B)$ may be empty.) The category, $\mathcal{D}$, is generally a nonfull subcategory of $\mathcal{C}$, for example when $\mathcal{C} = \mathcal{S}\mathrm{ets}$.

Say $\mathcal{C}$ is a category, we can make a new category, $\mathcal{C}^D$, the *dual* or *opposite category*, as follows: $\mathcal{O}\mathrm{b}(\mathcal{C}^D) = \mathcal{O}\mathrm{b}(\mathcal{C})$ and reverse the arrows, *i.e.*, for all $A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$,

$$\mathrm{Hom}_{\mathcal{C}^D}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A).$$

Definition 1.14 Let $\mathcal{C}$ and $\mathcal{C}'$ be categories. A *functor* (respectively, a *cofunctor*), F, from $\mathcal{C}$ to $\mathcal{C}'$ is a rule which associates to each object $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$ an object $F(A) \in \mathcal{O}\mathrm{b}(\mathcal{C}')$ and to each arrow $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ an arrow $F(u) \in \mathrm{Hom}_{\mathcal{C}'}(F(A), F(B))$ (resp. $F(u) \in \mathrm{Hom}_{\mathcal{C}'}(F(B), F(A))$) so that,

$$\begin{aligned} F(1_A) &= 1_{F(A)} \\ F(u \circ v) &= F(u) \circ F(v) \\ (\text{resp. } F(u \circ v) &= F(v) \circ F(u), \quad \text{for cofunctors.}) \end{aligned}$$

Remark: Obviously, Definition 1.14 can be made more formal by defining a functor, F, from $\mathcal{C}$ to $\mathcal{C}'$ as a pair, $\langle F^{\mathrm{ob}}, F^{\mathrm{fl}} \rangle$, where $F^{\mathrm{ob}} \colon \mathcal{O}\mathrm{b}(\mathcal{C}) \to \mathcal{O}\mathrm{b}(\mathcal{C}')$ and $F^{\mathrm{fl}} \colon \mathcal{F}\mathrm{l}(\mathcal{C}) \to \mathcal{F}\mathrm{l}(\mathcal{C}')$, so that, for every $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, we have $F^{\mathrm{fl}}(u) \in \mathrm{Hom}_{\mathcal{C}'}(F^{\mathrm{ob}}(A), F^{\mathrm{ob}}(B))$, and the conditions of Definition 1.14 hold (and similarly for cofunctors).

We use the notation $A \rightsquigarrow F(A)$ (or $u \rightsquigarrow F(u)$) to indicate that $F \colon \mathcal{C} \to \mathcal{C}'$ is a functor from $\mathcal{C}$ to $\mathcal{C}'$, and not just an ordinary function.

Examples of Functors

(1) For the categories in Examples (2)–(7), consider the rule:
$A \in \mathcal{O}\mathrm{b}(\mathcal{C}) \rightsquigarrow |A| =$ the underlying set of A, and
$u \in \mathcal{F}\mathrm{l}(\mathcal{C}) \rightsquigarrow |u| =$ the morphism, u, as a map of sets.
The functor, $|\ |$, is a functor from $\mathcal{C}$ to $\mathcal{S}\mathrm{ets}$, called the *forgetful functor* or *stripping functor*.

(2) A cofunctor, $F \colon \mathcal{C} \to \mathcal{C}'$, is just a functor, $F \colon \mathcal{C}^{\mathcal{D}} \to \mathcal{C}'$ (equivalently, $F \colon \mathcal{C} \to \mathcal{C}'^{D}$).

(3) We have the functor, $\mathbb{G}_a \colon \mathrm{RNG} \to \mathcal{A}\mathrm{b}$, given by taking $\mathbb{G}_a(R) = R$ as an additive group, for every ring, R. The functor, $\mathbb{G}_a$, is called the *additive group functor*.

(4) For every integer, $n \geq 0$, we have the functor, $\mathrm{GL}_n\colon \mathrm{CR} \to \mathcal{G}\mathrm{r}$, where $\mathrm{GL}_n(A)$ is the group of invertible $n \times n$ matrices with entries in A. When $n = 1$, the group GL_1 is denoted $\mathbb{G}_m$. This is the *multiplicative group functor*, it takes CR to $\mathcal{A}\mathrm{b}$. The functor $\mathbb{G}_m$ can be promoted to a functor, RNG $\longrightarrow \mathcal{G}\mathrm{r}$, taking the ring, A, to its group, A^*, of units.

(5) Let $(\mathrm{TOP}, *)$ be the category of topological spaces together with a base point. We have the subcategory $(\text{C-TOP}, *)$ consisting of connected and locally connected topological spaces with a base point. The morphisms of $(\text{C-TOP}, *)$ preserve base points. We have the functors (fundamental group)

$$\pi_1\colon (\text{C-TOP}, *) \to \mathcal{G}\mathrm{r},$$

and for $n > 1$ (nth homotopy group),

$$\pi_n\colon (\text{C-TOP}, *) \to \mathcal{A}\mathrm{b}.$$

(6) For every integer, $n \geq 0$, we have a functor (integral homology), TOP $\longrightarrow \mathcal{A}\mathrm{b}$, given by $X \rightsquigarrow H_n(X, \mathbb{Z})$ and a cofunctor (integral cohomology), TOP $\longrightarrow \mathcal{A}\mathrm{b}$, given by $X \rightsquigarrow H^n(X, \mathbb{Z})$.

(7) math.upenn.edu/ Given a group, G, for any integer, $n \geq 0$, we have a functor, $\mathcal{M}\mathrm{od}(G) \longrightarrow \mathcal{A}\mathrm{b}$, given by $A \rightsquigarrow H^n(G, A)$.

Definition 1.15 Say F and F' are two functors $\mathcal{C} \longrightarrow \mathcal{C}'$. A *morphism*, θ, from F to F' is a collection $\{\theta_A \mid A \in \mathcal{O}\mathrm{b}(\mathcal{C})\}$, where:

(1) $\theta_A\colon F(A) \to F'(A)$ in $\mathcal{C}'$, so that (consistency)

(2) For every $v\colon A \to B$ in $\mathcal{C}$, the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{\theta_A} & F'(A) \\ {\scriptstyle F(v)}\downarrow & & \downarrow{\scriptstyle F'(v)} \\ F(B) & \xrightarrow{\theta_B} & F'(B) \end{array}$$

commutes, for all $A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$.

A morphism of functors is also called a *natural transformation* of functors.

Examples of Morphisms of Functors:

(1) In the category $(\text{C-TOP}, *)$, we have the functors π_1 and $H_1(-, \mathbb{Z})$. The Hurewicz map

$$\pi_1(X) \xrightarrow{u_X} H_1(X, \mathbb{Z})$$

defines a morphism of functors.

(2) If G is a group and K is a subgroup of G, we have the obvious restriction functor $\mathrm{res}\colon \mathcal{M}\mathrm{od}(G) \to \mathcal{M}\mathrm{od}(K)$, and it induces a morphism of functors $\mathrm{res}\colon H^n(G, -) \to H^n(K, -)$.

(3) The determinant, $\det\colon \mathrm{GL}_n \to \mathbb{G}_m$, is a morphism of functors (from CR to $\mathcal{A}\mathrm{b}$).

(4) Check (DX) that with the above notion of morphisms, the functors from $\mathcal{C}$ to $\mathcal{C}'$ form a category themselves. This category is denoted $\mathrm{Fun}(\mathcal{C}, \mathcal{C}')$.

Proposition 1.38 *Given a category, $\mathcal{C}$, each object, A, of $\mathcal{C}$ gives rise to both a functor, h_A, and a cofunctor, h_A^D, from $\mathcal{C}$ to $\mathcal{S}$ets.*

Proof. For any given $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$, let

$$\begin{aligned} h_A(B) &= \mathrm{Hom}_{\mathcal{C}}(A, B) \\ h_A^D(B) &= \mathrm{Hom}_{\mathcal{C}}(B, A). \end{aligned}$$

Moreover, for every $v \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, define $h_A(v)\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$ by composition, so that for every $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$,

$$h_A(v)(u) = v \circ u,$$

and, for every $v \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, define $h_A^D(v)\colon \mathrm{Hom}_{\mathcal{C}}(C, A) \to \mathrm{Hom}_{\mathcal{C}}(B, A)$, again by composition, so that for every $u \in \mathrm{Hom}_{\mathcal{C}}(C, A)$,

$$h_A^D(v)(u) = u \circ v.$$

The reader should check that h_A and h_A^D are indeed functors (DX). □

The following proposition is half of the Yoneda embedding lemma:

Proposition 1.39 *Let A and $\widetilde{A}$ be two objects of $\mathcal{C}$ and suppose that the corresponding functors h_A and $h_{\widetilde{A}}$ are isomorphic, say by $\theta\colon h_A \to h_{\widetilde{A}}$. Then, A and $\widetilde{A}$ are isomorphic via a canonically determined isomorphism (dependent on θ).*

Proof. For every $B \in \mathcal{O}\mathrm{b}(\mathcal{C})$, we have an isomorphism

$$\theta_B\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(\widetilde{A}, B),$$

and this is functorial. Let $B = A$, then $\theta_A\colon \mathrm{Hom}_{\mathcal{C}}(A, A) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(\widetilde{A}, A)$, and we set $\psi = \theta_A(1_A)$, a morphism in $\mathrm{Hom}_{\mathcal{C}}(\widetilde{A}, A)$. Now, if we let $B = \widetilde{A}$, we get $\theta_{\widetilde{A}}\colon \mathrm{Hom}_{\mathcal{C}}(A, \widetilde{A}) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(\widetilde{A}, \widetilde{A})$, and we set $\varphi = \theta_{\widetilde{A}}^{-1}(1_{\widetilde{A}})$, a morphism in $\mathrm{Hom}_{\mathcal{C}}(A, \widetilde{A})$. Pick any z in $\mathrm{Hom}_{\mathcal{C}}(A, B)$. We would like to understand what $\theta_B(z)$ is. We have the commutative diagram

$$\begin{array}{ccc} z \in \mathrm{Hom}_{\mathcal{C}}(A, B) & \xrightarrow{\theta_B} & \mathrm{Hom}_{\mathcal{C}}(\widetilde{A}, B) \\ {\scriptstyle z\circ -}\uparrow & & \uparrow{\scriptstyle z\circ -} \\ 1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A) & \xrightarrow[\theta_A]{} & \mathrm{Hom}_{\mathcal{C}}(\widetilde{A}, A). \end{array}$$

Following the above commutative diagram clockwise, we get $\theta_B(z)$, and following it counterclockwise, we get $z \circ \psi$. We conclude that

$$\theta_B(z) = z \circ \psi.$$

Similarly, for any $\widetilde{z} \in \mathrm{Hom}_{\mathcal{C}}(\widetilde{A}, B)$, by considering the commutative diagram involving $\theta_{\widetilde{A}}^{-1}$ and θ_B^{-1}, we get

$$\theta_B^{-1}(\widetilde{z}) = \widetilde{z} \circ \varphi.$$

But then, we have

$$1_{\widetilde{A}} = \theta_{\widetilde{A}}(\varphi) = \varphi \circ \psi \quad \text{and} \quad 1_A = \theta_A^{-1}(\psi) = \psi \circ \varphi,$$

which shows that φ and ψ are inverse isomorphisms. Furthermore, φ (resp. ψ) determine θ, just as θ determines φ and ψ. □

Example. Recall that $\mathrm{Vect}(k)$ is the category of vector spaces over a field, k. There exists a cofunctor, $D\colon \mathrm{Vect}(k) \longrightarrow \mathrm{Vect}(k)$, given by: $V \rightsquigarrow V^D = \mathrm{Hom}_{\mathrm{Vect}(k)}(V, k) =$ the dual space of V; and for any linear map, $\theta\colon V \to W$, the map $\theta^D\colon W^D \to V^D$ is the adjoint of θ. By applying D again, we get a functor, $DD\colon \mathrm{Vect}(k) \longrightarrow \mathrm{Vect}(k)$. However, it is well-known that there exists a morphism of functors,
$\eta\colon \mathrm{id} \to DD$, where $\mathrm{id}(V) = V \xrightarrow{\eta_V} DD(V) = V^{DD}$, and this is functorial.

Two categories, $\mathcal{C}$ and $\mathcal{C}'$, are *equivalent* (resp. *isomorphic*) iff there exist functors $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ so that $F' \circ F \cong 1_{\mathcal{C}}$ and $F \circ F' \cong 1_{\mathcal{C}'}$ (resp. $F' \circ F = 1_{\mathcal{C}}$ and $F \circ F' = 1_{\mathcal{C}'}$). Here $1_{\mathcal{C}}$ denotes the identity functor from $\mathcal{C}$ to itself.

Proposition 1.40 *(Yoneda's Embedding Lemma) The functor $A \rightsquigarrow h^D_A$ establishes an equivalence of the category, $\mathcal{C}$, with a full subcategory of* $\mathrm{Fun}^D(\mathcal{C}, \mathcal{S}\mathrm{ets})$ *(where* $\mathrm{Fun}^D(\mathcal{C}, \mathcal{C}')$ *denotes the category of cofunctors from $\mathcal{C}$ to $\mathcal{C}'$).*

Proof. We already know from Proposition 1.39 that if we have an isomorphism $\theta\colon h^D_A \to h^D_{\widetilde{A}}$, then θ determines uniquely two mutually inverse isomorphisms $\psi\colon A \to \widetilde{A}$ and $\varphi\colon \widetilde{A} \to A$. So, two objects A and $\widetilde{A}$ in $\mathcal{O}\mathrm{b}(\mathcal{C})$ give isomorphic cofunctors iff they themselves are isomorphic. Given any $v \in \mathrm{Hom}_{\mathcal{F}}(h^D_A, h^D_{\widetilde{A}})$, where $\mathcal{F} = \mathrm{Fun}^D(\mathcal{C}, \mathcal{S}\mathrm{ets})$, we know (again) that there exists a morphism $\psi\colon A \to \widetilde{A}$, so that v is given by composing with ψ, *i.e.*, given a consistent family of morphisms, $v_B\colon h^D_A(B) \to h^D_{\widetilde{A}}(B)$, that is,
$v_B\colon \mathrm{Hom}_{\mathcal{C}}(B, A) \to \mathrm{Hom}_{\mathcal{C}}(B, \widetilde{A})$, we have $v_B(z) = \psi \circ z$, and our ψ is given by $\psi = v_A(1_A)$ (all this from the proof of Proposition 1.39). Hence, from v, we get a morphism $\psi\colon A \to \widetilde{A}$, thus

$$\mathrm{Hom}_{\mathcal{C}}(A, \widetilde{A}) \cong \mathrm{Hom}_{\mathcal{F}}(h^D_A, h^D_{\widetilde{A}}).$$

So, we indeed have an equivalence with a full subcategory of $\mathcal{F}$, namely the image consists of those cofunctors of the form h^D_A (easy details are left to the reader (DX)). □

Remark: What does Yoneda's lemma say? It says that any object $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$ is determined by its corresponding cofunctor h^D_A. The cofunctor, h^D_A, is a "collection of interconnected sets", $\mathrm{Hom}_{\mathcal{C}}(B, A)$ being the set associated with B.

Definition 1.16 Given a functor, F, from $\mathcal{C}$ to $\mathcal{S}\mathrm{ets}$ (resp. a cofunctor, G, from $\mathcal{C}^D$ to $\mathcal{S}\mathrm{ets}$), it is *representable* iff there exists a pair, (A, ξ), where $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$ and $\xi \in F(A)$, so that F is *isomorphic* to h_A *via* the morphism of functors, $\widetilde{\xi}\colon h_A \to F$, given by the consistent family of morphisms $\widetilde{\xi}_B\colon \mathrm{Hom}_{\mathcal{C}}(A, B) \to F(B)$ defined *via*

$$\widetilde{\xi}_B(u) = F(u)(\xi),$$

(resp. G is *isomorphic* to h^D_A *via* the morphism of functors, $\widetilde{\xi}\colon h^D_A \to G$, given by $\widetilde{\xi}_B\colon \mathrm{Hom}_{\mathcal{C}}(B, A) \to G(B)$. Here, $\widetilde{\xi}_B$ is defined *via* $\widetilde{\xi}_B(u) = G(u)(\xi)$).

The notion of representable functor is a key concept of modern mathematics. The underlying idea is to "lift" as much as possible of the knowledge we have about the category of sets to other categories. More specifically, we are interested in those functors from a category $\mathcal{C}$ to $\mathcal{S}\mathrm{ets}$ that are of the form h_A for some object $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$.

Remark: If (A, ξ) and (A', ξ') represent the same functor, then there exists *one and only one* isomorphism $A \xrightarrow{\sim} A'$ so that $\xi \in F(A)$ maps to $\xi' \in F(A')$. This is because we have the isomorphisms $\widetilde{\xi}\colon h_A \xrightarrow{\sim} F$ and $\widetilde{\xi'}\colon h_{A'} \xrightarrow{\sim} F$; and so, we have an isomorphism $\widetilde{\xi'}^{-1} \circ \widetilde{\xi}\colon h_A \xrightarrow{\sim} h_{A'}$. By Yoneda's lemma, $A \xrightarrow{\sim} A'$ *via* the isomorphism determined by $\widetilde{\xi}$ and $\widetilde{\xi'}$ and this maps ξ to ξ'. Uniqueness follows as everything is determined by ξ and ξ'.

Examples of Representable Functors:

(1) Let $\mathcal{C} = \mathcal{S}\mathrm{ets}$; consider the functor $F\colon \mathcal{S}\mathrm{ets}^D \to \mathcal{S}\mathrm{ets}$ given by: $F(S) =$ the collection of all subsets of S, and if $\theta\colon S \to T$ is a map of sets, the morphism $F(\theta)\colon F(T) \to F(S)$ is the map that sends every subset, V, of T to its inverse image, $\theta^{-1}(V)$, a subset of S. Is this a representable functor?

We need a set, Q, and an element, $\xi \in F(Q)$, i.e., some subset of Q, so that

$$h^D_Q(B) = \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(B, Q) \xrightarrow{\sim} F(B), \quad \textit{via } \widetilde{\xi}_B(u) = F(u)(\xi).$$

Now, we know that $F(u)\colon F(Q) \to F(B)$ is the map that sends a subset, S, of Q to its inverse image, $u^{-1}(S)$, a subset of B. So, $F(u)(\xi)$ is the inverse image of our chosen ξ.

Take $Q = \{0, 1\}$ and $\xi = \{1\} \subseteq Q$. Then, subsets of B are exactly of the form, $u^{-1}(1)$, for the various $u \in \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(B, Q)$, which are thus characteristic functions.

(2) Let $\mathcal{C} = \mathrm{RNG}$, and let $F\colon \mathrm{RNG} \to \mathcal{S}\mathrm{ets}$ be the stripping functor. Is it representable?

We need a ring, P, and an element, $\xi \in P$, so that for all rings, B,

$$\mathrm{Hom}_{\mathrm{RNG}}(P, B) \xrightarrow{\sim} |B|,$$

via

$$u \in \mathrm{Hom}_{\mathrm{RNG}}(P, B) \mapsto u(\xi) \in |B|.$$

Take $P = \mathbb{Z}[T]$, the polynomial ring in one variable with integral coefficients, and $\xi = T$. Then, any ring homomorphism $u \in \mathrm{Hom}_{\mathrm{RNG}}(\mathbb{Z}[T], B)$ is uniquely determined by $u(T) = b \in |B|$, and **any** b can be used.

Definition 1.17 Let $F\colon \mathcal{C} \to \mathcal{C}'$ and $G\colon \mathcal{C}' \to \mathcal{C}$ be two functors. The functor F is the *left (resp. right) adjoint* of G iff for every $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$ and $B \in \mathcal{O}\mathrm{b}(\mathcal{C}')$, we have functorial isomorphisms (in both A and B)

$$\begin{aligned} &\mathrm{Hom}_{\mathcal{C}'}(F(A), B) \quad \xrightarrow{\sim} \quad \mathrm{Hom}_{\mathcal{C}}(A, G(B)). \\ (\text{resp. } &\mathrm{Hom}_{\mathcal{C}'}(B, F(A)) \quad \xrightarrow{\sim} \quad \mathrm{Hom}_{\mathcal{C}}(G(B), A)). \end{aligned}$$

Observe that F is left-adjoint to G iff G is right-adjoint to F. Many so-called "universal constructions" arise from the existence of adjoint functors; this is a key concept in modern mathematics.

Remark: The concept of adjointness is related to the notion of representability of a functor, as shown by the following proposition whose simple proof is left to the reader:

Proposition 1.41 *A functor, $G\colon \mathcal{C}' \to \mathcal{C}$, has a left-adjoint if and only if, for every $A \in \mathcal{C}$, the functor $B \rightsquigarrow \mathrm{Hom}_{\mathcal{C}}(A, G(B))$ from $\mathcal{C}'$ to $\mathcal{S}\mathrm{ets}$ is representable. If $(F(A), \xi)$ represents this functor (so that $\widetilde{\xi}_B\colon \mathrm{Hom}_{\mathcal{C}'}(F(A), B) \cong \mathrm{Hom}_{\mathcal{C}}(A, G(B))$ is an isomorphism for every $B \in \mathcal{C}'$), then F is the object part of a left-adjoint of G for which the isomorphism $\widetilde{\xi}_B$ is functorial in B and yields the adjointness.*

A functor may have a right adjoint, but no left adjoint, and conversely (or no adjoint at all). For example, the functor, $G \rightsquigarrow G/[G, G] = G^{ab}$, from $\mathcal{G}\mathrm{r}$ to $\mathcal{A}\mathrm{b}$, is the left adjoint of the inclusion functor from $\mathcal{A}\mathrm{b}$ to $\mathcal{G}\mathrm{r}$. The inclusion views an abelian group just as a group. So, $G \rightsquigarrow G^{ab}$ has a right adjoint. However, we now prove that it has no left adjoint.

Suppose such a left adjoint, F, exists.

Claim 1: For any abelian group, H, the group $F(H)$ can never be simple unless $F(H) = \{1\}$, in which case, $H = \{1\}$.

The adjointness property states that for every group, G, we have a functorial isomorphism

$$\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(F(H), G) \cong \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(H, G^{ab}). \qquad (*)$$

If we take $G = F(H)$ in $(*)$, we have

$$\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(F(H), F(H)) \cong \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(H, F(H)^{ab}).$$

If $F(H) \neq \{1\}$ and $F(H)$ is non-abelian simple, then, on the left hand side there are at least two maps (id and the constant map that sends all elements to 1), even though on the righthand side there is a single

map, since $F(H)$ is non-abelian simple, a contradiction. If $F(H)$ is $\mathbb{Z}/p\mathbb{Z}$ for some prime p, take G in $(*)$ to be A_{3p}. Again, there are at least two maps in $\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(F(H), A_{3p})$, namely: the constant map and an embedding. But A_{3p} is simple; so, the righthand side has only one element, again a contradiction. Now, if $F(H) = \{1\}$, take $G = H$ in $(*)$. In this case, the left hand side has a single map but the righthand side has at least two maps if $H \neq \{1\}$.

Claim 2: $F(H)$ has no maximal normal subgroups. If $M \lhd F(H)$ and M is maximal, then $F(H)/M$ is simple. Let $G = F(H)/M$ in $(*)$. If $F(H)/M$ is non-abelian, there are at least two maps on the left hand side, but only one on the righthand side, a contradiction. If $F(H)/M$ is abelian, say $\mathbb{Z}/p\mathbb{Z}$, again take $G = A_{3p}$ in $(*)$. There are two maps (at least) on the left hand side (stemming from the two maps $F(H) \longrightarrow F(H)/M$) and only one on the righthand side. So, if $F(H)$ exists, it is not finitely generated.

Take $H = G = \mathbb{Z}/2\mathbb{Z}$. Then, we have

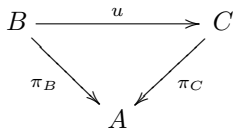
$$\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(F(\mathbb{Z}/2\mathbb{Z}), \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}).$$

Clearly, the righthand side has exactly two maps, and thus, so does the left hand side. But one of these maps is the constant map sending all elements to 1, so the other map must be surjective. If so, its kernel, K, is a subgroup of index 2, hence normal, and so, it must be maximal normal, a contradiction.

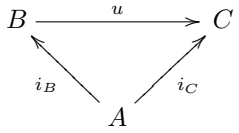
Therefore, the functor $G \rightsquigarrow G/[G,G] = G^{ab}$, from $\mathcal{G}\mathrm{r}$ to $\mathcal{A}\mathrm{b}$, has no left adjoint.

One often encounters situations (for example in topology, differential geometry and algebraic geometry) where the objects of interest are arrows "over" a given object (or the dual notion of arrows "co-over" a given object), for example, vector bundles, fibre bundles, algebras over a ring, etc. Such situations are captured by the abstract notion of "comma categories."

Definition 1.18 Let $\mathcal{C}$ be a category and fix some object, A, in $\mathcal{O}\mathrm{b}(\mathcal{C})$. We let $\mathcal{C}_A$, the *category over* A (or *comma category*), be the category whose objects are pairs (B, π_B), where B is some object in $\mathcal{O}\mathrm{b}(\mathcal{C})$ and π_B is a morphism in $\mathrm{Hom}_{\mathcal{C}}(B, A)$, and whose morphisms from (B, π_B) to (C, π_C) are the morphisms $u \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ making the following diagram commute:



Dually, we let $\mathcal{C}^A$, the *category co- over* A (also called *comma category*), be the category whose objects are pairs (B, i_B), where B is some object in $\mathcal{O}\mathrm{b}(\mathcal{C})$ and i_B is a morphism in $\mathrm{Hom}_{\mathcal{C}}(A, B)$, and whose morphisms from (B, i_B) to (C, i_C) are the morphisms $u \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ making the following diagram commute:



The notion of representable functor allows us to define products and coproducts in arbitrary categories.

Let $\mathcal{C}$ be any category. Say $\{A_\alpha\}_{\alpha \in \Lambda}$ is a set of objects in $\mathcal{O}\mathrm{b}(\mathcal{C})$.

(1) We get a cofunctor, F, from $\mathcal{C}^D$ to $\mathcal{S}\mathrm{ets}$ *via*

$$B \rightsquigarrow \prod_\alpha \mathrm{Hom}_{\mathcal{C}}(B, A_\alpha) = F(B),$$

where the above product is just the cartesian product of sets, and

(2) We get a functor, G, from $\mathcal{C}$ to $\mathcal{S}$ets *via*

$$B \rightsquigarrow \prod_{\alpha} \mathrm{Hom}_{\mathcal{C}}(A_\alpha, B) = G(B).$$

Are these (or either) representable?

First, consider (1). We need an object, $P \in \mathcal{O}\mathrm{b}(\mathcal{C})$ and some $\xi \in F(P)$, *i.e.* $\xi \in \prod_\alpha \mathrm{Hom}_{\mathcal{C}}(P, A_\alpha)$, which means that $\xi = \{pr_\alpha\}_\alpha$, where the pr_α are morphisms $pr_\alpha \colon P \to A_\alpha$.

Definition 1.19 When $(P, \{pr_\alpha\})$ exists, *i.e.* for every $B \in \mathcal{O}\mathrm{b}(\mathcal{C})$, there is a functorial isomorphism

$$\mathrm{Hom}_{\mathcal{C}}(B, P) \xrightarrow{\sim} \prod_{\alpha} \mathrm{Hom}_{\mathcal{C}}(B, A_\alpha),$$

via $u \mapsto (pr_\alpha \circ u)_\alpha$, the pair $(P, \{pr_\alpha\})$ is *the product* of the A_α's in $\mathcal{C}$. This product is denoted $\prod_\alpha A_\alpha$ (one usually drops the pr_α's). We have the (functorial) isomorphism

$$\mathrm{Hom}_{\mathcal{C}}(B, \prod_{\alpha} A_\alpha) \xrightarrow{\sim} \prod_{\alpha} \mathrm{Hom}_{\mathcal{C}}(B, A_\alpha). \qquad (*)$$

Remark: Definition 1.19 implies that for every family of morphisms,
$\{f_\alpha \colon B \to A_\alpha\} \in \prod_\alpha \mathrm{Hom}_{\mathcal{C}}(B, A_\alpha)$, there is a *unique* morphism, $u \colon B \to \prod_\alpha A_\alpha$, so that

$$f_\alpha = pr_\alpha \circ u, \quad \text{for all } \alpha.$$

This is called the *universal mapping property* of products. In general, universal mapping properties are another name for representing a functor. The latter is a more general and supple notion and we will mainly stick to it.

Now, consider (2). We need an object, $Q \in \mathcal{O}\mathrm{b}(\mathcal{C})$, and some $\xi \in G(Q)$, *i.e.* $\xi \in \prod_\alpha \mathrm{Hom}_{\mathcal{C}}(A_\alpha, Q)$, which means that $\xi = \{i_\alpha\}_\alpha$, where the i_α are morphisms $i_\alpha \colon A_\alpha \to Q$.

Definition 1.20 When $(Q, \{i_\alpha\})$ exists, *i.e.* for every $B \in \mathcal{O}\mathrm{b}(\mathcal{C})$, there is a functorial isomorphism

$$\mathrm{Hom}_{\mathcal{C}}(Q, B) \xrightarrow{\sim} \prod_{\alpha} \mathrm{Hom}_{\mathcal{C}}(A_\alpha, B),$$

via $u \mapsto (u \circ i_\alpha)_\alpha$, the pair $(Q, \{i_\alpha\})$ is *the coproduct* of the A_α's in $\mathcal{C}$. This coproduct is denoted $\coprod_\alpha A_\alpha$ (one usually drops the i_α's). We have the (functorial) isomorphism

$$\mathrm{Hom}_{\mathcal{C}}(\coprod_{\alpha} A_\alpha, B) \xrightarrow{\sim} \prod_{\alpha} \mathrm{Hom}_{\mathcal{C}}(A_\alpha, B). \qquad (**)$$

Of course, as above, there is a universal mapping property here, also.

Definition 1.21 The product in $\mathcal{C}_A$ is called the *fibred product over* A in $\mathcal{C}$. The coproduct in $\mathcal{C}^A$ is called the *fibred coproduct over* A in $\mathcal{C}$.

Remark: Given any family, $\{(A_\alpha, \pi_\alpha)\}_\alpha$, of objects in $\mathcal{C}_A$ (with $\pi_\alpha \colon A_\alpha \to A$), the fibred product of the A_α's over A in $\mathcal{C}$ is a pair, $(\prod_A A_\alpha, \xi)$, where $\prod_A A_\alpha$ is some object in $\mathcal{C}$ (together with a morphism, $\pi \colon \prod_A A_\alpha \to A$), and ξ consists of a family of morphisms, $pr_\alpha \colon \prod_A A_\alpha \to A_\alpha$, with

$$\pi_\alpha \circ pr_\alpha = \pi_\beta \circ pr_\beta \ (= \pi), \quad \text{for all } \alpha, \beta;$$

moreover, for any object, $B \in \mathcal{C}$, and any family of morphisms, $\{f_\alpha \colon B \to A_\alpha\}_\alpha$, with

$$\pi_\alpha \circ f_\alpha = \pi_\beta \circ f_\beta, \quad \text{for all } \alpha, \beta,$$

there is a *unique* morphism, $u \colon B \to \prod_A A_\alpha$, so that $f_\alpha = pr_\alpha \circ u$, for all α.

We leave it to the reader to unwind the definition of fibred coproducts over A in $\mathcal{C}$.

Examples of Products, Coproducts, Fibred Products and Fibred Coproducts:

(1) $\mathcal{C} = \mathcal{S}\text{ets}$. Given a family of sets, $\{A_\alpha\}_{\alpha\in\Lambda}$, does $\prod_\alpha A_\alpha$ or $\coprod_\alpha A_\alpha$ exist? If so, what are they?

For $\prod_\alpha A_\alpha$, we seek a set, P, and an element, ξ, in $F(P)$, where F is the cofunctor

$$T \rightsquigarrow F(T) = \prod_\alpha \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(T, A_\alpha).$$

This means that $\xi \in F(P)$ is just a tuple of maps, $pr_\alpha \colon P \to A_\alpha$. Take P to be the ordinary cartesian product of the A_α's and $pr_\alpha \colon P \to A_\alpha$, the αth projection. Check that this works (DX).

For $\coprod_\alpha A_\alpha$, we seek a set, Q, and an element, ξ, in $G(Q)$, where G is our functor

$$T \rightsquigarrow G(T) = \prod_\alpha \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(A_\alpha, T).$$

So, we need a family of maps $i_\alpha \colon A_\alpha \to Q$. Now, if Q is to work, then for every T, we need an isomorphism

$$\theta_T \colon \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(Q, T) \xrightarrow{\sim} \prod_\alpha \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(A_\alpha, T)$$

given by $\theta_T(\varphi) = (\varphi \circ i_\alpha)_\alpha$. Take $Q = \bigcup_\alpha A_\alpha$ (the disjoint union of the A_α's). The rest of the construction is easy (DX).

(2) $\mathcal{C} = \mathcal{A}\text{b}$, more generally, $\mathcal{C} = \mathcal{M}\text{od}(R)$ (R a ring) or $\mathcal{C} = \mathcal{M}\text{od}(G)$ (G a group).

We begin with products. Given a family, $\{A_\alpha\}_{\alpha\in\Lambda}$, with each A_α in $\mathcal{M}\text{od}(R)$, we seek $P \in \mathcal{M}\text{od}(R)$ and maps $pr_\alpha \colon P \to A_\alpha$ in $\mathcal{M}\text{od}(R)$, so that for every $T \in \mathcal{M}\text{od}(R)$, there is an isomorphism

$$\theta_T \colon \mathrm{Hom}_R(T, P) \xrightarrow{\sim} \prod_\alpha \mathrm{Hom}_R(T, A_\alpha),$$

where $\theta_T(\varphi) = \{pr_\alpha \circ \varphi\}_\alpha$ (the notation $\mathrm{Hom}_R(A, B)$ is usually used, instead of the more accurate but more cumbersome notation $\mathrm{Hom}_{\mathcal{M}\mathrm{od}(R)}(A, B)$). We see that P must be $\prod_\alpha A_\alpha$, the product in the category of sets, if this can be made an R-module. Now, $\prod_\alpha A_\alpha$ is an R-module *via* coordinatewise addition, with the R-action given by $r(\xi_\alpha) = (r\xi_\alpha)$. So, $\prod_\alpha A_\alpha$ is the product of the A_α's in $\mathcal{M}\text{od}(R)$.

Next, we consider coproducts. We seek $Q \in \mathcal{M}\text{od}(R)$ and maps $i_\alpha \colon A_\alpha \to Q$ in $\mathcal{M}\text{od}(R)$, so that for every $T \in \mathcal{M}\text{od}(R)$, there is an isomorphism

$$\theta_T \colon \mathrm{Hom}_R(Q, T) \xrightarrow{\sim} \prod_\alpha \mathrm{Hom}_R(A_\alpha, T),$$

where $\theta_T(\varphi) = \{\varphi \circ i_\alpha\}_\alpha$. The disjoint union $\bigcup_\alpha A_\alpha$ may be a first approximation to Q, but it is not good enough. Instead, we let

$$Q = \Big\{\xi \in \prod_\alpha A_\alpha \mid pr_\alpha(\xi) = 0 \quad \text{for all but finitely many } \alpha\Big\}.$$

This is an R-submodule of $\prod_\alpha A_\alpha$. The isomorphism

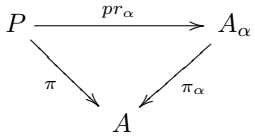
$$\theta_T\colon \mathrm{Hom}_R(Q,T) \xrightarrow{\sim} \prod_\alpha \mathrm{Hom}_R(A_\alpha, T)$$

can now be established. First, let $i_\alpha(u) = (\delta^u_\beta)_\beta$, where $\delta^u_\alpha = u$ and $\delta^u_\beta = 0$ for all $\beta \neq \alpha$. Given a family, $(\varphi_\alpha)_\alpha$, of maps $\varphi_\alpha\colon A_\alpha \to T$, for any $\xi = (\xi_\alpha)_\alpha \in Q$, set $\varphi(\xi) = \sum_\alpha \varphi_\alpha(\xi_\alpha) \in T$. If $\varphi \in \mathrm{Hom}_R(Q,T)$ is given, define $\varphi_\alpha = \varphi \circ i_\alpha$. This shows that if we set $\coprod_\alpha A_\alpha$ to be our R-module Q and the i_α to be our maps, $i_\alpha\colon A_\alpha \to Q$, as above, we have proved the proposition:

Proposition 1.42 *The categories: $\mathcal{S}$ets, $\mathcal{A}$b, $\mathcal{M}$od(R), $\mathcal{M}$od(G) all possess arbitrary products and coproducts.*

How about fibred products and coproducts?

(3) Let us go back to $\mathcal{C} = \mathcal{S}$ets, and first consider fibred products over A. A first approximation to the product, P, in $\mathcal{S}\mathrm{ets}_A$, is $\prod_\alpha A_\alpha$. However, this is not good enough because there is no "structure map", $\pi\colon P \to A$, so that



commutes for all α. We let

$$P_A = \Big\{\xi \in \prod_\alpha A_\alpha \mid \pi_\alpha(\xi_\alpha) = \pi_\beta(\xi_\beta), \quad \text{for all } \alpha, \beta\Big\}.$$

This is a set (possibly empty), and it lies over A; indeed, we can define $\pi\colon P_A \to A$ by $\pi(\xi) = \pi_\alpha(\xi_\alpha)$, for any chosen α, since this is well-defined by definition of P_A. We write $\prod_A A_\alpha$ for P_A and, for every α, we define the map, $pr_\alpha\colon \prod_A A_\beta \to A_\alpha$, as the restriction of $pr_\alpha\colon \prod A_\beta \to A_\alpha$ to $\prod_A A_\alpha$. The reader should check that this yields products in $\mathcal{S}\mathrm{ets}_A$.

Coproducts are a bit harder. It is natural to try $\bigcup_\alpha A_\alpha$ as a first approximation, but this is not good enough: this does not tell us what $i\colon A \to Q$ is. The difficulty is that $\bigcup_\alpha A_\alpha$ is too big, and we need to identify some of its elements. To do so, we define an equivalence relation on $\bigcup_\alpha A_\alpha$, in two steps. First, we define *immediate equivalence*. Given $\xi \in A_\alpha$ and $\eta \in A_\beta$, we say that ξ and η are *immediately equivalent*, denoted $\xi \approx \eta$, iff there is some $a \in A$, so that $\xi = i_\alpha(a)$ and $\eta = i_\beta(a)$. The relation $\approx$ is clearly reflexive and symmetric but it is not necessarily transitive. So, we define $\sim$ to be the equivalence relation generated by $\approx$. This means that $\xi \sim \eta$ iff there exist $x_0, \ldots, x_t \in \bigcup_\alpha A_\alpha$, so that

$$\xi = x_0,\ x_0 \approx x_1,\ x_1 \approx x_2,\ \ldots, x_{t-1} \approx x_t,\ x_t = \eta.$$

(For example, if $\xi \approx x$ and $x \approx \eta$, then $\xi = i_\alpha(a)$, $x = i_\beta(a)$, $x = i_\beta(b)$ and $\eta = i_\gamma(b)$. Note that $i_\beta(a) = i_\beta(b)$.) We let $\coprod_A A_\alpha = (\bigcup_\alpha A_\alpha)\,/\sim$, and $i\colon A \to \coprod_A A_\alpha$ is given by $i(a) =$ class of $i_\alpha(a)$, for any fixed α (this is well-defined, by definition of $\sim$). The verification that $\coprod_A A_\alpha$ works is left as an exercise (DX). *Therefore, the category of sets has arbitrary fibred coproducts as well.*

(4) $\mathcal{C} = \mathcal{A}$b, $\mathcal{M}$od(R), $\mathcal{M}$od(G).

For fibred products, we use $\prod_A A_\alpha$, as constructed for $\mathcal{S}$ets, but made into an R-module (resp. G-module), in the usual way.

For fibred coproducts, begin with $\coprod_\alpha A_\alpha$ (in $\mathcal{C}$), and define N to be the submodule generated by the elements $i_\alpha(a) - i_\beta(a)$ with $a \in A$ and α, β arbitrary. Take

$$\coprod_A A_\alpha = \left(\coprod_\alpha A_\alpha\right)/N.$$

Again, the reader should check that $\coprod_A A_\alpha$ works (DX). *Therefore,* $\mathcal{A}$b, $\mathcal{M}$od(R), $\mathcal{M}$od(G), *all have arbitrary fibred products and coproducts*.

We now consider products and coproducts in the category of groups, $\mathcal{G}$r. There is no difficulty for products: Use $\prod_\alpha A_\alpha$, the usual cartesian product of the A_α's, as sets, and make $\prod_\alpha A_\alpha$ into a group under coordinatewise multiplication. The same idea works for fibred products. However, coproducts require a new idea.

Given the family of groups, $\{A_\alpha\}_{\alpha\in\Lambda}$, write $A_\alpha^0 = A_\alpha - \{1\}$. Let

$$S = \bigcup_\alpha^{\cdot} A_\alpha^0,$$

and consider, S^n, the n-fold cartesian product of S. We can view S^n as the set of *words of length* n over the alphabet S; each word is an n-tuple, $(\sigma_{\alpha_1}, \ldots, \sigma_{\alpha_n})$, with $\sigma_\beta \in A_\beta$. We call such a word *admissible* iff $A_{\alpha_j} \neq A_{\alpha_{j+1}}$, for $j = 1, 2, \ldots, n-1$. Let S^{n*} denote the set of admissible words of length n, and let

$$Q = \left(\bigcup_{n\geq 1} S^{n*}\right) \cup \{\emptyset\}.$$

(The special word, $\emptyset$, is the "empty word".) Multiplication in Q is defined as follows:
Given $(\sigma) = (\sigma_{\alpha_1}, \ldots, \sigma_{\alpha_r})$ and $(\tau) = (\tau_{\beta_1}, \ldots, \tau_{\beta_s})$ in Q, set

$$(\sigma)(\tau) = (\sigma_{\alpha_1}, \ldots, \sigma_{\alpha_r}, \tau_{\beta_1}, \ldots, \tau_{\beta_s}),$$

the result of concatenating the r-tuple, (σ), with the s-tuple, (τ). In case one of (σ) or (τ) is $\emptyset$, the concatenation is just the non-empty word and $\emptyset\emptyset$ is $\emptyset$. The word $(\sigma)(\tau)$ is admissible of length $r+s$, except if $\alpha_r = \beta_1$, in which case we need to perform a reduction process to obtain an admissible word:

(1) Form $\sigma_{\alpha_r}\tau_{\beta_1}$ in $A_{\alpha_r} = A_{\beta_1}$. There are two cases:

(a) $\sigma_{\alpha_r}\tau_{\beta_1} \neq 1_{\alpha_r}\ (= 1_{\beta_1})$; then

$$(\sigma_{\alpha_1}, \ldots, \sigma_{\alpha_{r-1}}, \sigma_r\tau_{\beta_1}, \tau_{\beta_2}, \ldots, \tau_{\beta_s})$$

is an admissible word of length $r+s-1$, and the reduction process ends with this word as output.

(b) $\sigma_{\alpha_r}\tau_{\beta_1} = 1_{\alpha_r}\ (= 1_{\beta_1})$; then, omit σ_{α_r} and τ_{β_1}, form

$$(\sigma_{\alpha_1}, \ldots, \sigma_{\alpha_{r-1}}, \tau_{\beta_2}, \ldots, \tau_{\beta_s}),$$

a word of length $r+s-2$, and if necessary, go back to (1) above.

Since both step (a) and (b) decrease the length of the current word, the reduction process must end with some admissible word of length $l \leq r+s$, or the empty word.

The set Q with the above multiplication is indeed a group with identity element, $\emptyset$ (DX). (The map $i_\alpha\colon A_\alpha \to Q$ sends $\sigma \in A_\alpha$ to the length-one word (σ) if $\sigma \neq 1$ or to $\emptyset$ if $\sigma = 1$.) In summary, we get

Theorem 1.43 *The category of groups, $\mathcal{G}\mathrm{r}$, possesses arbitrary coproducts (old fashioned name: "free product of the A_α.")*

Definition 1.22 Given any set, S, define the *the free group on* S to be the group $\mathrm{Fr}(S) = \coprod_S \mathbb{Z}$.

We have just shown that coproducts exist in the category $\mathcal{G}\mathrm{r}$. What about coproducts in the category $\mathcal{G}\mathrm{r}^A$, where A is any group?

Given a family $\{(G_\alpha, i_\alpha)\}_{\alpha\in\Lambda}$ in $\mathcal{G}\mathrm{r}^A$, form $G = \coprod_\alpha G_\alpha$, in the category $\mathcal{G}\mathrm{r}$. In G, consider the collection of elements

$$\{i_\alpha(a)i_\beta^{-1}(a) \mid a \in A,\ i_\alpha\colon A \to G_\alpha,\ \alpha \text{ and } \beta \in \Lambda\};$$

let N be the *normal* subgroup of G generated by the above elements. Then, $G/N \in \mathcal{O}\mathrm{b}(\mathcal{G}\mathrm{r}^A)$, because the map $i\colon A \to G/N$ given by $i(a) =$ image of $i_\alpha(a)$ in G/N (for any fixed α) is well-defined (since image of $i_\alpha(a) =$ image of $i_\beta(a)$ in G/N). Check that, (DX), $(G/N, i)$ is the fibred coproduct of the G_α's. (Old terminology: *amalgamated product of the* G_α over A.)

Examples of fibred coproducts: (1) Let U and V be two sets. Form the intersection $U \cap V$; we have inclusion maps $i_U\colon U \cap V \to U$ and $i_V\colon U \cap V \to V$. We know that $U \amalg V = U \uplus V$, the disjoint union of U and V, and then, the set-theoretic union of U and V is given by

$$U \cup V = U \coprod_{U\cap V} V.$$

(2) Consider the category $(\mathrm{TOP}, *)$ of ("nice", i.e., connected, locally connected) topological spaces with a base point. Given two spaces $(U, *)$ and $(V, *)$ in $(\mathrm{TOP}, *)$, consider $(U \cap V, *)$. Then, again,

$$(U \cup V, *) = (U, *) \coprod_{(U\cap V,*)} (V, *), \quad \text{in } (\mathrm{TOP}, *).$$

Van Kampen's theorem says that

$$\pi_1(U \cup V, *) = \pi_1(U, *) \coprod_{\pi_1(U\cap V,*)} \pi_1(V, *),$$

which may also be written as

$$\pi_1\left((U, *) \coprod_{(U\cap V,*)} (V, *)\right) = \pi_1(U, *) \coprod_{\pi_1(U\cap V,*)} \pi_1(V, *).$$

In other words, van Kampen's theorem says that π_1 commutes with fibred coproducts.

Go back to the free group, $\mathrm{Fr}(S)$. We have

$$\begin{aligned} \mathrm{Hom}_{\mathcal{G}\mathrm{r}}(\mathrm{Fr}(S), G) &= \mathrm{Hom}_{\mathcal{G}\mathrm{r}}(\coprod_S \mathbb{Z}, G) \\ &\cong \prod_S \mathrm{Hom}_{\mathcal{G}\mathrm{r}}(\mathbb{Z}, G) \\ &\cong \prod_S |G| = \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |G|). \end{aligned}$$

Corollary 1.44 *The functor, $S \rightsquigarrow \mathrm{Fr}(S)$, from $\mathcal{S}\mathrm{ets}$ to $\mathcal{G}\mathrm{r}$ is the left adjoint to the stripping functor, $G \rightsquigarrow |G|$, from $\mathcal{G}\mathrm{r}$ to $\mathcal{S}\mathrm{ets}$.*

Corollary 1.45 *If $S \longrightarrow T$ is surjective, then $\mathrm{Fr}(S) \longrightarrow \mathrm{Fr}(T)$ is a surjection of groups. Also, $\mathrm{Fr}(S) \cong \mathrm{Fr}(T)$ iff $\#(S) = \#(T)$ (i.e., S and T have the same cardinality).*

Proof. If $u\colon S \to T$ is a surjection in $\mathcal{S}\mathrm{ets}$, then there is a map $v\colon T \to S$ so that $u \circ v = 1_T$. Since Fr is a functor, we get homomorphisms $\mathrm{Fr}(u)\colon \mathrm{Fr}(S) \to \mathrm{Fr}(T)$ and $\mathrm{Fr}(v)\colon \mathrm{Fr}(T) \to \mathrm{Fr}(S)$; also, $\mathrm{Fr}(u) \circ \mathrm{Fr}(v) = 1_{\mathrm{Fr}(T)}$, which shows that $\mathrm{Fr}(u)$ is surjective.

If $\#(S) = \#(T)$, it is obvious that $\mathrm{Fr}(S) \cong \mathrm{Fr}(T)$. Conversely, assume that $\mathrm{Fr}(S) \cong \mathrm{Fr}(T)$. We know that

$$\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(\mathrm{Fr}(S), G) \cong \mathrm{Hom}_{\mathcal{G}\mathrm{r}}(\mathrm{Fr}(T), G)$$

for all G. Take $G = \mathbb{Z}/2\mathbb{Z}$. Then, the left hand side is isomorphic to $\mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |\mathbb{Z}/2\mathbb{Z}|) = \mathcal{P}(S)$ (where $\mathcal{P}(S) =$ power set of S) and the righthand side is isomorphic to $\mathcal{P}(T)$. Therefore, $\#(\mathcal{P}(S)) = \#(\mathcal{P}(T))$; and so, $\#(S) = \#(T)$. $\square$

Given a group, G, consider its underlying set, $|G|$, and then the group $\mathrm{Fr}(|G|)$. Since

$$\mathrm{Hom}_{\mathcal{G}\mathrm{r}}(\mathrm{Fr}(|G|), G) \cong \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(|G|, |G|),$$

the image of the identity map, $\mathrm{id}_G \in \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(|G|, |G|)$, yields a canonical surjection, $\mathrm{Fr}(|G|) \longrightarrow G$. If S is a subset of $|G|$, then, the inclusion map, $S \hookrightarrow |G|$, yields a morphism of groups, $\mathrm{Fr}(S) \longrightarrow G$.

Definition 1.23 A set, $S \subseteq |G|$, *generates* a group, G, iff the canonical map $\mathrm{Fr}(S) \longrightarrow G$ is surjective.

This definition agrees with our old use of *generation of a group* in previous sections. Say S generates G. Then, we have the exact sequence

$$0 \longrightarrow K \longrightarrow \mathrm{Fr}(S) \longrightarrow G \longrightarrow 0,$$

where K is the kernel of the surjective morphism, $\mathrm{Fr}(S) \longrightarrow G$ (so, K is normal in $\mathrm{Fr}(S)$). There is also a set, T, so that

$$\mathrm{Fr}(T) \longrightarrow K \longrightarrow 0 \quad \text{is exact.}$$

By splicing the two exact sequences, we get an exact sequence

$$\mathrm{Fr}(T) \longrightarrow \mathrm{Fr}(S) \longrightarrow G \longrightarrow 0,$$

called a *presentation of* G. Sometimes, a presentation is defined as a sequence

$$\mathrm{Fr}(T) \longrightarrow \mathrm{Fr}(S) \longrightarrow G \longrightarrow 0,$$

where the smallest *normal* subgroup containing $\mathrm{Im}\,(\mathrm{Fr}(T))$ is equal to the kernel of $\mathrm{Fr}(S) \longrightarrow G$. (Note that such a sequence is not necessarily exact at the group $\mathrm{Fr}(S)$.)

The following fundamental theorem about free groups was proved independently by J. Nielson and O. Schreier:

Theorem 1.46 *(Nielson-Schreier (1929)) Every subgroup of a free group is a free group.*

The original proof is quite messy. The theory of group actions on trees yields a more direct and more transparent proof.

We conclude this section on categories with one more interesting example of adjoint functors from homotopy theory.

Example: Consider the category, h-TOP, whose objects are the same as those of TOP, but whose morphisms, $\mathrm{Hom}_{\text{h-TOP}}(X, Y)$, are the homotopy classes of maps $X \longrightarrow Y$. Given any space, X, in h-TOP, we

can form ΣX, the *suspension of* X: This is the space obtained by taking two new points, say 0 and 1, and forming the double cone obtained by joining 0 and 1 to every point of X, as illustrated in Figure 1.2.

We also have, ΩY, the *loop space on* Y, where ΩY consists of all continuous maps, $S^1 \longrightarrow Y$, from the unit circle to Y (say, mapping $(1, 0)$ to the base point of Y). Then, we have the isomorphism

$$\mathrm{Hom}_{\text{h-TOP}}(\Sigma X, Y) \cong \mathrm{Hom}_{\text{h-TOP}}(X, \Omega Y)$$

i.e., suspension is left-adjoint to loops. For instance, given any $\theta \in \mathrm{Hom}_{\text{h-TOP}}(\Sigma X, Y)$, for any $p \in X$, send p to the image by θ of the loop $l(p)$ $(= (*, 0, p, 1, *)$ in $\Sigma X)$, in Y.

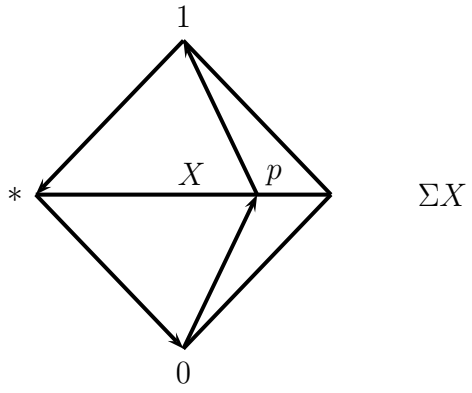


Figure 1.2: A suspension of X

1.8 Further Readings

El que anda mucho y lee mucho,
Vee mucho y sabe mucho.
—**Miguel Cervantes**

Some group theory is covered in every algebra text. Among them, we mention Michael Artin [2], Lang [34], Hungerford, [27], Jacobson [29], Mac Lane and Birkhoff [37], Dummit and Foote [11], Van Der Waerden [47] and Bourbaki [4]. More specialized books include Rotman [43], Hall [22], Zassenhaus [52], Rose [42] and Gorenstein [19]. For group cohomology, see also Cartan and Eilenberg [9], Rotman [44], Mac Lane [36] and Serre [45]. Mac Lane [35] is a good reference for category theory.

Chapter 2

Rings and Modules

2.1 Introduction

Linear algebra—meaning vector space theory over a field—is the part of algebra used most often in analysis, in geometry and in various applied fields. The natural generalization to the case when the base object is a ring rather than a field is the notion of "module." The theory of modules both delineates in sharp relief the elementary and deeper structure of vector spaces (and their linear transformations) and provides the essential "linear springboard" to areas such as number theory, algebraic geometry and functional analysis. It turns out to be surprisingly deep because the collection of "all" modules over a fixed ring has a profound influence on the structure of that ring. For a commutative ring, it even specifies the ring! Just as in analysis, where the first thing to consider in analyzing the local behavior of a given smooth function is its linear approximation, so in geometric applications the first idea is to pass to an appropriate linear approximation and this is generally a module.

2.2 Polynomial Rings, Commutative and Noncommutative

Consider the categories RNG and CR, and pick some ring, A, from each. We also have the category, RNG^A, called the *category of rings over* A (or *category of* A*-algebras*), and similarly, CR^A, and we have the stripping functors $\mathrm{RNG}^A \rightsquigarrow \mathcal{S}\mathrm{ets}$ and $\mathrm{CR}^A \rightsquigarrow \mathcal{S}\mathrm{ets}$.

Is there an adjoint functor to each? We seek a functor, $P\colon \mathcal{S}\mathrm{ets} \rightsquigarrow \mathcal{C}$, where $\mathcal{C} = \mathrm{RNG}^A$ or CR^A, so that

$$\mathrm{Hom}_{\mathcal{C}}(P(S), B) \cong \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |B|)$$

for every $B \in \mathcal{C}$.

Case 1: CR^A.

Theorem 2.1 *There exists a left-adjoint functor to the stripping functor,* $\mathrm{CR}^A \rightsquigarrow \mathcal{S}\mathrm{ets}$.

Proof. Given a set, S, let $\widetilde{\mathbb{N}}$ denote the set of non-negative integers and write $\widetilde{\mathbb{N}}_S$ for

$$\widetilde{\mathbb{N}}_S = \{\xi\colon S \to \widetilde{\mathbb{N}} \mid \xi(s) = 0, \quad \text{except for finitely many } s \in S\}.$$

Note that $\mathbb{N}_S$ consists of the functions $S \longrightarrow \widetilde{\mathbb{N}}$ with compact support (where S and $\widetilde{\mathbb{N}}$ are given the discrete topology).

Remark: We may think of the elements, ξ, of $\widetilde{\mathbb{N}}_S$ as finite *multisets* of elements of S, *i.e.*, finite sets with multiple occurrences of elements: For any $s \in S$, the number $\xi(s)$ is the number of occurrences of s in ξ. If we think of each

member, s, of S as an "indeterminate," for any $\xi \in \widetilde{\mathbb{N}}_S$, if $\xi(s_i) = n_i > 0$ for $i = 1, \ldots, t$, then ξ corresponds to the monomial $s_1^{n_1} \cdots s_t^{n_t}$.

We define a multiplication operation on $\widetilde{\mathbb{N}}_S$ as follows: For $\xi, \eta \in \widetilde{\mathbb{N}}_S$,

$$(\xi\eta)(s) = \xi(s) + \eta(s).$$

(This multiplication operation on $\widetilde{\mathbb{N}}_S$ is associative and has the identity element, ξ_0, with $\xi_0(s) = 0$ for all $s \in S$. Thus, $\widetilde{\mathbb{N}}_S$ is a *monoid*. Under the interpretation of elements of $\widetilde{\mathbb{N}}_S$ as multisets, multiplication corresponds to union and under the interpretation as monomials, it corresponds to the intuitive idea of multiplication of monomials. See below for precise ways of making these intuitions correct.)

Define $A[S]$ by

$$A[S] = \{f \colon \widetilde{\mathbb{N}}_S \to A \mid f(\xi) = 0, \quad \text{except for finitely many } \xi \in \widetilde{\mathbb{N}}_S\}.$$

Remark: We should think of each $f \in A[S]$ as a polynomial in the indeterminates, s ($s \in S$), with coefficients from A; each $f(\xi)$ is the coefficient of the monomial ξ. See below where X_s is defined.

In order to make $A[S]$ into a ring, we define addition and multiplication as follows:

$$\begin{aligned} (f+g)(\xi) &= f(\xi) + g(\xi) \\ (fg)(\xi) &= \sum_{\substack{\eta,\eta',\\ \eta\eta'=\xi}} f(\eta)g(\eta'). \end{aligned}$$

Multiplication in $A[S]$ is also called the *convolution product*. The function with constant value, $0 \in A$, is the zero element for addition and the function denoted 1, given by

$$1(\xi) = \begin{cases} 0 & \text{if } \xi \neq \xi_0 \\ 1 & \text{if } \xi = \xi_0, \end{cases}$$

is the identity element for multiplication. The reader should check that under our operations, $A[S]$ is a commutative ring with identity (DX). For example, we check that 1 is an identity for multiplication. We have

$$(f \cdot 1)(\xi) = \sum_{\eta\eta'=\xi} f(\eta)1(\eta') = \sum_{\eta\xi_0=\xi} f(\eta).$$

However, for all $s \in S$, we have $\eta\xi_0(s) = \eta(s) + \xi_0(s) = \eta(s)$, and so, $\eta = \xi$. Consequently, $(f \cdot 1)(\xi) = f(\xi)$, for all ξ.

We have an injection $A \longrightarrow A[S]$ *via* $\alpha \in A \mapsto \alpha \cdot 1$. Here, $\alpha \cdot 1$ is given by

$$\alpha \cdot 1(\xi) = \alpha(1(\xi)) = \begin{cases} 0 & \text{if } \xi \neq \xi_0 \\ \alpha & \text{if } \xi = \xi_0. \end{cases}$$

Therefore, $A[S] \in \mathrm{CR}^A$. It remains to check the "universal mapping property."

Say $\theta \in \mathrm{Hom}_{\mathrm{CR}^A}(A[S], B)$. Now, we can define two injections $S \hookrightarrow \widetilde{\mathbb{N}}_S$ and $S \hookrightarrow A[S]$ (a map of sets) as follows: Given any $s \in S$, define $\Delta_s \in \widetilde{\mathbb{N}}_S$ by

$$\Delta_s(t) = \begin{cases} 0 & \text{if } t \neq s \\ 1 & \text{if } t = s, \end{cases}$$

and define $X_s \in A[S]$ by

$$X_s(\xi) = \begin{cases} 0 & \text{if } \xi \neq \Delta_s \\ 1 & \text{if } \xi = \Delta_s. \end{cases}$$

Then, if we set $\theta^\flat(s) = \theta(X_s)$, we get a set map $\theta^\flat \in \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |B|)$.

Conversely, let $\varphi \in \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |B|)$. Define $\widetilde{\varphi}\colon \widetilde{\mathbb{N}}_S \to B$ *via*

$$\widetilde{\varphi}(\xi) = \prod_{s\in S} \varphi(s)^{\xi(s)} \in B.$$

Now, set $\varphi^\sharp(f)$, for $f \in A[S]$, to be

$$\varphi^\sharp(f) = \sum_{\xi} f(\xi)\widetilde{\varphi}(\xi).$$

(Of course, since $B \in \mathrm{CR}^A$, we view $f(\xi)$ as an element of B *via* the corresponding morphism $A \longrightarrow B$.)

The reader should check (DX) that:

(a) $\varphi^\sharp$ is a homomorphism and

(b) The operations $\sharp$ and $\flat$ are mutual inverses. □

The definition of $A[S]$ has the advantage of being perfectly rigorous, but it is quite abstract. We can give a more intuitive description of $A[S]$. For this, for any $\xi \in \widetilde{\mathbb{N}}_S$, set

$$X^{(\xi)} = \prod_{s\in S} X_s^{\xi(s)}, \quad \text{in } A[S],$$

and call it a *monomial*. The reader should check (DX) that

$$X^{(\xi)}(\eta) = \delta_{\xi\eta}, \quad \text{for all } \xi, \eta \in \widetilde{\mathbb{N}}_S.$$

Hence, the map $\xi \mapsto X^{(\xi)}$ is a bijection of $\widetilde{\mathbb{N}}_S$ to the monomials (c.f. the remark on monomials made earlier). Moreover, we claim that every $f \in A[S]$ can be written as

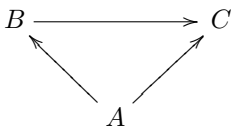
$$f = \sum_{\xi} f(\xi)X^{(\xi)}.$$

This is because

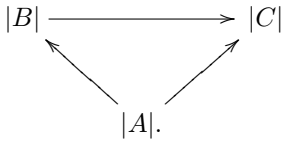
$$\left(\sum_{\xi} f(\xi)X^{(\xi)}\right)(\eta) = \sum_{\xi} f(\xi)\delta_{\xi\eta} = f(\eta).$$

The usual notation for $\xi(s)$ is ξ_s, and then, $X^{(\xi)} = \prod_{s\in S} X_s^{\xi_s}$, and our f's in $A[S]$ are just polynomials in the usual sense, as hinted at already. However, since S may be infinite, our formalism allows us to deal with polynomials in infinitely many indeterminates. Note that any polynomial involves just a finite number of the variables.

What happened to $|A|$ in all this? After all, in CR^A, we have rings, B, and maps $i_A\colon A \to B$. So, the commutative diagram



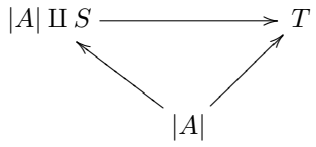
would give



Consider the category of $|A|$-sets, $\mathcal{S}\text{ets}^{|A|}$. Given any set, S, make an $|A|$-set:

$$|A| \amalg S = |A| \cup S.$$

This is an $|A|$-set, since we have the canonical injection, $|A| \longrightarrow |A| \amalg S$. Let T be any $|A|$-set and look at $\text{Hom}_{\mathcal{S}\text{ets}^{|A|}}(|A| \amalg S, T)$, i.e., maps $|A| \amalg S \longrightarrow T$ such that the diagram



commutes. We know that

$$\text{Hom}_{\mathcal{S}\text{ets}^{|A|}}(|A| \amalg S, T) \subseteq \text{Hom}_{\mathcal{S}\text{ets}}(|A|, T) \prod \text{Hom}_{\mathcal{S}\text{ets}}(S, T)$$

and the image is $\text{Hom}_{\mathcal{S}\text{ets}^{|A|}}(|A|, T) \prod \text{Hom}_{\mathcal{S}\text{ets}}(S, T)$. But $\text{Hom}_{\mathcal{S}\text{ets}^{|A|}}(|A|, T)$ consists of a single element, and so,

$$\text{Hom}_{\mathcal{S}\text{ets}^{|A|}}(|A| \amalg S, T) \cong \text{Hom}_{\mathcal{S}\text{ets}}(S, T).$$

Thus, we have the functorial isomorphism

$$\text{Hom}_{\text{CR}^A}(A[S], B) \cong \text{Hom}_{\mathcal{S}\text{ets}^{|A|}}(|A| \amalg S, |B|).$$

Corollary 2.2 *A necessary and sufficient condition that* $\mathbb{Z}[S] \cong \mathbb{Z}[T]$ *(in* CR*) is that* $\#(S) = \#(T)$.

Proof. If $\#(S) = \#(T)$, then there exist mutually inverse bijections, $\varphi\colon S \to T$ and $\psi\colon T \to S$. Hence, by functoriality, $\mathbb{Z}[S]$ is isomorphic to $\mathbb{Z}[T]$ (*via* $\mathbb{Z}[S](\varphi)$ and $\mathbb{Z}[T](\psi)$). Now, take $B = \mathbb{Z}/2\mathbb{Z}$, and assume that $\mathbb{Z}[S] \cong \mathbb{Z}[T]$. Then, we know that

$$\text{Hom}_{\text{CR}}(\mathbb{Z}[S], B) \cong \text{Hom}_{\text{CR}}(\mathbb{Z}[T], B),$$

and since $\text{Hom}_{\text{CR}}(\mathbb{Z}[S], B) \cong \text{Hom}_{\mathcal{S}\text{ets}}(S, \{0,1\})$ and $\text{Hom}_{\text{CR}}(\mathbb{Z}[T], B) \cong \text{Hom}_{\mathcal{S}\text{ets}}(T, \{0,1\})$, we have

$$\text{Hom}_{\mathcal{S}\text{ets}}(S, \{0,1\}) \cong \text{Hom}_{\mathcal{S}\text{ets}}(T, \{0,1\}).$$

This implies that $2^{\#(S)} = 2^{\#(T)}$, and thus, $\#(S) = \#(T)$. $\square$

Case 2: RNG^R, where R is a given ring (not necessarily commutative). For every set, S, and every R-algebra, $B \in \text{RNG}^R$, let

$$\text{Hom}^{(c)}_{\mathcal{S}\text{ets}}(S, |B|) = \{\varphi \in \text{Hom}_{\mathcal{S}\text{ets}}(S, |B|) \mid (\forall s \in S)(\forall \xi \in \text{Im}\,(|R|))(\varphi(s)\xi = \xi\varphi(s))\}.$$

Theorem 2.3 *There exists a functor,* $R\langle S\rangle$*, from* $\mathcal{S}\text{ets}$ *to* RNG^R*, so that*

$$\text{Hom}_{\text{RNG}^R}(R\langle S\rangle, B) \cong \text{Hom}^{(c)}_{\mathcal{S}\text{ets}}(S, |B|), \quad \textit{functorially.}$$

Sketch of proof. (A better proof *via* tensor algebras will be given later.) Given S, pick a "symbol", X_s, for each $s \in S$, and map $\mathbb{N}$ to the "positive powers of X_s," *via* $n \mapsto X_s^n$, and define $X_s^m \cdot X_s^n = X_s^{m+n}$. Let $\mathbb{N}_s = \{X_s^n \mid n \geq 1\} \cong \mathbb{N}$ (as monoid), and let

$$\mathcal{S} = \coprod_{s \in S} \mathbb{N}_s.$$

Consider $\mathcal{S}^{(p)}$, the cartesian product of p copies of S, with $p \geq 1$. An element of $\mathcal{S}^{(p)}$ is a tuple of the form $(X_{r_1}^{a_1}, \ldots, X_{r_p}^{a_p})$, and is called a *monomial*. Call a monomial *admissible* iff $r_i \neq r_{i+1}$, for $i = 1, \ldots, p-1$. Multiplication of admissible monomials is concatenation, with possible one-step reduction, if necessary. Call $\mathcal{S}^*$ the union of all the admissible monomials from the various $\mathcal{S}^{(p)}$, with $p \geq 1$, together with the "empty monomial", $\emptyset$. Set

$$R\langle S\rangle = \{f\colon \mathcal{S}^* \to R \mid f(\xi) = 0, \quad \text{except for finitely many } \xi \in \mathcal{S}^*\}.$$

There is a map $R \longrightarrow R\langle S\rangle$ $(\alpha \mapsto \alpha\emptyset)$. We make $R\langle S\rangle$ into a ring by defining addition and multiplication as in the commutative case:

$$\begin{aligned}(f+g)(\xi) &= f(\xi) + g(\xi)\\ (fg)(\xi) &= \sum_{\substack{\eta,\eta',\\ \eta\eta'=\xi}} f(\eta)g(\eta'),\end{aligned}$$

where ξ, η and η' are admissible monomials. Then, $R\langle S\rangle$ is an R-algebra, and it satisfies Theorem 2.3 (DX). □

Theorem 2.4 *Say T is a subset of S. Then, there exists a canonical injection $i\colon A[T] \to A[S]$, and $A[S]$ becomes an $A[T]$-algebra. In the category of $A[T]$-algebras, we have the isomorphism*

$$A[S] \cong A[T][S-T]$$

(Here $S - T$ denotes the complement of T in S, and A is in CR*.)*

Proof. We have an inclusion, $T \hookrightarrow S$, and for every $B \in \mathrm{CR}^A$, restriction to T gives a surjection

$$\mathrm{res}\colon \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |B|) \longrightarrow \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(T, |B|).$$

Because we are in the category of sets, there is a map, θ, so that $\mathrm{res} \circ \theta = \mathrm{id}$. Now, the maps θ and res induce maps Θ and Res so that $\mathrm{Res} \circ \Theta = \mathrm{id}$, as shown below:

$$\begin{array}{ccc}\mathrm{Hom}_{\mathrm{CR}^A}(A[S], B) & \xrightarrow{\cong} & \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |B|)\\ {\scriptstyle \mathrm{Res}}\downarrow\uparrow{\scriptstyle \Theta} & & {\scriptstyle \mathrm{res}}\downarrow\uparrow{\scriptstyle \theta}\\ \mathrm{Hom}_{\mathrm{CR}^A}(A[T], B) & \xrightarrow{\cong} & \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(T, |B|).\end{array}$$

If we let $B = A[S]$, we get a map $i = \mathrm{Res}(\mathrm{id}_{A[S]})\colon A[T] \longrightarrow A[S]$. If we let $B = A[T]$, then, since Res is onto, there is a map $\pi\colon A[S] \to A[T]$ so that $\mathrm{Res}(\pi) = \mathrm{id}_{A[T]}$. It follows that i is an injection, and thus, $A[S]$ is an $A[T]$-algebra.

We have

$$\mathrm{Hom}_{\mathrm{CR}^{A[T]}}(A[T][S-T], B) \cong \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S-T, |B|).$$

The given map, $|A[T]| \longrightarrow |B|$, yields a fixed map, $T \longrightarrow |B|$. For any given map, $S - T \longrightarrow |B|$, therefore, we get a canonical map, $T \amalg (S-T) \longrightarrow |B|$, *i.e.*, $S \longrightarrow |B|$, depending *only* on the map $S - T \longrightarrow |B|$. Therefore, there is an injection

$$\mathrm{Hom}_{\mathrm{CR}^{A[T]}}(A[T][S-T], B) \hookrightarrow \mathrm{Hom}_{\mathrm{CR}^A}(A[S], B),$$

and the image is just $\mathrm{Hom}_{\mathrm{CR}^{A[T]}}(A[S], B)$. By Yoneda's lemma, $A[S] \cong A[T][S-T]$, as an $A[T]$-algebra. □

From now on, we will write $\mathrm{Hom}_A(B, C)$ instead of $\mathrm{Hom}_{\mathrm{CR}^A}(B, C)$ and similarly for RNG^R. If $X^{(\xi)}$ is a monomial, then we set

$$\deg(X^{(\xi)}) = \sum_{s \in S} \xi(s) \in \mathbb{Z}_{\geq 0}.$$

If $f \in A[S]$, say $f = \sum_{(\xi)} a_{(\xi)} X^{(\xi)}$, then

$$\deg(f) = \sup\{\deg(X^{(\xi)}) \mid a_{(\xi)} \neq 0\}.$$

In particular, note that $\deg(0) = -\infty$.

Proposition 2.5 *The canonical map, $A \longrightarrow A[S]$, establishes an isomorphism of A with the polynomials of degree ≤ 0 in $A[S]$. Any $\alpha \neq 0$ in A goes to a polynomial of degree 0, only $0 \in A$ goes to a polynomial of degree < 0. If $f, g \in A[S]$, then*

(a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.

(b) $\deg(fg) \leq \deg(f) + \deg(g)$.
If A is without zero divisors then we have equality in (b) and

(c) The units of $A[S]$ are exactly the units of A.

(d) The ring $A[S]$ has no zero divisors.

Proof. Since we deal with degrees and each of the two polynomials f, g involves finitely many monomials, we may assume that S is a finite set. The map $A \longrightarrow A[S]$ is given by $\alpha \mapsto \alpha \cdot 1$ and 1 has degree 0, so it is trivial that we have an isomorphism of A with the polynomials of degree ≤ 0.

Say $S = \{1, \ldots, n\}$ and label the X_s as $X_1, \ldots, X_n$. The monomials are lexicographically ordered:

$$X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n}$$

iff $a_1 = b_1, \ldots, a_j = b_j$ and $a_{j+1} < b_{j+1}$ $(j = 0, \ldots, n-1)$.

(a) If $f = \sum_{(\xi)} a_{(\xi)} X^{(\xi)}$ and $g = \sum_{(\xi)} b_{(\xi)} X^{(\xi)}$, then $f + g = \sum_{(\xi)} (a_{(\xi)} + b_{(\xi)}) X^{(\xi)}$.
If $\deg(f+g) > \max\{\deg(f), \deg(g)\}$, then there is some η so that

$$\deg(X^{(\eta)}) > \deg(X^{(\xi)}), \quad \text{for all } \xi \text{ occurring in } f \text{ and } g, \text{ and } a_{(\eta)} + b_{(\eta)} \neq 0,$$

a contradiction.

(b) With f and g as in (a), we have

$$fg = \sum_{\xi} \left(\sum_{\substack{\eta, \eta', \\ \eta\eta' = \xi}} a_{(\eta)} b_{(\eta')} \right) X^{(\xi)}. \qquad (*)$$

Now,

$$\deg(X^{(\eta)}) + \deg(X^{(\eta')}) = \sum_s (\eta\eta')(s) = \sum_s \xi(s) = \deg(X^{(\xi)}).$$

However, $a_{(\eta)} \neq 0$ implies that $\deg(X^{(\eta)}) \leq \deg(f)$ and $b_{(\eta')} \neq 0$ implies that $\deg(X^{(\eta')}) \leq \deg(g)$, and this shows that $\deg(X^{(\xi)}) \leq \deg(f) + \deg(g)$, for any $X^{(\xi)}$ with nonzero coefficient in $(*)$.

When A is a domain, pick η to be the *first* monomial in the lexicographic ordering with $X^{(\eta)}$ of degree equal to $\deg(f)$, and similarly, pick η' to be the *first* monomial in the lexicographic ordering with $X^{(\eta')}$ of degree equal to $\deg(g)$. Then (DX), $X^{(\eta)} X^{(\eta')}$ is the monomial occurring first in the lexicographic ordering and of degree equal to $\deg(f) + \deg(g)$ in fg. Its coefficient is $a_{(\eta)} b_{(\eta')} \neq 0$, as A has no nonzero divisors; so, we have equality in (b).

(c) Say $u \in A[S]$ is a unit. Then, there is some $v \in A[S]$, so that $uv = vu = 1$. Consequently, $\deg(uv) = 0$, but $\deg(uv) = \deg(u) + \deg(v)$. Thus, $\deg(u) = \deg(v) = 0$ (as $\deg(u), \deg(v) \geq 0$), i.e., u, v are units of A.

(d) If $f, g \neq 0$, then $\deg(fg) = \deg(f) + \deg(g) \geq 0$, so $fg \neq 0$. $\square$

Definition 2.1 Suppose A is a commutative ring and B is a commutative A-algebra. Pick a subset, $S \subseteq |B|$. The set, S, is called *algebraically independent over A* (or *the elements of S are independent transcendentals over A*) iff the canonical map, $A[S] \longrightarrow B$, is a monomorphism. The set, S, is *algebraically dependent over A* iff the map, $A[S] \longrightarrow B$, is not a monomorphism. When $S = \{X\}$, then X is *transcendental*, resp. *algebraic over A* iff S is algebraically independent (resp. algebraically dependent) over A. The algebra, B, is a *finitely generated A-algebra* iff there is a finite subset, $S \subseteq |B|$, so that the canonical map $A[S] \longrightarrow B$ is surjective.

2.3 Operations on Modules; Finiteness Conditions for Rings and Modules

Let $R \in \mathrm{RNG}$, then by an R-module, we always mean a *left* R-module. Observe that a right R-module is exactly a left R^{op}-module. (Here, R^{op} is the opposite ring, whose multiplication $\cdot_{\mathrm{op}}$ is given by $x \cdot_{\mathrm{op}} y = y \cdot x$.) Every ring, R, is a module over itself and over R^{op}. By ideal, we always mean a *left* ideal. This is just an R-submodule of R. If an ideal, $\mathfrak{I}$, is both a left and a right ideal, then we call $\mathfrak{I}$ a *two-sided ideal*.

Let M be an R-module and $\{M_\alpha\}_{\alpha \in \Lambda}$ be a collection of R-submodules of M.

(0) $\bigcap_\alpha M_\alpha$ is an R-submodule of M.

(1) Note that we have a family of inclusion maps, $M_\alpha \hookrightarrow M$; so, we get an element of $\prod_\alpha \mathrm{Hom}_R(M_\alpha, M)$. But then, we have a map

$$\coprod_{\alpha \in \Lambda} M_\alpha \longrightarrow M. \qquad (*)$$

We define $\sum_\alpha M_\alpha$, a new submodule of M called *the sum of the M_α, via* any of the following three equivalent (DX) ways:

(a) Image of $(\coprod_{\alpha \in \Lambda} M_\alpha \longrightarrow M)$.

(b) $\bigcap \{N \mid (1)\ N \subseteq M$, as R-submodule; (2) $M_\alpha \subseteq N$, for all $\alpha \in \Lambda.\}$

(c) $\{\sum_{\mathrm{finite}} m_\alpha \mid m_\alpha \in M_\alpha\}$.

Clearly, $\sum_\alpha M_\alpha$ is the smallest submodule of M containing all the M_α.

(2) Let S be a subset of M. For any $s \in S$, the map $\rho \mapsto \rho s$, from R to Rs, is a surjection, where $Rs = \{\rho s \mid \rho \in R\}$. Thus, we get the submodule $\sum_{s \in S} Rs$ (equal to the image of $\coprod_S R \longrightarrow M$) and called *the submodule generated by S*; this module is denoted $\mathrm{mod}(S)$ or RS. We say that S *generates* M iff $RS = M$ and that M is a *finitely generated R-module* (for short, a *f.g. R-module*) iff there is a finite set, S, and a surjection $\coprod_S R \longrightarrow M$.

(3) The *free module on a set, S,* is just $\coprod_S R$. Observe that (DX) the functor from $\mathcal{S}\mathrm{ets}$ to $\mathcal{M}\mathrm{od}(R)$ given by $S \rightsquigarrow \coprod_S R$ is the left adjoint of the stripping functor from $\mathcal{M}\mathrm{od}(R)$ to $\mathcal{S}\mathrm{ets}$; i.e., for every R-module, M, we have the functorial isomorphism

$$\mathrm{Hom}_R(\coprod_S R, M) \cong \mathrm{Hom}_{\mathcal{S}\mathrm{ets}}(S, |M|).$$

Remark: An R-module, M, is free over R (i.e., $M \cong \coprod_S R$ for some set S) iff M possesses a Hamel basis over R (DX). The basis is indexed by S. To give a homomorphism of a free module to a module, M, is the same as giving the images of a Hamel basis in M, and these images may be chosen arbitrarily.

(4) The transporter of S to N. Let M be an R-module, S be a subset of M and N an R-submodule of M. The *transporter of S to N*, denoted $(S \to N)$, is given by

$$(S \to N) = \{\rho \in R \mid \rho S \subseteq N\}.$$

(Old notation: $(N : S)$. Old terminology: *residual quotient of N by S.*)
When $N = (0)$, then $(S \to (0))$ has a special name: the *annihilator* of S, denoted $\mathrm{Ann}(S)$. Observe:

(a) $(S \to N)$ is *always* an ideal of R.

(b) So, $\mathrm{Ann}(S)$ is an ideal of R. But if S is *a submodule* of M, then $\mathrm{Ann}(S)$ is a two-sided ideal of R. For if $\rho \in \mathrm{Ann}(S)$ and $\xi \in R$, we have $(\rho\xi)(s) = \rho(\xi s) \subseteq \rho S = (0)$. Thus, $\rho\xi \in \mathrm{Ann}(S)$.

(c) Similarly, if S is a *submodule* of M, then $(S \to N)$ is a two-sided ideal of R.

An R-module, M, is *finitely presented* (for short, *f.p.*) iff there are some *finite* sets, S and T, and an exact sequence

$$\coprod_T R \longrightarrow \coprod_S R \longrightarrow M \longrightarrow 0.$$

This means that M is finitely generated and that the kernel, K, of the surjection, $\coprod_S R \longrightarrow M$, is also finitely generated. Note that f.p. implies f.g.

Definition 2.2 An R-module, M, has the *ascending chain condition (ACC)* (resp. the *descending chain condition (DCC))* iff every ascending chain of submodules

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \subseteq M_n \subseteq \cdots,$$

eventually stabilizes (resp. every descending chain of submodules

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots \supseteq M_n \supseteq \cdots,$$

eventually stabilizes.) If M has the ACC it is called *noetherian* and if it has the DCC it is called *artinian*. The module, M, has the *maximal condition* (resp. *minimal condition*) iff every nonempty family of submodules of M has a maximal (resp. minimal) element.

Proposition 2.6 *Given a module, M, over R consider all the statements*

(1) M is noetherian (has the ACC).

(2) M has the maximal property.

(3) Every submodule of M is finitely generated.

(4) M is artinian (has the DCC).

(5) M has the minimal property.

Then, (1)–(3) are equivalent and (4) and (5) are equivalent.

Proof. (1) $\Longrightarrow$ (2). Let $\mathcal{F}$ be a given nonempty family of submodules of M. If there is no maximal element of $\mathcal{F}$, given $M_1 \in \mathcal{F}$, there is some M_2 in $\mathcal{F}$ so that $M_1 < M_2$. Repeating the argument, we find there is some $M_3 \in \mathcal{F}$ so that $M_2 < M_3$, and by induction, for every $n \geq 1$, we find some $M_{n+1} \in \mathcal{F}$ so that $M_n < M_{n+1}$. So, we find an infinite strictly ascending chain

$$M_1 < M_2 < M_3 < \cdots < M_t < \cdots,$$

contradicting (1).

(2) $\Longrightarrow$ (3). Observe that the maximal property for M is inherited by every submodule.

Claim: The maximal property for a module implies that it is finitely generated. If so, we are done. Pick M with the maximal property and let

$$\mathcal{F} = \{N \subseteq M \mid N \text{ is a submodule of } N \text{ and } N \text{ is f.g.}\}$$

The family, $\mathcal{F}$, is nonempty since for every $m \in M$, the module $Rm \subseteq M$ is a submodule of M generated by $\{m\}$, and so, $Rm \in \mathcal{F}$. Now, $\mathcal{F}$ has a maximal element, say T. If $T \neq M$, then there is some $m \in M$ with $m \notin T$. But now, $T + Rm > T$ and $T + Rm$ is finitely generated by the generators of T plus the new generator m, a contradiction. Therefore, $M = T \in \mathcal{F}$; and so, M is f.g.

(3) $\Longrightarrow$ (1). Take an ascending chain,

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_r \subseteq \cdots,$$

and look at $N = \bigcup_{i=1}^{\infty} M_i$. Note that N is a submodule of M. So, by (3), the module N is finitely generated. Consequently, there is some t so that M_t contains all the generators of N, and then we have $N \subseteq M_t \subseteq M_r \subseteq N$, for all $r \geq t$. Therefore, $M_t = M_r = N$ for all $r \geq t$.

(4) $\Longrightarrow$ (5). The proof is obtained from the proof of (1) $\Longrightarrow$ (2) *mutatis mutandis*.

(5) $\Longrightarrow$ (4). Say

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots \supseteq M_r \supseteq \cdots$$

is a descending chain in M. Let $\mathcal{F} = \{M_i \mid i \geq 1\}$. By (5), the family $\mathcal{F}$ has a minimal element, say M_r. Then, it is clear that the chain stabilizes at r. □

Proposition 2.7 *Let M be a module and write (α), (β) and (γ) for the finiteness properties*

(α) *finite generation*

(β) *ACC*

(γ) *DCC*

Then,

(A) If M has any of (α), (β), (γ), so does every factor module of M.

(B) If M has (β) or (γ), so does every submodule of M.

(C) Say $N \subseteq M$ is a submodule and N and M/N have any one of (α), (β), (γ). Then, M also has the same property.

Proof. (A) If M is f.g., then there is a surjection

$$\coprod_S R \longrightarrow M, \quad \text{with } \#(S) \text{ finite.}$$

Let $\overline{M}$ be a factor module of M; there is a surjection $M \longrightarrow \overline{M}$. By composition, we get a surjection

$$\coprod_S R \longrightarrow M \longrightarrow \overline{M},$$

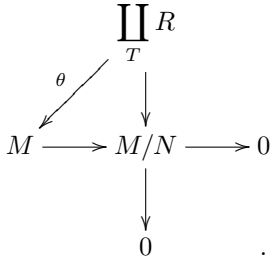
and so, $\overline{M}$ is f.g. Any ascending (resp. descending) chain in $\overline{M}$ lifts to a similar chain of M. The rest is clear.

(B) Any ascending (resp. descending) chain in $N \subseteq M$ is a similar chain of M; the rest is clear.

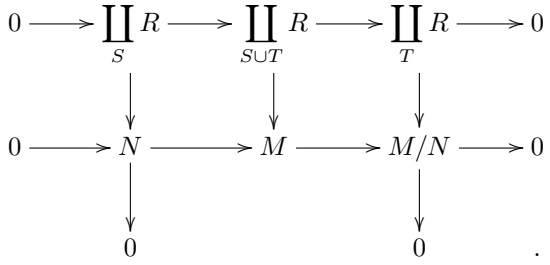
(C) Say N and M/N have (α). Then, there are two finite (disjoint) sets, S and T, and surjections

$$\coprod_S R \longrightarrow N \longrightarrow 0 \quad \text{and} \quad \coprod_T R \longrightarrow M/N \longrightarrow 0.$$

Consider the diagram:



As $\coprod_T R$ is free, there exists an arrow, $\theta\colon \coprod_T R \longrightarrow M$, shown above, and the diagram commutes. Now, consider the diagram:

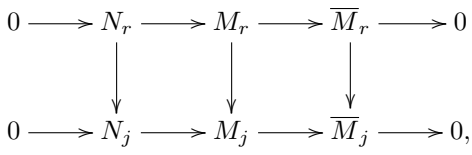


We obtain the middle vertical arrow by the map θ and the set map $S \longrightarrow M$ (*via* $S \longrightarrow N \hookrightarrow M$). By construction, our diagram commutes. We claim that the middle arrow is surjective. For this, we chase the diagram: Choose m in M and map m to $\overline{m} \in M/N$. There is some $\xi \in \coprod_T R$ so that $\xi \mapsto \overline{m}$. However, ξ comes from $\eta \in \coprod_{S\cup T} R$. Let $\widetilde{\eta}$ be the image in M of η. Since the diagram is commutative, $\overline{\widetilde{\eta}} = \overline{m}$, and so, $\widetilde{\eta} - m$ maps to 0 in M/N. Consequently, there is some $n \in N$ so that $\widetilde{\eta} - m = n$. Yet, n comes from some ρ in $\coprod_S R \hookrightarrow \coprod_{S\cup T} R$ (i.e., $\widetilde{\rho} = n$). Consider $\eta - \rho \in \coprod_{S\cup T} R$. The image of $\eta - \rho$ in M is $\widetilde{\eta} - \widetilde{\rho} = m + n - n = m$, proving surjectivity. As $S \cup T$ is finite, the module, M, has (α).

Next, assume N and M/N have (β). Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \subseteq M_r \subseteq \cdots$$

be an ascending chain in M. Write $\overline{M}_j$ for the image of M_j in M/N. By the ACC in M/N, there is some $t \geq 1$ so that $\overline{M}_j = \overline{M}_t$ for all $j \geq t$. If we let $N_j = M_j \cap N$, we get an ascending chain in N. By the ACC in N, this chains stabilizes, i.e., there is some $s \geq 1$ so that $N_j = N_s$ for all $j \geq s$. Let $r = \max\{s, t\}$. We claim that $M_j = M_r$ for all $j \geq r$. We have the diagram



where the rows are exact and the vertical arrows on the left and on the right are surjections. A diagram chase yields the fact that the middle vertical arrow is also surjective.

Finally, assume N and M/N have (γ). The same argument works with the arrows and inclusions reversed.
□

Corollary 2.8 *Say $\{M_\lambda\}_{\lambda\in\Lambda}$ is a family of R-modules. Then, $\coprod_\lambda M_\lambda$ has one of (α), (β), (γ) iff each M_λ has the corresponding property and Λ is finite.*

Proof. We have a surjection

$$\coprod_\lambda M_\lambda \longrightarrow M_\mu \longrightarrow 0, \quad \text{for any fixed } \mu.$$

Consequently, (α), (β), (γ) for $\coprod_\lambda M_\lambda$ implies (α), (β), (γ) for M_μ, by the previous proposition. It remains to prove that Λ is finite.

First, assume that $\coprod_\lambda M_\lambda$ has (α), and further assume that Λ is infinite. There is some finite set, S, and a surjection $\coprod_S R \longrightarrow \coprod_\lambda M_\lambda$. We may assume that $S = \{1, \ldots, n\}$, for some positive integer, n. Then, we have the canonical basis vectors, $e_1, \ldots, e_n$, of $\coprod_S R$, and their images $\overline{e}_1, \ldots, \overline{e}_n$ generate $\coprod_\lambda M_\lambda$. Each image $\overline{e}_i$ is a finite tuple in $\coprod_\lambda M_\lambda$. Yet, the union of the finite index sets so chosen is again finite and for any μ not in this finite set, the image of M_μ in $\coprod_\lambda M_\lambda$ is not covered. This contradicts the fact that the $\overline{e}_i$'s generate $\coprod_\lambda M_\lambda$, and so, Λ must be finite.

We treat (β) and (γ) together. Again, assume that Λ is infinite. Then, there is a countably infinite subset of Λ, denote it $\{\lambda_1, \lambda_2, \ldots\}$, and the chains

$$M_{\lambda_1} < M_{\lambda_1} \amalg M_{\lambda_2} < M_{\lambda_1} \amalg M_{\lambda_2} \amalg M_{\lambda_3} < \cdots$$

and

$$\coprod_{j=1}^{\infty} M_{\lambda_j} > \coprod_{j\neq 1} M_{\lambda_j} > \coprod_{j\neq 1,2} M_{\lambda_j} > \cdots$$

are infinite ascending (resp. descending) chains of $\coprod_\lambda M_\lambda$, a contradiction.

Finally, assume that each M_λ has (α) or (β) or (γ) and that Λ is finite. We use induction on $\#(\Lambda)$. Consider the exact sequence

$$0 \longrightarrow \coprod_{j\neq 1} M_j \longrightarrow \coprod_{j\in\Lambda} M_j \longrightarrow M_1 \longrightarrow 0.$$

Then, (α) (resp. (β), (γ)) holds for the right end by hypothesis, and it also holds for the left end, by induction; so, (α) (resp. (β), (γ)) holds in the middle. □

Corollary 2.9 *Say R is noetherian (has the ACC on ideals) or artinian (has the DCC on ideals). Then,*

(1) Every f.g. free module, $\coprod_S R$, is noetherian, resp. artinian, as R-module (remember, $\#(S) < \infty$).

(2) Every f.g. R-module is noetherian, resp. artinian.

(3) When R is noetherian, every f.g. R-module is f.p. Finitely presented modules are always f.g.

Proof. (1) and (2) are trivial from Corollary 2.8.

As for (3), that f.p. implies f.g. is clear by the definition. Say M is f.g. Then, we have an exact sequence

$$0 \longrightarrow K \longrightarrow \coprod_S R \longrightarrow M \longrightarrow 0,$$

with $\#(S) < \infty$. By (1), the module $\coprod_S R$ is noetherian; by Proposition 2.6, the module K is f.g. Thus, there is some finite set, T, so that

$$\coprod_T R \longrightarrow K \longrightarrow 0 \quad \text{is exact.}$$

By splicing the two sequences, we get the exact sequence

$$\coprod_T R \longrightarrow \coprod_S R \longrightarrow M \longrightarrow 0,$$

which shows that M is f.p. □

Counter-examples.

(1) A subring of a noetherian ring need not be a noetherian ring. Take $A = \mathbb{C}[X_1, X_2, \ldots, X_n, \ldots]$ the polynomial ring in countably many variables, and let $K = \mathrm{Frac}(A)$. Every field is noetherian as a ring (a field only has two ideals, (0) and itself). We have $A \subseteq K$, yet A is not noetherian, for we claim that we have the ascending chain of ideals

$$(X_1) < (X_1, X_2) < (X_1, X_2, X_3) < \cdots$$

Would this chain stabilize, then we would have $(X_1, \ldots, X_n) = (X_1, \ldots, X_n, X_{n+1})$, for some $n \geq 1$. Now, there would be some polynomials $f_1, \ldots, f_n$ in A so that

$$X_{n+1} = f_1 X_1 + \cdots + f_n X_n.$$

Map A to $\mathbb{C}$ *via* the unique homomorphism sending X_j to 0 for $j = 1, \ldots, n$, and sending X_j to 1 for $j > n$. We get $1 = 0$, a contradiction. Therefore, the chain is strictly ascending.

(2) A module which is finitely generated need not be finitely presented. Let $A = \mathbb{C}[X_1, \ldots, X_n, \ldots]$, the polynomial algebra over $\mathbb{C}$ in countably many variables. Then, $\mathbb{C}$ is an A-module because of the exact sequence

$$0 \longrightarrow \mathfrak{I} = (X_1, \ldots, X_n, \ldots) \longrightarrow A \longrightarrow \mathbb{C} \longrightarrow 0,$$

in which the map $A \longrightarrow \mathbb{C}$ is given by $f \mapsto f(0)$; the ring A acts on $\mathbb{C}$ *via* $f \cdot z = f(0)z$, where $f \in A$ and $z \in \mathbb{C}$. Assume that $\mathbb{C}$ is finitely presented. Then, there are some finite sets, S and T, and an exact sequence

$$\coprod_T A \longrightarrow \coprod_S A \longrightarrow \mathbb{C} \longrightarrow 0.$$

We get the diagram

$$\begin{array}{ccccccccc} & & \coprod_T A & \longrightarrow & \coprod_S A & \longrightarrow & \mathbb{C} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \Theta} & & \| & & \\ 0 & \longrightarrow & \mathfrak{I} & \longrightarrow & A & \longrightarrow & \mathbb{C} & \longrightarrow & 0 \end{array}$$

To construct the vertical arrows, let $e_1, \ldots, e_s$ be the usual generators of $\coprod_S A$. If $z_1, \ldots, z_s \in \mathbb{C}$ are their images, there exist $\lambda_1, \ldots, \lambda_s \in A$ so that

$$\sum_{j=1}^{s} \lambda_j e_j \mapsto \sum_{j=1}^{s} \lambda_j(0) z_j = 1.$$

We have the ($\mathbb{C}$-linear) map, $\mathbb{C} \longrightarrow A$, so our z_j lie in A. Then, we have $\sum_{j=1}^{s} \lambda_j(0) z_j = 1$, in A. If we send $e_j \mapsto z_j \in A$, we get an A-linear map, $\Theta\colon \coprod_S A \to A$, and there is some $\xi \in \coprod_S A$ with $\Theta(\xi) = 1 \in A$. Namely, take

$$\xi = \sum_{j=1}^{s} \lambda_j(0) e_j.$$

But then, Θ is onto, because its image is an ideal which contains 1. A diagram chase implies that there exists some $\varphi\colon \coprod_T A \to \mathfrak{I}$ rendering the diagram commutative. Another diagram chase gives the fact that φ is surjective. But then, $\mathfrak{I}$ is finitely generated, a contradiction. Therefore, $\mathbb{C}$ is not f.p. (over A).

Remark: The difficulty is that A is much "bigger" than $\mathbb{C}$, and thus, the surjection $A \longrightarrow \mathbb{C}$ has to "kill" an infinite number of independent elements.

Consider the category, $\mathcal{M}\mathrm{od}(R)$. We can also look at subcategories of $\mathcal{M}\mathrm{od}(R)$ having some additional properties. For example, a subcategory, $\mathcal{C}$, of $\mathcal{M}\mathrm{od}(R)$ is a *localizing subcategory* iff

(a) Whenever M and $N \in \mathcal{O}\mathrm{b}(\mathcal{C})$ and $\theta\colon M \to N$ is a morphism of $\mathcal{C}$, then Ker θ and Coker $\theta = (N/\mathrm{Im}\ \theta)$ lie in $\mathcal{O}\mathrm{b}(\mathcal{C})$ and the morphisms Ker $\theta \longrightarrow M$ and $N \longrightarrow$ Coker θ are arrows of $\mathcal{C}$.

(b) Whenever
$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \quad \text{is exact (in } \mathcal{M}\mathrm{od}(R))$$
and $M', M'' \in \mathcal{O}\mathrm{b}(\mathcal{C})$, then $M \in \mathcal{O}\mathrm{b}(\mathcal{C})$ and the sequence is exact in $\mathcal{C}$.

Example: Let $\mathcal{C} = \mathcal{M}\mathrm{od}^{\mathrm{fg}}(R)$ be the full subcategory of finitely generated R-modules, where R is noetherian. The reader should check that $\mathcal{C}$ is a localizing subcategory.

Recall that an R-module is a *simple* iff it has *no* nontrivial submodules; a composition series is a finite descending chain
$$M = M_0 > M_1 > M_2 > \cdots > M_t = (0)$$
in which all the factors M_j/M_{j+1} are simple. We know from the Jordan–Hölder theorem that the number of composition factors, t, is an invariant and the composition factors are unique (up to isomorphism and rearrangement). We set $\lambda_R(M) = t$, and call it the *length* of M; if M does not have a composition series, set $\lambda_R(M) = \infty$.

Say $\mathcal{C}$ is a localizing subcategory of $\mathcal{M}\mathrm{od}(R)$ and φ is a function on $\mathcal{O}\mathrm{b}(\mathcal{C})$ to some fixed abelian group, A.

Definition 2.3 The function, φ, is an *Euler function* iff whenever
$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \quad \text{is exact in } \mathcal{C},$$
we have $\varphi(M) = \varphi(M') + \varphi(M'')$.

Proposition 2.10 *A necessary and sufficient condition that a module, M, have finite length is that M has both ACC and DCC on submodules. The function λ_R on the full subcategory of finite-length modules (which is a localizing subcategory), is an Euler function. If φ is an Euler function on some localizing subcategory of $\mathcal{M}\mathrm{od}(R)$ and if*
$$(E) \qquad 0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_t \longrightarrow 0$$
is an exact sequence in this subcategory, then
$$\chi_\varphi((E)) = \sum_{j=1}^{t} (-1)^j \varphi(M_j) = 0.$$

Proof. First, assume that M has finite length. We prove the ACC and the DCC by induction on $\lambda_R(M)$. If $\lambda_R(M) = 1$, then M is simple, so the ACC and the DCC hold trivially. Assume that this is true for $\lambda_R(M) = t$, and take $\lambda_R(M) = t + 1$. We have a composition series
$$M = M_0 > M_1 > M_2 > \cdots > M_{t+1} = (0),$$
and so, $\lambda_R(M_1) = t$ and $\lambda_R(M/M_1) = 1$. But the sequence
$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M/M_1 \longrightarrow 0 \quad \text{is exact,}$$
and the ACC and DCC hold on the ends, by induction. Therefore, they hold in the middle.

Now, assume that the DCC and the ACC hold for M. Let
$$\mathcal{F} = \{N \subseteq M \mid N \neq M,\ N \text{ is a submodule of } M.\}$$

The family $\mathcal{F}$ is nonempty (the trivial module (0) is in $\mathcal{F}$) and by the ACC, it has a maximal element, M_1; so, M/M_1 is simple. Apply the same argument to M_1: We get $M_2 < M_1$ with M_1/M_2 simple. By induction, we get a strictly descending chain

$$M = M_0 > M_1 > M_2 > \cdots > M_t > \cdots$$

However, by the DCC, this chain must stabilize. Now, if it stabilizes at M_t, we must have $M_t = (0)$, since otherwise we could repeat the first step in the argument for M_t. This proves that $\lambda_R(M) = t < \infty$.

Say $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is exact in $\mathcal{M}\mathrm{od}^{\mathrm{fl}}(R)$. Pick a composition series for M''. We get a strictly descending chain

$$M'' = M_0'' > M_1'' > M_2'' > \cdots > M_t'' = (0).$$

By the second homomorphism theorem, we get a lifted sequence

$$M = M_0 > M_1 > M_2 > \cdots > M_t = M',$$

and if we pick a composition series for M', we get the following composition series with $s + t = \lambda_R(M') + \lambda_R(M'')$ factors, as required:

$$M = M_0 > M_1 > M_2 > \cdots > M_t = M' > M_1' > M_2' > \cdots > M_s' = (0).$$

Say

$$(E) \qquad 0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_{t-2} \longrightarrow M_{t-1} \xrightarrow{\theta} M_t \longrightarrow 0$$

is an exact sequence. Then, we have the two exact sequences

$$\begin{aligned} (E') \qquad & 0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_{t-2} \longrightarrow \mathrm{Ker}\ \theta \longrightarrow 0 \quad \text{and} \\ (E'') \qquad & 0 \longrightarrow \mathrm{Ker}\ \theta \longrightarrow M_{t-1} \longrightarrow M_t \longrightarrow 0. \end{aligned}$$

The cases $t = 1, 2, 3$ are trivial (DX). By using induction on t, we see that the proposition is true for (E') and (E''). Thus, we get

$$\begin{aligned} \sum_{j=1}^{t-2} (-1)^j \varphi(M_j) + (-1)^{t-1} \varphi(\mathrm{Ker}\ \theta) &= 0 \quad \text{and} \\ \varphi(\mathrm{Ker}\ \theta) &= \varphi(M_{t-1}) - \varphi(M_t). \end{aligned}$$

If we add the first equation to $(-1)^t$ times the second equation we get

$$\sum_{j=1}^{t-2} (-1)^j \varphi(M_j) = (-1)^t \varphi(M_{t-1}) - (-1)^t \varphi(M_t),$$

and so,

$$\chi_\varphi((E)) = \sum_{j=1}^{t-2} (-1)^j \varphi(M_j) + (-1)^{t-1} \varphi(M_{t-1}) + (-1)^t \varphi(M_t) = 0,$$

as claimed. □

Theorem 2.11 *(Hilbert Basis Theorem (1890)) If A is a commutative noetherian ring, then so is the polynomial ring $A[X]$.*

Proof. Let A_n be the submodule of $A[X]$ consisting of the polynomials of degree at most n. The module, A_n, is a free module over A (for example, $1, X, X^2, \ldots, X^n$ is a basis of A_n). If $\mathfrak{A}$ is an ideal of $A[X]$, then $\mathfrak{A} \cap A_n$ is a submodule of A_n. As A_n (being finitely generated over A) is a noetherian module, $\mathfrak{A} \cap A_n$ is also finitely generated, say by $\alpha_1, \alpha_2, \ldots, \alpha_{\kappa(n)}$ ($\in A[X]$). If $f \in \mathfrak{A}$ and $\deg(f) \leq n$, then $f \in A_n$; so,

$$f = a_1\alpha_1 + \cdots + a_{\kappa(n)}\alpha_{\kappa(n)}, \quad \text{with } a_j \in A.$$

Now, let $\mathfrak{A}^*$ be the subset of A consisting of all $a \in A$ so that either $a = 0$ or there is some polynomial f in $\mathfrak{A}$ having a as its leading coefficient, i.e., $f = aX^r + O(X^{r-1})$. We claim that $\mathfrak{A}^*$ is an ideal of A.

Say a and b are in $\mathfrak{A}^*$. Then, there are some polynomials $f, g \in \mathfrak{A}$ so that $f = aX^r + O(X^{r-1})$ and $g = bX^s + O(X^{s-1})$. Take $t = \max\{r, s\}$. Then, $X^{t-r}f \in \mathfrak{A}$ and $X^{t-s}g \in \mathfrak{A}$, since $\mathfrak{A}$ is an ideal. But,

$$X^{t-r}f = aX^t + O(X^{t-1}) \quad \text{and} \quad X^{t-s}g = bX^t + O(X^{t-1}),$$

and this implies that $a \pm b \in \mathfrak{A}^*$, as $a \pm b$ is the leading coefficient of $X^{t-r}f \pm X^{t-s}g \in \mathfrak{A}$. If $\lambda \in A$ and $a \in \mathfrak{A}^*$, then it is clear that $\lambda a \in \mathfrak{A}^*$. Therefore, $\mathfrak{A}^*$ is indeed an ideal in A. Now, A is a noetherian ring, therefore $\mathfrak{A}^*$ is finitely generated as an ideal. So, there exist $\beta_1, \ldots, \beta_t \in \mathfrak{A}^* \subseteq A$, such that for any $\beta \in \mathfrak{A}^*$, we have $\beta = \sum_{i=1}^t \lambda_i\beta_i$, for some $\lambda_i \in A$. Now, by definition of $\mathfrak{A}^*$, for every $\beta_i \in \mathfrak{A}^*$, there is some $f_i(X) \in \mathfrak{A}$ so that $f_i(X) = \beta_i X^{n_i} + O(X^{n_i-1})$. Let $n = \max\{n_1, \ldots, n_t\}$ and consider the generators $\alpha_1, \ldots, \alpha_{\kappa(n)}$ of $\mathfrak{A}_n = A_n \cap \mathfrak{A}$.

Claim: The set $\{\alpha_1, \ldots, \alpha_{\kappa(n)}, f_1, \ldots, f_t\}$ generates $\mathfrak{A}$.

Pick some $g \in \mathfrak{A}$. Then, $g(X) = \beta X^r + O(X^{r-1})$, for some r. If $r \leq n$, then $g(X) \in \mathfrak{A}_n$, and thus, $g = \lambda_1\alpha_1 + \cdots + \lambda_{\kappa(n)}\alpha_{\kappa(n)}$, with $\lambda_i \in A$. Say $r > n$. Now, $\beta \in \mathfrak{A}^*$, so there are elements $\lambda_1, \ldots, \lambda_t \in A$ such that $\beta = \lambda_1\beta_1 + \cdots + \lambda_t\beta_t$. Consider the polynomial

$$P(X) = \sum_{i=1}^{t} \lambda_i X^{r-n_i} f_i(X),$$

and examine $g(X) - P(X)$. We have

$$g(X) - P(X) = \beta X^r - \sum_{i=1}^{t} \lambda_i X^{r-n_i} f_i(X) + O(X^{r-1}) = O(X^{r-1}),$$

and thus there is a $P(X) \in (f_1, \ldots, f_t)$ so that $\deg(g(X) - P(X)) \leq r - 1$. By repeating this process, after finitely many steps, we get

$$g(X) - \sum_{i=1}^{t} h_i(X) f_i(X) = O(X^{\leq n}).$$

Since this polynomial belongs to $\mathfrak{A}$, we deduce that it belongs to $\mathfrak{A}_n$. However, $\mathfrak{A}_n$ is generated by $\alpha_1, \ldots, \alpha_{\kappa(n)}$, and so, $g(X)$ is an $A[X]$-linear combination of the $f_i(X)$'s and the $\alpha_j(X)$'s, as desired. □

Remark: The reader should reprove Hilbert's theorem using the same argument but involving ascending chains. This is Noether's argument (DX).

Corollary 2.12 *Say $R \in$ RNG. If R is noetherian, so is $R\langle X\rangle$.*

Proof. We have $R\langle X\rangle = R[X]$, and the same proof works. □

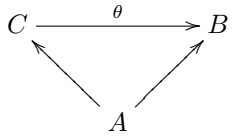
Corollary 2.13 *If A (in* CR*) is noetherian, then so is $A[X_1, \ldots, X_n]$.*

Corollary 2.14 *(Hilbert's original theorem) The polynomial ring $\mathbb{Z}[X_1, \ldots, X_n]$ is noetherian. If k is a field (Hilbert chose $\mathbb{C}$) then $k[X_1, \ldots, X_n]$ is noetherian.*

Corollary 2.15 *(of the proof–(DX)) If k is a field, then $k[X]$ is a PID.*

Corollary 2.16 *Say A is a noetherian ring ($A \in$ CR) and B is a finitely generated A-algebra. Then, B is a noetherian ring.*

Proof. The hypothesis means that B is a homomorphic image of a polynomial ring $C = A[X_1, \ldots, X_n]$ in such a way that the diagram



commutes, where $A \longrightarrow C$ is the natural injection of A into $C = A[X_1, \ldots, X_n]$. The ring $A[X_1, \ldots, X_n]$ is noetherian, by Corollary 2.13. The map θ makes B into a C-module and B is finitely generated as C-*module*. Now, C-submodules are exactly the ideals of B (DX). Since B is finitely generated as C-module and C is noetherian, this implies that B is a noetherian C-module. Therefore, the ACC on C-submodules holds, and since these are ideals of B, the ring B is noetherian. □

To be finitely generated as A-algebra is **very** different from being finitely generated as A-module.

Given an exact sequence of modules,

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

there are situations where it is useful to know that M' is f.g, given that M and M'' satisfy certain finiteness conditions. We will give below a proposition to this effect. The proof makes use of Schanuel's lemma. First, introduce the following terminology: Given a module M, call an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0,$$

a *presentation* of M if F is free. Note that M is f.p. iff there is a presentation of M in which both F and K are f.g.

Proposition 2.17 *If M is a Λ-module, then M is f.p. iff every presentation*

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0, \qquad (*)$$

in which F is f.g. has K f.g. and at least one such exists.

Proof. The direction ($\Leftarrow$) is clear.

($\Rightarrow$). Say M is f.p.; we have an exact sequence

$$0 \longrightarrow K' \longrightarrow F' \longrightarrow M \longrightarrow 0,$$

where both K' and F' are f.g. and F' is free. Pick any presentation, $(*)$, with F f.g. If we apply Schanuel's lemma, we get

$$F' \coprod K \cong F \coprod K',$$

But, the righthand side is f.g. and K is a quotient of the left hand side, so it must be f.g. □

Remark: The forward implication of Proposition 2.17 also holds even if F is not free. A simple proof using the snake lemma will be given at the end of Section 2.5.

2.4 Projective and Injective Modules

Let $F\colon \mathcal{M}\mathrm{od}(R) \to \mathcal{M}\mathrm{od}(S)$ be a functor (where $R, S \in \mathrm{RNG}$). Say

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \tag{$*$}$$

is exact in $\mathcal{M}\mathrm{od}(R)$. What about

$$0 \longrightarrow F(M') \longrightarrow F(M) \longrightarrow F(M'') \longrightarrow 0? \tag{$**$}$$

(1) The sequence $(**)$ is a complex if F is an *additive* functor. (Observe that $\mathrm{Hom}_R(M, N)$ is an abelian group, so is $\mathrm{Hom}_S(F(M), F(N))$. We say F is additive iff $\mathrm{Hom}_R(M, N) \xrightarrow{F(\cdot)} \mathrm{Hom}_S(F(M), F(N))$ is a homomorphism, i.e., preserves addition.)

(2) The functor, F, is *exact* iff when $(*)$ is exact then $(**)$ is exact (the definition for cofunctors is identical).

(3) The functor, F, is a *left-exact* if whenever the sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M''$$

is exact, then the sequence

$$0 \longrightarrow F(M') \longrightarrow F(M) \longrightarrow F(M'')$$

is exact, *right exact* if whenever the sequence

$$M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is exact, then the sequence

$$F(M') \longrightarrow F(M) \longrightarrow F(M'') \longrightarrow 0$$

is exact.

(4) The functor, F, is *half-exact* (same definition for cofunctors) iff when $(*)$ is exact

$$F(M') \longrightarrow F(M) \longrightarrow F(M'')$$

is still exact.

(5) The cofunctor, G, is *left exact* if whenever the sequence

$$M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is exact, then the sequence

$$0 \longrightarrow G(M'') \longrightarrow G(M) \longrightarrow G(M')$$

is exact, *right exact* if if whenever the sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M''$$

is exact, then the sequence

$$G(M'') \longrightarrow G(M) \longrightarrow G(M') \longrightarrow 0$$

is exact.

Remark: *The chirality of a functor is determined by the image category.*

Examples of exact (left-exact, right-exact, etc.) functors:

(1) Let $F\colon \mathcal{M}\mathrm{od}(R) \to \mathcal{M}\mathrm{od}(\mathbb{Z})$ be given by: $F(M) =$ underlying abelian group of M. The functor F is exact.

(2) Take a set, Λ, and look at

$$\mathcal{M}\mathrm{od}(R)^{\Lambda} = \{\{M_\alpha\}_{\alpha\in\Lambda} \mid \text{each } M_\alpha \in \mathcal{M}\mathrm{od}(R)\},$$

together with obvious morphisms. We have two functors from $\mathcal{M}\mathrm{od}(R)^{\Lambda}$ to $\mathcal{M}\mathrm{od}(R)$. They are:

$$\{M_\alpha\} \rightsquigarrow \prod_\alpha M_\alpha \quad \text{and} \quad \{M_\alpha\} \rightsquigarrow \coprod_\alpha M_\alpha.$$

Both are exact functors (this is special to modules). The next proposition is a most important example of left-exact functors:

Proposition 2.18 *Fix an R-module, N. The functor from $\mathcal{M}\mathrm{od}(R)$ to $\mathcal{A}\mathrm{b}$ (resp. cofunctor from $\mathcal{M}\mathrm{od}(R)$ to $\mathcal{A}\mathrm{b}$) given by $M \rightsquigarrow \mathrm{Hom}_R(N, M)$ (resp. $M \rightsquigarrow \mathrm{Hom}_R(M, N)$) is left-exact (***N.B.: both are left-exact***).*

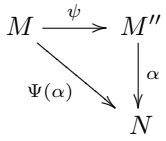
Proof. Consider the case of a cofunctor (the case of a functor is left to the reader (DX)). Assume that

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

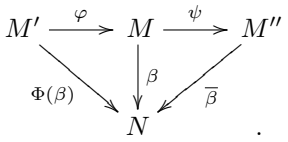
is exact. Look at the sequence obtained by applying $\mathrm{Hom}_R(-, N)$ to the above exact sequence:

$$0 \longrightarrow \mathrm{Hom}_R(M'', N) \xrightarrow{\Psi} \mathrm{Hom}_R(M, N) \xrightarrow{\Phi} \mathrm{Hom}_R(M', N) \longrightarrow 0,$$

where $\Phi = - \circ \varphi$ and $\Psi = - \circ \psi$. Pick $\alpha \in \mathrm{Hom}_R(M'', N)$ and assume that $\Psi(\alpha) = 0$. We have the commutative diagram



and since $M \xrightarrow{\psi} M''$ is surjective, we deduce that $\alpha = 0$. Now, pick $\beta \in \mathrm{Hom}_R(M, N)$ and assume that $\Phi(\beta) = 0$. We have the commutative diagram (see argument below)



Since $\Phi(\beta) = 0$, we have $\mathrm{Im}\ \varphi \subseteq \mathrm{Ker}\ \beta$; so, by the first homomorphism theorem, there is a homomorphism $\overline{\beta}\colon M/M' = M'' \to N$, as shown, making the above diagram commute. Thus, $\Psi(\overline{\beta}) = \overline{\beta} \circ \psi = \beta$, and so, $\beta \in \mathrm{Im}\ \Psi$. $\square$

There may be some modules, N, so that our Hom functors become exact as functors of M. This is the case for the class of R-modules introduced in the next definition:

Definition 2.4 A module, P, is *projective (over R)* iff the functor $M \rightsquigarrow \mathrm{Hom}_R(P, M)$ is exact. A module, Q, is *injective (over R)* iff the cofunctor $M \rightsquigarrow \mathrm{Hom}_R(M, Q)$ is exact.

Remarks:

(1) Any free R-module is projective over R.

Proof. Say $F = \coprod_S R$. Consider the functor $M \rightsquigarrow \mathrm{Hom}_R(\coprod_S R, M)$. The righthand side is equal to $\prod_S \mathrm{Hom}_R(R, M) = \prod_S M$, but we know that the functor $M \rightsquigarrow \prod_S M$ is exact. □

(2) A functor is left-exact iff it preserves the left-exactness of a short left-exact sequence (resp. a cofunctor is left-exact iff it transforms a short right-exact sequence into a left-exact sequence), and *mutatis mutandis* for right exact functors or cofunctors.

(3) Compositions of left (resp. right) exact functors are left (resp. right) exact. Similarly, compositions of exact functors are exact.

We say that an exact sequence

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

splits iff there is a map $\sigma\colon M'' \to M$ so that $p \circ \sigma = \mathrm{id}_{M''}$. Such a map, σ, is called a *splitting* of the sequence. The following properties are equivalent (DX):

Proposition 2.19 *(1) The sequence*

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

splits.

(2) Given our sequence as in (1),

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

there is a map $\pi\colon M \to M'$ so that $\pi \circ i = \mathrm{id}_{M'}$.

(3) There is an isomorphism $M' \amalg M'' \cong M$.

Proposition 2.20 *Let P be an R-module, then the following are equivalent:*

(1) P is projective over R.

(2) Given a diagram

$$\begin{array}{ccccc} & & & & P \\ & & & & \downarrow \xi \\ M & \longrightarrow & M'' & \longrightarrow & 0, \end{array}$$

there exists a map, $\theta\colon P \to M$, lifting ξ, rendering the diagram commutative (lifting property).

(3) Any exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow P \longrightarrow 0$ splits.

(4) There exists a free module, F, and another module, $\widetilde{P}$, so that $P \amalg \widetilde{P} \cong F$.

Proof. (1) ⇒ (2). Given the projective module, P and the diagram

$$\begin{array}{ccccc} & & & & P \\ & & & & \downarrow \xi \\ M & \longrightarrow & M'' & \longrightarrow & 0, \end{array}$$

the exact sequence gives the map

$$\mathrm{Hom}_R(P, M) \longrightarrow \mathrm{Hom}_R(P, M'') \qquad (\dagger)$$

and the diagram gives an element, ξ, of $\mathrm{Hom}_R(P, M'')$. But P is projective, and so, $(\dagger)$ is surjective. Consequently, ξ comes from some $\eta \in \mathrm{Hom}_R(P, M)$, proving the lifting property.

(2) $\Rightarrow$ (3). Given an exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow P \longrightarrow 0,$$

we get the diagram

$$\begin{array}{ccccc} & & P & & \\ & & \| & & \\ M & \longrightarrow & P & \longrightarrow & 0. \end{array}$$

The lifting property gives the backwards map $P \longrightarrow M$, as required.

(3) $\Rightarrow$ (4). Given P, there is a free module, F. and a surjection, $F \longrightarrow P$. We get the exact sequence

$$0 \longrightarrow \widetilde{P} \longrightarrow F \longrightarrow P \longrightarrow 0,$$

where $\widetilde{P} = \mathrm{Ker}\,(F \longrightarrow P)$. By hypothesis, this sequence splits. Therefore, by property (3) of Proposition 2.19, we have $F \cong P \amalg \widetilde{P}$.

(4) $\Rightarrow$ (1). We have $F \cong P \amalg \widetilde{P}$, for some free R-module, F. Now, $F = \coprod_S R$, for some set, S, and so, for any N,

$$\mathrm{Hom}_R(F, N) = \prod_S \mathrm{Hom}_R(R, N) = \prod_S N.$$

The functor $N \rightsquigarrow \mathrm{Hom}_R(F, N)$ is exact; yet, this functor is $N \rightsquigarrow \mathrm{Hom}_R(P, N) \prod \mathrm{Hom}_R(\widetilde{P}, N)$. Assume that the sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \quad \text{is exact,}$$

we need to show that $\mathrm{Hom}_R(P, M) \longrightarrow \mathrm{Hom}_R(P, M'')$ is surjective. This follows by chasing the diagram (DX):

$$\begin{array}{ccc} \mathrm{Hom}(F, M) & \xrightarrow{\cong} & \mathrm{Hom}(P, M) \prod \mathrm{Hom}(\widetilde{P}, M) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(F, M'') & \xrightarrow{\cong} & \mathrm{Hom}(P, M'') \prod \mathrm{Hom}(\widetilde{P}, M'') \\ \downarrow & & \\ 0 & & . \end{array}$$

□

Given an R-module, M, a *projective resolution* (resp. a *free resolution*) of M is an exact (possibly infinite) sequence (= *acyclic resolution*) of modules

$$\cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M,$$

with all the $P_i's$ projective (resp. free)

Corollary 2.21 *Every R-module possesses a projective resolution (even a free resolution).*

Proof. Since free modules are projective, it is enough to show that free resolutions exist. Find a free module, F_0, so that there is a surjection, $F_0 \longrightarrow M$. Let $M_1 = \mathrm{Ker}\,(F_0 \longrightarrow M)$, and repeat the process. We get a free module, F_1, and a surjection, $F_1 \longrightarrow M_1$. By splicing the two exact sequences
$0 \longrightarrow M_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$ and $F_1 \longrightarrow M_1 \longrightarrow 0$, we get the exact sequence $F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$. We obtain a free resolution by repeating the above process. □

Proposition 2.22 *Given a family, $\{P_\alpha\}_{\alpha\in\Lambda}$, of modules, the coproduct $\coprod_\alpha P_\alpha$ is projective iff each P_α is projective.*

Proof. Assume that each P_α is projective. This means that for every α, the functor $M \rightsquigarrow \mathrm{Hom}_R(P_\alpha, M)$ is exact. As the product functor is exact and composition of exact functors is exact, the functor
$M \rightsquigarrow \prod_\alpha \mathrm{Hom}_R(P_\alpha, M)$ is exact. But

$$\prod_\alpha \mathrm{Hom}_R(P_\alpha, M) = \mathrm{Hom}_R(\coprod_\alpha P_\alpha, M).$$

Therefore, $\coprod_\alpha P_\alpha$ is projective.

Conversely, assume that $\coprod_\alpha P_\alpha$ is projective. By Proposition 2.20, there is a free module, F, and another (projective) module, $\widetilde{P}$, with

$$\Big(\coprod_\alpha P_\alpha\Big) \coprod \widetilde{P} \cong F.$$

Pick any β, then

$$P_\beta \coprod \left(\Big(\coprod_{\alpha\neq\beta} P_\alpha\Big) \coprod \widetilde{P}\right) \cong F.$$

Again, by Proposition 2.20, the module P_β is projective. □

The product of projectives *need not* be projective. (See, HW Problem V.B.VI.)

Remark: Projective modules can be viewed as a natural generalization of free modules. The following characterization of projective modules in terms of linear forms is an another illustration of this fact. Moreover, this proposition can used to prove that invertible ideals of an integral domain are precisely the projective ideals, a fact that plays an important role in the theory of Dedekind rings (see Chapter 3, Section 3.6).

Proposition 2.23 *An R-module, M, is projective iff there exists a family, $\{e_i\}_{i\in I}$, of elements of M and a family, $\{\varphi_i : M \to R\}_{i\in I}$, of R-linear maps such that*

(i) For all $m \in M$, we have $\varphi_i(m) = 0$, for all but finitely $i \in I$.

(ii) For all $m \in M$, we have $m = \sum_i \varphi_i(m)e_i$.

In particular, M is generated by the family $\{e_i\}_{i\in I}$.

Proof. First, assume that M is projective and let $\psi : F \to M$ be a surjection from a free R-module, F. The map, ψ, splits, we let $\varphi : M \to F$ be its splitting. If $\{f_i\}_{i\in I}$ is a basis of F, we set $e_i = \psi(f_i)$. Now, for each $m \in M$, the element $\varphi(m)$ can be written uniquely as

$$\varphi(m) = \sum_k r_k f_k,$$

where $r_k \in R$ and $r_k = 0$ for all but finitely many k. Define $\varphi_i : M \to R$ by $\varphi_i(m) = r_i$; it is clear that φ_i is R-linear and that (i) holds. For every $m \in M$, we have

$$m = (\psi \circ \varphi)(m) = \psi\Big(\sum_k r_k f_k\Big) = \sum_k \varphi_k(m)e_k,$$

which is (ii). Of course, this also shows the e_k generate M.

Conversely, assume (i) and (ii). Consider the free module $F = \coprod_{i\in I} R$ and let $\{f_i\}_{i\in I}$ be a basis of F. Define the map $\psi\colon F \to M$ *via* $f_i \mapsto e_i$. To prove that M is projective, by Proposition 2.20 (4), it is enough to find a map $\varphi\colon M \to F$ with $\psi \circ \varphi = 1_M$. Define φ *via*

$$\varphi(m) = \sum_k \varphi_k(m) f_k.$$

The sum on the righthand side is well-defined because of (i), and by (ii),

$$(\psi \circ \varphi)(m) = \sum_k \varphi_k(m) e_k = m.$$

Therefore, M is a cofactor of a free module, so it is projective. □

We would like to test submodules, L, of M as to whether $L = M$ by testing *via* surjections $M \longrightarrow N$. That is, suppose we know that for every N and every surjection $M \longrightarrow N$ we have $L \hookrightarrow M \longrightarrow N$ is also surjective. How restrictive can we be with the N's, yet get a viable test?

There may be some superfluous N, e.g., those N for which $M \longrightarrow N \longrightarrow 0$ automatically implies that $L \longrightarrow M \longrightarrow N$ is surjective. There may even be some such N's that work for *all* L. Thus, it is preferable to fix attention on N and seek small enough M so that N matters in the testing of all L. This yields a piece of the following definition:

Definition 2.5 A surjection, $M \longrightarrow N$, is a *minimal* (*essential*, or *covering*) *surjection* iff for all $L \subseteq M$, whenever $L \longrightarrow M \longrightarrow N$ is surjective, we can conclude $L = M$. A submodule, K, is *small* (*superfluous*) iff for every submodule, $L \subseteq M$, when $L + K = M$, then $L = M$. A submodule, K, is *large* (*essential*) iff for all submodules, $L \subseteq M$, when $L \cap K = (0)$, then $L = (0)$. The injection $K \longrightarrow M$ is *essential* (*minimal*) iff K is large.

Proposition 2.24 *The following are equivalent for surjections $\theta\colon M \to N$:*

(1) $M \xrightarrow{\theta} N$ *is a minimal surjection.*

(2) $\operatorname{Ker}\theta$ *is small.*

(3) $\operatorname{Coker}(L \longrightarrow M \longrightarrow N) = (0)$ *implies* $\operatorname{Coker}(L \longrightarrow M) = (0)$*, for any submodule, $L \subseteq M$.*

Proof. (1) ⇒ (2). Pick L, and assume $L + \operatorname{Ker}\theta = M$. So, $\theta(L) = \theta(M) = N$. Thus, $L = M$, by (1), which shows that $\operatorname{Ker}\theta$ is small.

(2) ⇒ (3). Say $L \subseteq M$ and assume that $\operatorname{Coker}(L \longrightarrow M \longrightarrow N) = (0)$. Therefore, $N = \operatorname{Im}(L \longrightarrow N)$, and we deduce that

$$L + \operatorname{Ker}\theta = M,$$

by the second homomorphism theorem. By (2), we get $L = M$; so, $\operatorname{Coker}(L \longrightarrow M) = (0)$.

(3) ⇒ (1). This is just the definition. □

Definition 2.6 A surjection $P \longrightarrow N$ is a *projective cover* iff

(1) The module P is projective

(2) It is a minimal surjection.

Projective covers may not exist. For example, $\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is a surjection and $\mathbb{Z}$ is projective. If $P \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is a projective cover, then the lemma below implies that P is torsion-free. Hence, we can replace $P \longrightarrow \mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$. However, the following argument now shows that $\mathbb{Z}/2\mathbb{Z}$ has no projective cover. We have the surjection $\theta\colon \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$. This is not a minimal surjection because $2\mathbb{Z}$ is not small. (Clearly, Ker $\theta = 2\mathbb{Z}$; so, say $L = d\mathbb{Z}$ and $d\mathbb{Z} + 2\mathbb{Z} = \mathbb{Z}$. Then, $(d, 2) = 1$, so d is odd. Yet, $d\mathbb{Z} = \mathbb{Z}$ only when $d = 1$. Thus, the module $2\mathbb{Z}$ is not small.) Now, suppose $d\mathbb{Z} \xrightarrow{\theta} \mathbb{Z}/2\mathbb{Z}$ is surjective, then d must be odd. If $k\mathbb{Z} \subseteq d\mathbb{Z}$ maps onto $\mathbb{Z}/2\mathbb{Z}$, then, as Ker $\theta = 2d\mathbb{Z}$, we get $(k, 2d) = d$. Let $b = k/d$; the integer b must be odd. Then, the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 2\mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \\ 0 & \longrightarrow & 2d\mathbb{Z} & \longrightarrow & d\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0, \end{array}$$

(in which the vertical arrows are isomorphisms: multiply by d) shows that the inclusion $k\mathbb{Z} \subseteq d\mathbb{Z}$ corresponds to the inclusion $b\mathbb{Z} \subseteq \mathbb{Z}$. Our previous argument implies $b = 1$; so, $k = d$, and $d\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is not minimal.

Lemma 2.25 *If R has no zero divisors and P is a projective R-module then P is torsion-free.*

Proof. Since the torsion-free property is inherited by submodules, we may assume that P is a free module. Moreover, coproducts of torsion-free modules are torsion-free, so we may assume that $P = R$. But, R has no zero-divisors; so, it is torsion-free. □

Proposition 2.26 *Say R is a ring and $\mathcal{J}(R)$ is its Jacobson radical (i.e., $\mathcal{J}(R)$ is equal to the intersection of all maximal ideals of R). Then, the surjection $R \longrightarrow R/\mathcal{J}(R)$ is a projective cover. In particular, when R is commutative local, then $R \longrightarrow R/\mathfrak{m}_R$ is a projective cover.*

Proof. Pick $L \subseteq R$, a submodule of R, i.e., an ideal of R, such that $L + \mathcal{J}(R) = R$. If $L \neq R$, then $L \subseteq \mathfrak{M}$, where $\mathfrak{M}$ is some maximal ideal. But, $\mathcal{J}(R) \subseteq \mathfrak{M}$, and so $L + \mathcal{J}(R) \subseteq \mathfrak{M}$. The latter inclusion shows that $L + \mathcal{J}(R) \neq R$, a contradiction; so, $\mathcal{J}(R)$ is small. □

For injective modules, the situation is nearly dual to the projective case. It is exactly dual as far as categorical properties are concerned. However, the notion of free module is not categorical, and so, results about projective modules involving free modules have no counterpart for injective modules. On the other hand, the situation for injectives is a bit better than for projectives.

Proposition 2.27 *The following are equivalent for a module, Q:*

(1) The module, Q, is injective.

(2) Given a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \downarrow{\scriptstyle \xi} & & \\ & & Q & & \end{array}$$

there exists an extension, $\theta\colon M \to Q$, of ξ, making the diagram commute (extension property).

(3) Every exact sequence $0 \longrightarrow Q \longrightarrow M \longrightarrow M'' \longrightarrow 0$ splits.

Proof. (DX)

Proposition 2.28 *Given a family, $\{Q_\alpha\}_{\alpha\in\Lambda}$, of modules, the product $\prod_\alpha Q_\alpha$ is injective iff each Q_α is injective.*

Proof. (DX)

Theorem 2.29 *(Baer Representation Theorem) An R-module, Q, is injective iff it has the extension property w.r.t. the sequence*

$$0 \longrightarrow \mathfrak{A} \longrightarrow R, \tag{$*$}$$

where $\mathfrak{A}$ is an ideal of R.

Proof. If Q is injective, it is clear that Q has the extension property w.r.t. $(*)$.

Conversely, assume that the extension property holds for $(*)$. What does this mean? We have the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathfrak{A} & \longrightarrow & R \\ & & \varphi \downarrow & \swarrow_{\psi} & \\ & & Q & & \end{array}$$

in which ψ extends φ; so, for all $\xi \in \mathfrak{A}$, we have $\varphi(\xi) = (\psi \restriction \mathfrak{A})(\xi)$. In particular, $\psi(1) \in Q$ exists, say $q = \psi(1)$. Since $\xi \cdot 1 = \xi$ for all $\xi \in \mathfrak{A}$, we have

$$\varphi(\xi) = \psi(\xi) = \xi\psi(1) = \xi q.$$

Given the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \varphi \downarrow & & \\ & & Q & & \end{array}$$

define $\mathcal{S}$ by

$$\mathcal{S} = \left\{ (N, \psi) \;\middle|\; \begin{array}{l} (1)\ N \text{ is a submodule of } M, \quad (2)\ M' \subseteq N, \\ (3)\ \psi\colon N \to Q \text{ extends } \varphi \text{ to } N. \end{array} \right\}$$

Partially order $\mathcal{S}$ by inclusion and agreement of extensions. Then, $\mathcal{S}$ is inductive (DX). By Zorn's lemma, there is a maximal element, (N_0, ψ_0), in $\mathcal{S}$. We claim that $N_0 = M$. If $N_0 \neq M$, there is some $m \in M - N_0$. Let $\mathfrak{A}$ be the transporter of m into N_0, i.e.,

$$(m \longrightarrow N_0) = \{\rho \in R \mid \rho m \in N_0\}.$$

Define the R-module map, $\theta\colon \mathfrak{A} \to Q$, by $\theta(\rho) = \psi_0(\rho m)$. Look at the module $N_0 + Rm$, which strictly contains N_0. If $z \in N_0 + Rm$, then $z = z_0 + \rho m$, for some $z_0 \in N_0$ and some $\rho \in R$. Set

$$\psi(z) = \psi_0(z_0) + \rho q,$$

where $q = \Theta(1)$ and Θ is an extension of θ (guaranteed to exist, by the hypothesis). We must prove that ψ is a well-defined map, i.e., if $z = z_0 + \rho m = \widetilde{z_0} + \widetilde{\rho} m$, then

$$\psi_0(z_0) + \rho q = \psi_0(\widetilde{z_0}) + \widetilde{\rho} q.$$

Now, if $\psi\colon N_0 + Rm \to Q$ is indeed well-defined, then it is an extension of ψ_0 to the new module $N_0 + Rm > N_0$, contradicting the maximality of N_0. Therefore, $N_0 = M$, and we are done.

If $z = z_0 + \rho m = \widetilde{z_0} + \widetilde{\rho} m$, then $z_0 - \widetilde{z_0} = (\widetilde{\rho} - \rho)m$; so $\widetilde{\rho} - \rho \in \mathfrak{A}$. Consequently,

$$\theta(\widetilde{\rho} - \rho) = \psi_0((\widetilde{\rho} - \rho)m).$$

Yet,

$$\theta(\widetilde{\rho} - \rho) = \Theta(\widetilde{\rho} - \rho) = (\widetilde{\rho} - \rho)\Theta(1) = (\widetilde{\rho} - \rho)q,$$

and so, we get

$$\psi_0(z_0 - \widetilde{z_0}) = \psi_0((\widetilde{\rho} - \rho)m) = \theta(\widetilde{\rho} - \rho) = (\widetilde{\rho} - \rho)q.$$

Therefore, we deduce that

$$\psi_0(z_0) + \rho q = \psi_0(\widetilde{z_0}) + \widetilde{\rho} q,$$

establishing that ψ is well-defined. □

Recall that an R-module, M, is *divisible* iff for every $\lambda \in R$ with $\lambda \neq 0$, the map $M \xrightarrow{\lambda} M$ (multiplication by λ), is surjective.

Corollary 2.30 *If $R \in$ CR has no zero-divisors, then an injective R-module is automatically divisible. Moreover, if R is a P.I.D., a necessary and sufficient condition that Q be injective is that Q be divisible. Therefore, over P.I.D.'s, every factor module of an injective is injective.*

Proof. Let $\lambda \in R$, with $\lambda \neq 0$. Since R has no zero divisors, the map $R \xrightarrow{\lambda} R$ is a monomorphism. Thus, the image of this map is an ideal, $\mathfrak{A}$, and the exact sequence

$$0 \longrightarrow \mathfrak{A} \longrightarrow R$$

is just the exact sequence

$$0 \longrightarrow R \xrightarrow{\lambda} R.$$

Apply the cofunctor $\mathrm{Hom}_R(-, Q)$. If Q is injective, this cofunctor is exact, and we get the exact sequence

$$\mathrm{Hom}_R(R, Q) \xrightarrow{\lambda} \mathrm{Hom}_R(R, Q) \longrightarrow 0.$$

So, the sequence $Q \xrightarrow{\lambda} Q \longrightarrow 0$ is exact, which proves that Q is divisible.

If R is a P.I.D., then every ideal is principal, so, every exact sequence $0 \longrightarrow \mathfrak{A} \longrightarrow R$, where $\mathfrak{A}$ is an ideal, is of the form $0 \longrightarrow R \xrightarrow{\lambda} R$, for some $\lambda \in R$. If Q is divisible, the sequence $Q \xrightarrow{\lambda} Q \longrightarrow 0$ is exact, and we get that

$$\mathrm{Hom}_R(R, Q) \xrightarrow{\lambda} \mathrm{Hom}_R(R, Q) \longrightarrow 0 \quad \text{is exact;}$$

this means that $\mathrm{Hom}_R(-, Q)$ is exact on sequences

$$0 \longrightarrow \mathfrak{A} \longrightarrow R \longrightarrow R/\mathfrak{A} \longrightarrow 0,$$

where $\mathfrak{A}$ is an ideal, i.e., the extension property holds for ideals, $\mathfrak{A}$, of R. By applying Baer's theorem we conclude that Q is injective.

The reader will easily verify that factor modules of divisible modules are divisible (DX). Consequently, the last statement of the corollary holds. □

Theorem 2.31 *(Baer Embedding Theorem) Every R-module is a submodule of an injective module.*

Proof. The proof assigned for homework (Problem 57) is based on Eckmann's proof. Here is Godement's proof [18] (probably the shortest proof). The first step is to show that any $\mathbb{Z}$-module, M, can be embedded into M^{DD}, where $M^D = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. Given a $\mathbb{Z}$-module, M, we define a natural $\mathbb{Z}$-linear map, $m \mapsto \widehat{m}$, from M to M^{DD}, in the usual way: For every $m \in M$ and every $f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$,

$$\widehat{m}(f) = f(m).$$

It is clear that such a map is $\mathbb{Z}$-linear.

Proposition 2.32 *For every $\mathbb{Z}$-module, M, the natural map $M \longrightarrow M^{DD}$ is injective.*

Proof. It is enough to show that $m \neq 0$ implies that $\widehat{m} \neq 0$, *i.e.*, there is some $f \in M^D = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ so that $f(m) \neq 0$.

Consider the cyclic subgroup $\mathbb{Z}m$ of M generated by m. If m has finite order $n \geq 1$, then $\mathbb{Z}m \cong \mathbb{Z}/n\mathbb{Z}$. The $\mathbb{Z}$-linear map $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ given by $f(1) = 1/n \pmod{\mathbb{Z}}$ is obviously an injection. Since $0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow M$ is exact and $\mathbb{Q}/\mathbb{Z}$ is injective, the map $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ extends to a $\mathbb{Z}$-linear map $\widehat{f}\colon M \to \mathbb{Q}/\mathbb{Z}$ with $\widehat{f}(m) \neq 0$, as claimed.

If $\mathbb{Z}m$ is infinite (m has infinite order), then we have the $\mathbb{Z}$-linear surjection $g\colon \mathbb{Z}m \to \mathbb{Z}/2\mathbb{Z}$ given by $g(m) = 1 \pmod 2$. We also have the injective $\mathbb{Z}$-linear map $f_2\colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ given by $f_2(1) = 1/2 \pmod{\mathbb{Z}}$, and since $\mathbb{Q}/\mathbb{Z}$ is injective, the $\mathbb{Z}$-linear map $f_2\colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ extends to a $\mathbb{Z}$-linear map $\widehat{f_2}\colon M \to \mathbb{Q}/\mathbb{Z}$, with $\widehat{f_2}(1) \neq 0$. Then the composition $\widehat{f} = \widehat{f_2} \circ g$ is a $\mathbb{Z}$-linear map $\widehat{f}\colon M \to \mathbb{Q}/\mathbb{Z}$ such that $\widehat{f}(m) = \widehat{f_2}(g(m)) = \widehat{f_2}(1) \neq 0$. □

Recall that given a ring R, the ring R^{op} is the ring with the same underlying set R, the same adddition operation $+$, and the multiplication operation $*^{\mathrm{op}}$ given by $\lambda *^{\mathrm{op}} \mu = \mu * \lambda$ for all $\lambda, \mu \in R$. If M is an R-module and N is any $\mathbb{Z}$-module, then we can define a map from $R \times \mathrm{Hom}_{\mathbb{Z}}(M, N)$ to $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ as follows: for all $\alpha \in R$ and all $f \in \mathrm{Hom}_{\mathbb{Z}}(M, N)$,

$$(\alpha f)(m) = f(\alpha m), \quad \text{for all } m \in M. \tag{$*_R$}$$

Since $\alpha *^{\mathrm{op}} \beta = \beta * \alpha$, we have

$$(\alpha(\beta f))(m) = (\beta f)(\alpha m) = f(\beta(\alpha m)) = f((\beta * \alpha)m) = ((\beta * \alpha)f)(m) = ((\alpha *^{\mathrm{op}} \beta)f)(m).$$

The equation

$$(\alpha(\beta f))(m) = f(\beta(\alpha m)) = ((\alpha *^{\mathrm{op}} \beta)f)(m)$$

shows that $(*_R)$ defines a left action of R^{op} on $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ which makes $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ into a R^{op}-module.

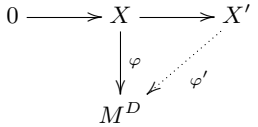
Similarly, if M is an R^{op}-module and N is any $\mathbb{Z}$-module, then $(*_R)$ defines a left action of R on $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ which makes $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ into an R-module, since

$$(\alpha(\beta f))(m) = (\beta f)(\alpha m) = f(\beta(\alpha m)) = f((\beta *^{\mathrm{op}} \alpha)m) = f((\alpha * \beta)m) = ((\alpha * \beta)f)(m).$$

Then $M^D = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is an R^{op}-module if M is an R-module (resp. an R-module if M is an R^{op}-module). Furthermore, the $\mathbb{Z}$-injection, $M \longrightarrow M^{DD}$, is an R-injection. The crux of Godement's proof is the following proposition.

Proposition 2.33 *If M is a projective R^{op}-module, then M^D is an injective R-module.*

Proof. Consider the diagram



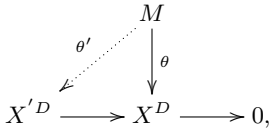
where the row is exact. To prove that M^D is injective, we need to prove that φ extends to a map $\varphi'\colon X' \to M^D$. The map φ yields the map $M^{DD} \longrightarrow X^D$, and since we have an injection $M \longrightarrow M^{DD}$, we get a map $\theta\colon M \to X^D$. Now, since $\mathbb{Q}/\mathbb{Z}$ is injective, $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ maps the exact sequence

$$0 \longrightarrow X \longrightarrow X'$$

to the exact sequence

$$\mathrm{Hom}_{\mathbb{Z}}(X', \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0,$$

i.e., $X'^D \longrightarrow X^D \longrightarrow 0$. So, we have the diagram



where the row is exact, and since M is projective, the map θ lifts to a map $\theta'\colon M \to X'^D$. Consequently, we get a map $X'^{DD} \longrightarrow M^D$, and since we have an injection $X' \longrightarrow X'^{DD}$, we get a map $X' \longrightarrow M^D$ extending φ, as desired. Therefore, M^D is injective. □

We can now prove Theorem 2.31. Consider the R^{op}-module M^D. We know that there is a free R^{op}-module, F, so that

$$F \longrightarrow M^D \longrightarrow 0 \quad \text{is exact.}$$

But, F being free is projective. We get the exact sequence

$$0 \longrightarrow M^{DD} \longrightarrow F^D.$$

By Proposition 2.33, the module F^D is injective. Composing the natural injection $M \longrightarrow M^{DD}$ with the injection $M^{DD} \longrightarrow F^D$, we obtain our injection, $M \longrightarrow F^D$, of M into an injective. □

Corollary 2.34 *Every R-module, M, has an injective resolution*

$$0 \longrightarrow M \longrightarrow Q_0 \longrightarrow Q_1 \longrightarrow Q_2 \longrightarrow \cdots,$$

where the Q_i's are injective and the sequence is exact.

How about minimal injections? Recall that $N \longrightarrow M$ is a minimal (essential) injection iff N is large in M, which means that for any $L \subseteq M$, if $N \cap L = (0)$, then $L = (0)$.

We have the following characterization of essential injections, analogous to the characterization of minimal surjections:

Proposition 2.35 *The following are equivalent for injections $\theta\colon N \to M$:*

(1) $N \xrightarrow{\theta} M$ is essential.

(2) Given any module, Z, and any map, $M \xrightarrow{\varphi} Z$, if $N \longrightarrow M \xrightarrow{\varphi} Z$ is injective, then φ is injective.

(3) $\mathrm{Ker}\,(N \longrightarrow M \longrightarrow Z) = (0)$ *implies* $\mathrm{Ker}\,(M \longrightarrow Z) = (0)$*, for any module, Z.*

Proof. (DX)

In contradistinction to the case of covering surjections, essential injections always exist.

Proposition 2.36 *Given an injection, $N \longrightarrow M$, there exists a submodule, K, of M so that*

(1) The sequence $0 \longrightarrow N \longrightarrow M/K$ is exact, and

(2) It is an essential injection.

Proof. Let

$$\mathcal{S} = \{K \subseteq M \mid K \cap N = (0)\}.$$

Since $(0) \in \mathcal{S}$, the set $\mathcal{S}$ is nonempty. Partially order $\mathcal{S}$ by inclusion. If $\{Z_\alpha\}_\alpha$ is a chain in $\mathcal{S}$, let $Z = \bigcup_\alpha Z_\alpha$, a submodule of M. We have

$$Z \cap N = \left(\bigcup_\alpha Z_\alpha\right) \cap N = \bigcup_\alpha (Z_\alpha \cap N) = (0),$$

since $Z_\alpha \cap N) = (0)$, for all α. Therefore, $\mathcal{S}$ is inductive, and by Zorn's lemma, it has a maximal element, say K. Since $K \cap N = (0)$, property (1) is satisfied. For (2), take $L \subseteq M/K$ so that $L \cap \mathrm{Im}\,(N) = (0)$. We must show that $L = (0)$. By the second homomorphism theorem, L corresponds to $\widetilde{L}$ in M, with $K \subseteq \widetilde{L} \subseteq M$, and we are reduced to proving that $\widetilde{L} = K$.

Claim: For every $\eta \in \widetilde{L}$, if $\eta \notin K$, then $\eta \notin N$.

If $\eta \in \widetilde{L}$ and $\eta \notin K$ and $\eta \in N$, then $\overline{\eta} \in L \cap \mathrm{Im}\,(N)$, and so, $\overline{\eta} = 0$, since $L \cap \mathrm{Im}\,(N) = (0)$. (As usual, $\eta \mapsto \overline{\eta}$, denotes the canonical map $M \longrightarrow M/K$.) Yet $\eta \notin K$, a contradiction; the claim holds.

Assume that $\xi \in \widetilde{L}$ and $\xi \notin K$. Consider $K + R\xi$, a submodule of $\widetilde{L}$ strictly containing K. Since K is a maximal module with $K \cap N = (0)$, there is some $\eta \in (K + R\xi) \cap N$, with $\eta \neq 0$. Consequently, we have $\eta \in \widetilde{L}$ and $\eta \in N$. Now, if $\eta \in K$, then $\eta \in N \cap K = (0)$, contradicting the fact that $\eta \neq 0$; so, we must have $\eta \notin K$. However, this contradicts the claim. Therefore, ξ cannot exist, and $\widetilde{L} = K$. □

Terminology: The module Q is an *injective hull of* M iff

(1) $M \longrightarrow Q$ is an essential injection, and

(2) The module Q is injective.

Theorem 2.37 *(Baer–Eckmann–Schopf) Every R-module has an injective hull.*

Proof. By Baer's embedding theorem (Theorem 2.31), there is an injective module, Q, so that $0 \longrightarrow M \longrightarrow Q$ is exact. Set

$$\mathcal{S} = \{L \mid M \subseteq L \subseteq Q \quad \text{and } 0 \longrightarrow M \longrightarrow L \text{ is essential}\}.$$

Since $M \in \mathcal{S}$, the set $\mathcal{S}$ is nonempty. The set $\mathcal{S}$ is partially ordered by inclusion, and it is inductive (DX). By Zorn's lemma, $\mathcal{S}$ has a maximal element, say L. I claim that L is injective. Look at the exact sequence $0 \longrightarrow L \longrightarrow Q$. By the argument in the previous proposition on essential extensions, there is a maximal $K \subseteq Q$, so that $K \cap L = (0)$ and $0 \longrightarrow L \longrightarrow Q/K$ is essential. Look at the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \longrightarrow & Q/K \\ & & \downarrow{\scriptstyle \varphi} & & \\ & & Q & & \end{array} .$$

Since Q is injective, there is a map, $\psi\colon Q/K \to Q$, extending φ; let $T = \mathrm{Im}\,\psi$. The map ψ is injective, because $\psi \restriction L$ is injective and the row is essential. Thus, $\psi\colon Q/K \to T$ is an isomorphism; moreover, $L \subseteq T$. We contend that $T = L$. To see this, we will prove that $0 \longrightarrow M \longrightarrow T$ is essential. Now, being essential is a transitive property (DX); since T is essential over L (because $Q/K \cong T$ and Q/K is essential over L) and L is essential over M, we see that T is essential over M. But, L is maximal essential over M (in Q) and $L \subseteq T$; so, we conclude that $T = L$. Therefore, $L \cong Q/K$ and we have the maps

$$Q \longrightarrow Q/K \cong L \quad \text{and} \quad L \longrightarrow Q.$$

It follows that the sequence

$$0 \longrightarrow K \longrightarrow Q \longrightarrow L \longrightarrow 0$$

splits. Consequently, L is also injective; so, L is the required injective hull. □

Proposition 2.38 *(Uniqueness of projective covers and injective hulls.) Say $P \longrightarrow M$ is a projective cover and $\widetilde{P} \longrightarrow M$ is another surjection with $\widetilde{P}$ projective. Then, there exist $\widetilde{P}', \widetilde{P}'' \subseteq \widetilde{P}$, both projective so that*

(a) $\widetilde{P} = \widetilde{P}' \amalg \widetilde{P}''$.

(b) $P \cong \widetilde{P}'$.

(c) In the diagram

$$\begin{array}{ccccc} & & \widetilde{P} & & \\ & & \downarrow{\scriptstyle \widetilde{p}} & & \\ P & \xrightarrow{p} & M & \longrightarrow & 0 \\ & & \downarrow & & \\ & & 0 & & \end{array}$$

there are maps $\pi\colon \widetilde{P} \to P$ and $i\colon P \to \widetilde{P}$ in which π is surjective and i is injective, $\widetilde{P}'' = \operatorname{Ker}\pi$, $\widetilde{P}' = \operatorname{Im} i$ and $\widetilde{p} \restriction \widetilde{P}'\colon \widetilde{P}' \to M$ is a projective cover.

If M and $\widetilde{M}$ are isomorphic modules, then every isomorphism, $\theta\colon M \to \widetilde{M}$, extends to an isomorphism of projective covers, $P \longrightarrow \widetilde{P}$. The same statements hold for injective hulls and injections, $M \longrightarrow \widetilde{Q}$, where $\widetilde{Q}$ is injective, mutatis mutandis.

Proof. As $\widetilde{P}$ is projective, there is a map $\pi\colon \widetilde{P} \to P$, making the diagram commute. We claim that the map π is surjective. To see this, observe that $p(\operatorname{Im}\pi) = \operatorname{Im}\widetilde{p} = M$. Hence, $\operatorname{Im}\pi = P$, as P is a covering surjection. As P is projective and π is a surjection, π splits, i.e., there is a map $i\colon P \to \widetilde{P}$ and $\pi \circ i = \mathrm{id}_P$; it easily follows that i is injective. Define $\widetilde{P}'' = \operatorname{Ker}\pi$ and $\widetilde{P}' = \operatorname{Im} i$. We know that $i\colon P \to \widetilde{P}'$ is an isomorphism, and

$$0 \longrightarrow \operatorname{Ker}\pi\ (= \widetilde{P}'') \longrightarrow \widetilde{P} \longrightarrow P\ (\cong \widetilde{P}') \longrightarrow 0 \quad \text{is split exact;}$$

so, we deduce that $\widetilde{P} = \widetilde{P}' \amalg \widetilde{P}''$. The rest is clear.

For injectives, turn the arrows around, replace coproducts by products, etc. (DX). □

2.5 The Five Lemma and the Snake Lemma

Proposition 2.39 *(The five lemma.) Given a commutative diagram with exact rows*

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \downarrow{\scriptstyle \varphi_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5, \end{array}$$

then

(a) If φ_2 and φ_4 are injective and φ_1 is surjective, then φ_3 is injective.

(b) If φ_2 and φ_4 are surjective and φ_5 is injective, then φ_3 is surjective.

(c) If φ_1, φ_2, φ_4 , φ_5 are isomorphisms, then so is φ_3.

Proof. Obviously, (a) and (b) imply (c). Both (a) and (b) are proved by chasing the diagram (DX). □

Proposition 2.40 *(The snake lemma.) Given a commutative diagram with exact rows*

$$\begin{array}{ccccccc} & & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \longrightarrow 0 \\ & & \downarrow{\scriptstyle \delta_1} & & \downarrow{\scriptstyle \delta_2} & & \downarrow{\scriptstyle \delta_3} \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 \end{array} \quad ,$$

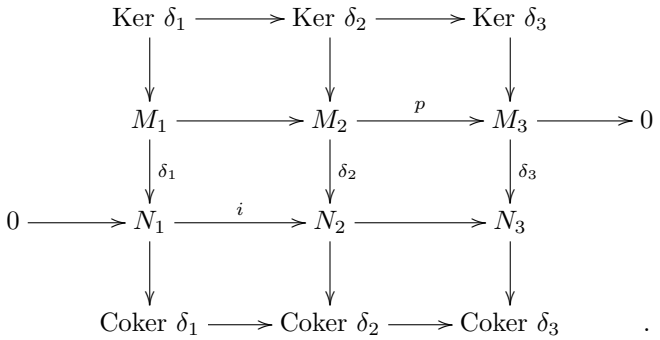
then there exists a six term exact sequence

$$\text{Ker } \delta_1 \longrightarrow \text{Ker } \delta_2 \longrightarrow \text{Ker } \delta_3 \xrightarrow{\delta} \text{Coker } \delta_1 \longrightarrow \text{Coker } \delta_2 \longrightarrow \text{Coker } \delta_3,$$

(where δ is called the connecting homomorphism) and if $M_1 \longrightarrow M_2$ is injective, so is Ker $\delta_1 \longrightarrow$ Ker δ_2, *while if $N_2 \longrightarrow N_3$ is surjective, so is* Coker $\delta_2 \longrightarrow$ Coker δ_3.

Proof. Simple diagram chasing shows Ker $\delta_1 \longrightarrow$ Ker $\delta_2 \longrightarrow$ Ker δ_3 is exact and
Coker $\delta_1 \longrightarrow$ Coker $\delta_2 \longrightarrow$ Coker δ_3 is also exact (DX). Moreover, it also shows the very last assertions of the proposition.

We have to construct the connecting homomorphism, δ. Consider the commutative diagram:



Pick $\xi \in$ Ker δ_3, and consider ξ as an element of M_3. There is some $\eta \in M_2$ so that $p(\eta) = \xi$. So, we have $\delta_2(\eta) \in N_2$, and Im $\delta_2(\eta)$ in N_3 is $\delta_3(\xi) = 0$. As the lower row is exact and i is injective, η gives a unique $x \in N_1$, with $i(x) = \delta_2(\eta)$. We define our $\delta(\xi)$ as the projection of x on Coker δ_1. However, we need to check that this map is well-defined.

If we chose a different element, say $\widetilde{\eta}$, from η, where $p(\eta) = p(\widetilde{\eta}) = \xi$, then the construction is canonical from there on. Take $\delta_2(\eta)$ and $\delta_2(\widetilde{\eta})$. Since $\eta - \widetilde{\eta}$ goes to zero under p, there is some $y \in M_1$, so that $\eta - \widetilde{\eta} =$ Im (y) in M_2. Consequently $\eta = \widetilde{\eta} +$ Im (y); so, $\delta_2(\eta) = \delta_2(\widetilde{\eta}) + \delta_2(\text{Im}\,(y))$. But, $\delta_2(\text{Im}\,(y)) = i(\delta_1(y))$, and so,

$$\delta_2(\eta) = \delta_2(\widetilde{\eta}) + i(\delta_1(y)). \qquad (*)$$

As before, we have some unique elements x and $\widetilde{x}$ in N_1, so that $i(x) = \delta_2(\eta)$ and $i(\widetilde{x}) = \delta_2(\widetilde{\eta})$; so, by $(*)$, we get $i(x) = i(\widetilde{x}) + i(\delta_1(y))$. As i is injective, we conclude that

$$x = \widetilde{x} + \delta_1(y);$$

so, x and $\widetilde{x}$ have equal projections in Coker δ_1, and our definition of $\delta(\xi)$ is independent of the lift, η, of ξ to M_2. The rest is tedious diagram chasing (DX). □

Remark: As we said in Section 2.3, Proposition 2.17 also holds under slightly more general assumptions and its proof is a very nice illustration of the snake lemma. Here it is:

Proposition 2.41 *Let*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

be an exact sequence of Λ-modules. If M is f.g. and M'' is f.p., then, M' is f.g.

Proof. Let

$$F_1 \longrightarrow F_0 \longrightarrow M'' \longrightarrow 0$$

be a finite presentation of M'' (so, F_0, F_1 are free and f.g.) Consider the diagram

$$\begin{array}{ccccccc} & & F_1 & \longrightarrow & F_0 & \longrightarrow & M'' \longrightarrow 0 \\ & & & & & & \| \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0. \end{array}$$

Now, F_0 is free, so there exists a map $F_0 \longrightarrow M$ lifting the surjection $F_0 \longrightarrow M''$. Call this map θ. From the commutative diagram which results when θ is added, we deduce a map $\gamma\colon F_1 \to M'$. Hence, we find the bigger commutative diagram

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ & & F_1 & \longrightarrow & F_0 & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\theta} & & \| & & \\ 0 & \longrightarrow & M' & \xrightarrow[\varphi]{} & M & \xrightarrow[\psi]{} & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \operatorname{Coker}\gamma & \longrightarrow & \operatorname{Coker}\theta & \longrightarrow & 0 & & \end{array}$$

But, by the snake lemma, $\operatorname{Coker}\gamma \cong \operatorname{Coker}\theta$. However, $\operatorname{Coker}\theta$ is f.g. as M is f.g. The image of γ is f.g. as F_1 is f.g. And now, M' is caught between the f.g. modules $\operatorname{Im}\gamma$ and $\operatorname{Coker}\gamma$; so, M' is f.g. $\square$

2.6 Tensor Products and Flat Modules

Let R be a ring (not necessarily commutative). In this section, to simplify the notation, the product of R-modules, M and N, *viewed as sets*, will be denoted $M \times N$, instead of $M \underset{\mathcal{S}\text{ets}}{\prod} N$. For any R^{op}-module, M, any R-module, N, and any abelian group, Z, we set

$$\text{Bi}_R(M,N;Z) = \left\{ \varphi\colon M \times N \longrightarrow Z \;\middle|\; \begin{array}{l} (1)\ (\forall m, m' \in M)(\forall n \in N)(\varphi(m+m',n) = \varphi(m,n) + \varphi(m',n)) \\ (2)\ (\forall m \in M)(\forall n, n' \in N)(\varphi(m,n+n') = \varphi(m,n) + \varphi(m,n')) \\ (3)\ (\forall m \in M)(\forall n \in N)(\forall r \in R)(\varphi(mr,n) = \varphi(m,rn)) \end{array} \right\}.$$

Observe that

(1) The set $\text{Bi}_R(M,N;Z)$ is an abelian group under addition; i.e., if $\varphi, \psi \in \text{Bi}_R(M,N;Z)$, then $\varphi + \psi \in \text{Bi}_R(M,N;Z)$.

(2) The map $Z \rightsquigarrow \text{Bi}_R(M,N;Z)$ is a functor from $\mathcal{A}\text{b}$ to $\mathcal{S}\text{ets}$. Is this functor representable? To be more explicit, does there exist an abelian group, $T(M,N)$, and an element, $\Phi \in \text{Bi}_R(M,N;T(M,N))$, so that the pair $(T(M,N),\Phi)$ represents $\text{Bi}_R(M,N;-)$, i.e., the map

$$\text{Hom}_{\mathbb{Z}}(T(M,N),Z) \xrightarrow{\sim} \text{Bi}_R(M,N;Z)$$

via $\varphi \mapsto \varphi \circ \Phi$, is a functorial isomorphism?

Theorem 2.42 *The functor $Z \rightsquigarrow \text{Bi}_R(M,N;Z)$ from $\mathcal{A}\text{b}$ to $\mathcal{S}\text{ets}$ is representable.*

Proof. Write $\mathcal{F}$ for the free abelian group on the set $M \times N$. Recall that $\mathcal{F}$ consists of formal sums

$$\sum_{\alpha} \xi_\alpha (m_\alpha, n_\alpha),$$

where $\xi_\alpha \in \mathbb{Z}$, with $\xi_\alpha = 0$ for all but finitely many α's, and with $m_\alpha \in M$ and $n_\alpha \in N$. Consider the subgroup, $\mathcal{N}$, of $\mathcal{F}$ generated by the elements

$$\begin{aligned} &(m_1 + m_2, n) - (m_1, n) - (m_2, n) \\ &(m_1, n_1 + n_2) - (m, n_1) - (m, n_2) \\ &(mr, n) - (m, rn). \end{aligned}$$

Form $\mathcal{F}/\mathcal{N}$ and write $m \otimes_R n$ for the image of (m,n) in $\mathcal{F}/\mathcal{N}$. We have

(α) $(m_1 + m_2) \otimes_R n = m_1 \otimes_R n + m_2 \otimes_R n$.

(β) $m \otimes_R (n_1 + n_2) = m \otimes_R n_1 + m \otimes_R n_2$.

(γ) $(mr) \otimes_R n = m \otimes_R (rn)$.

Let $T(M,N) = \mathcal{F}/\mathcal{N}$ and let Φ be given by $\Phi(m,n) = m \otimes_R n$. Then, ($\alpha$), ($\beta$), ($\gamma$) imply that Φ belongs to $\text{Bi}_R(M,N;T(M,N))$, and the assignment, $\varphi \mapsto \varphi \circ \Phi$, gives the functorial map

$$\text{Hom}_{\mathbb{Z}}(T(M,N),Z) \longrightarrow \text{Bi}_R(M,N;Z).$$

We need to prove that this map is an isomorphism. Pick $\theta \in \text{Bi}_R(M,N;Z)$; we claim that θ yields a homomorphism, $T(M,N) \longrightarrow Z$. Such a homomorphism is merely a homomorphism, $\mathcal{F} \longrightarrow Z$, that vanishes on $\mathcal{N}$. But, $\mathcal{F}$ is free; so we just need to know the images of the basis elements, (m,n), in Z. For this, map (m,n) to $\theta(m,n)$. The induced homomorphism vanishes on the generators of $\mathcal{N}$, as θ is bilinear; thus, θ yields a map

$$\Xi(\theta)\colon \mathcal{F}/\mathcal{N} \longrightarrow Z,$$

and we get our inverse map $\text{Bi}_R(M,N;Z) \longrightarrow \text{Hom}_{\mathbb{Z}}(T(M,N),Z)$. Routine checking shows that the maps $\varphi \mapsto \varphi \circ \Phi$ and $\theta \mapsto \Xi(\theta)$ are functorial and mutual inverses. $\square$

Definition 2.7 The group, $T(M,N) = \mathcal{F}/\mathcal{N}$, constructed in Theorem 2.42, is called the *tensor product of* M *and* N *over* R and is denoted $M \otimes_R N$.

Remark: Note that Theorem 2.42 says two things:

(1) For every $\mathbb{Z}$-linear map, $f\colon M \otimes_R N \to Z$, the map, φ, given by $\varphi(m,n) = f(m \otimes n)$, for all $m \in M$ and $n \in N$, is bilinear (i.e., $\varphi \in \mathrm{Bi}_R(M,N;Z)$), and

(2) For every bilinear map, $\varphi \in \mathrm{Bi}_R(M,N;Z)$, there is a *unique* $\mathbb{Z}$-linear map, $f\colon M \otimes_R N \to Z$, with $\varphi(m,n) = f(m \otimes n)$, for all $m \in M$ and $n \in N$. In most situations, this is the property to use in order to define a map from a tensor product to another module.

One should avoid "looking inside" a tensor product, especially when defining maps. Indeed, given some element $w \in M \otimes_R N$, there may be different pairs, $(m,n) \in M \times N$ and $(m',n') \in M \times N$, with $w = m \otimes_R n = m' \otimes_R n'$. Worse, one can have $m \otimes_R n = \sum_\alpha m_\alpha \otimes_R n_\alpha$. Thus, defining a function as $f(m \otimes_R n)$ for all $m \in M$ and $n \in N$ usually does not make sense; there is no guarantee that $f(m \otimes_R n)$ and $f(m' \otimes_R n')$ should agree when $m \otimes_R n = m' \otimes_R n'$. The "right way" to define a function on $M \otimes_R N$ is to first define a function, φ, on $M \times N$, and then to check that φ is bilinear (i.e., $\varphi \in \mathrm{Bi}_R(M,N;Z)$). Then, there is a unique homomorphism, $f\colon M \otimes_R N \to Z$, so that $f(m \otimes_R n) = \varphi(m,n)$. Having shown that f exists, we now may safely use its description in terms of elements, $m \otimes n$, since they generate $M \otimes_R N$. We will have many occasions to use this procedure in what follows.

Basic properties of the tensor product:

Proposition 2.43 *The tensor product, $M \otimes_R N$, is a functor of each variable (from R^{op}-modules to $\mathcal{A}\mathrm{b}$ or from R-modules to $\mathcal{A}\mathrm{b}$). Moreover, as a functor, it is right-exact.*

Proof. Just argue for M, the argument for N being similar. Say $f\colon M \to \widetilde{M}$ is an R^{op}-morphism. Consider $M \times N$ and the map: $\widetilde{f}(m,n) = f(m) \otimes n$. This is clearly a bilinear map $M \times N \longrightarrow \widetilde{M} \otimes_R N$. By the defining property of $M \otimes_R N$, we obtain our map (in $\mathcal{A}\mathrm{b}$) $M \otimes_R N \longrightarrow \widetilde{M} \otimes_R N$. Consequently, **now that we know the map is defined**, we see that it is given by

$$m \otimes n \mapsto f(m) \otimes n.$$

For right-exactness, again vary M (the proof for N being similar). Consider the exact sequence

$$M' \xrightarrow{i} M \longrightarrow M'' \longrightarrow 0. \tag{$\dagger$}$$

We must prove that

$$M' \otimes_R N \longrightarrow M \otimes_R N \longrightarrow M'' \otimes_R N \longrightarrow 0 \quad \text{is exact.} \tag{$\dagger\dagger$}$$

Pick a test abelian group, Z, and write C for $\mathrm{Coker}\,(M' \otimes_R N \longrightarrow M \otimes_R N)$. We have the exact sequence

$$M' \otimes_R N \longrightarrow M \otimes_R N \longrightarrow C \longrightarrow 0. \tag{$*$}$$

Now, $\mathrm{Hom}_{\mathcal{A}\mathrm{b}}(-,Z)$ is left-exact, so we get the exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(C,Z) \longrightarrow \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(M \otimes_R N, Z) \xrightarrow{i^*} \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(M' \otimes_R N, Z). \tag{$**$}$$

The two terms on the righthand side are isomorphic to $\mathrm{Bi}_R(M,N;Z)$ and $\mathrm{Bi}_R(M',N;Z)$, and the map, i^*, is

$$\varphi \in \mathrm{Bi}_R(M,N;Z) \mapsto i^*\varphi \in \mathrm{Bi}_R(M',N;Z), \quad \text{where } i^*\varphi(m',n) = \varphi(i(m'),n).$$

When is $i^*\varphi = 0$? Observe that $i^*\varphi = 0$ iff $\varphi(i(m'), n) = 0$ for all $m' \in M'$ and all $n \in N$. So, $\mathrm{Hom}_{\mathcal{A}\mathrm{b}}(C, Z)$ is the subgroup of $\mathrm{Bi}_R(M, N; Z)$ given by

$$\{\varphi \in \mathrm{Bi}_R(M, N; Z) \mid (\forall m' \in M')(\forall n \in N)(\varphi(i(m'), n) = 0)\},$$

and denoted $\mathrm{Bi}^*_R(M, N; Z)$.

Claim: There is a canonical (functorial in Z) isomorphism

$$\mathrm{Bi}^*_R(M, N; Z) \cong \mathrm{Bi}_R(M'', N; Z).$$

Say $\varphi \in \mathrm{Bi}^*_R(M, N; Z)$. Pick $\overline{m} \in M''$ and $n \in N$, choose any $m \in M$ lifting $\overline{m}$ and set

$$\psi(\overline{m}, n) = \varphi(m, n).$$

If $\widetilde{m}$ is another lift, then, as (†) is exact, $\widetilde{m} - m = i(m')$ for some $m' \in M'$. So, $\varphi(\widetilde{m} - m, n) = 0$, as $\varphi \in \mathrm{Bi}^*_R(M, N; Z)$. But, $\varphi(\widetilde{m} - m, n) = \varphi(\widetilde{m}, n) - \varphi(m, n)$, and so, $\varphi(\widetilde{m}, n) = \varphi(m, n)$, which proves that ψ is well-defined. Consequently, we have the map $\varphi \mapsto \psi$ from $\mathrm{Bi}^*_R(M, N; Z)$ to $\mathrm{Bi}_R(M'', N; Z)$. If $\psi \in \mathrm{Bi}_R(M'', N; Z)$, pick any $m \in M$ and $n \in N$ and set $\varphi(m, n) = \psi(\overline{m}, n)$ (where $\overline{m}$ is the image of m in M''). These are inverse maps. Therefore, we obtain the isomorphism

$$\mathrm{Bi}^*_R(M, N; Z) \cong \mathrm{Bi}_R(M'', N; Z),$$

functorial in Z, as claimed. However, the righthand side is isomorphic to $\mathrm{Hom}_{\mathcal{A}\mathrm{b}}(M'' \otimes_R N, Z)$, and so, by Yoneda's lemma, we see that $C \cong M'' \otimes_R N$, and (††) is exact. □

Proposition 2.44 *Consider R as R^{op}-module. Then, $R \otimes_R M \xrightarrow{\sim} M$. Similarly, if R is considered as R-module, then $M \otimes_R R \xrightarrow{\sim} M$. Say $M = \coprod_{i=1}^{t} M_i$, then*

$$M \otimes_R N \cong \coprod_{i=1}^{t} (M_i \otimes_R N).$$

(Similarly for N.)

Proof. We treat the first case $R \otimes_R M \xrightarrow{\sim} M$, the second one being analogous. Pick a test group, Z, and look at $\mathrm{Hom}_{\mathcal{A}\mathrm{b}}(R \otimes_R M, Z) \cong \mathrm{Bi}_R(R, M; Z)$. Any $\varphi \in \mathrm{Bi}_R(R, M; Z)$ satisfies $\varphi(r, m) = \varphi(1, rm)$, by bilinearity. Now, set $\varphi_0(m) = \varphi(1, m)$. Then, as φ is bilinear, we deduce that $\varphi_0 \colon M \to Z$ is a group homomorphism. The map $\varphi \mapsto \varphi_0$ is clearly an isomorphism from $\mathrm{Bi}_R(R, M; Z)$ to $\mathrm{Hom}_R(M, Z)$, functorial in Z, and so, we obtain an isomorphism

$$\mathrm{Hom}_{\mathcal{A}\mathrm{b}}(R \otimes_R M, Z) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(M, Z)$$

functorial in Z. By Yoneda's lemma, we get the isomorphism $R \otimes_R M \xrightarrow{\sim} M$.

For coproducts, we use an induction on t. The base case, $t = 1$, is trivial. For the induction step, look at the exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow \coprod_{j=2}^{t} M_j \longrightarrow 0.$$

This sequence is not only exact, but split exact. Now, from this, tensoring with N on the right and using the induction hypothesis, we get another split exact sequence (DX)

$$0 \longrightarrow M_1 \otimes_R N \longrightarrow M \otimes_R N \longrightarrow \coprod_{j=2}^{t} (M_j \otimes_R N) \longrightarrow 0;$$

so,

$$M \otimes_R N \cong \coprod_{i=1}^{t} (M_i \otimes_R N). \qquad \square$$

In the next section we will prove that tensor product commutes with arbitrary coproducts.

Computation of some tensor products:

(1) Say $F = \coprod_S R$, as R^{op}-module (with S finite). Then,

$$F \otimes_R N = (\coprod_S R) \otimes_R N \cong \coprod_S (R \otimes_R N) \cong \coprod_S N.$$

Similarly, $M \otimes_R F \cong \coprod_S M$, if $F = \coprod_S R$, as R-module (with S finite).

(1a) Assume G is also free, say $G = \coprod_T R$ (with T finite), as an R-module. Then,

$$F \otimes_R G \cong \coprod_S G = \coprod_S \coprod_T R = \coprod_{S \times T} R.$$

(2) Say $\mathfrak{A}$ is an R^{op}-ideal of R. Then $(R/\mathfrak{A}) \otimes_R M \cong M/\mathfrak{A}M$. Similarly, if $\mathfrak{A}$ is an R-ideal of R, then for any R^{op}-module, M, we have $M \otimes_R (R/\mathfrak{A}) \cong M/M\mathfrak{A}$. (These are basic results.)

Proof. We have the exact sequence

$$0 \longrightarrow \mathfrak{A} \longrightarrow R \longrightarrow R/\mathfrak{A} \longrightarrow 0,$$

where $\mathfrak{A}$ is an R^{op}-ideal. By tensoring on the right with M, we get the right-exact sequence

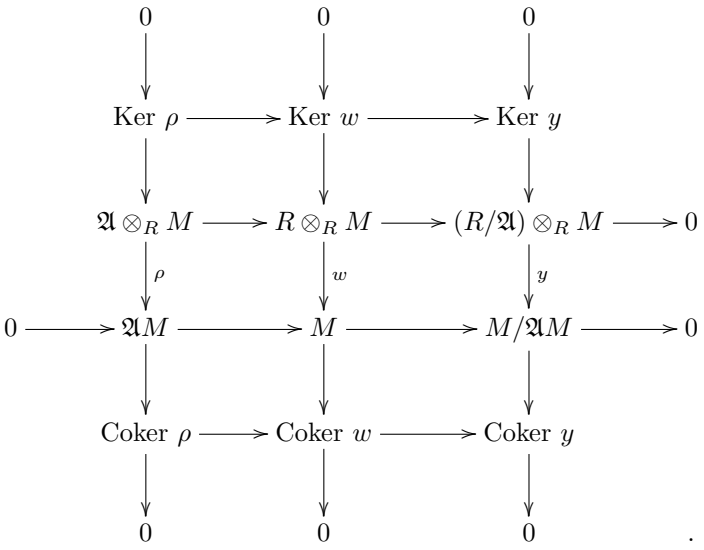
$$\mathfrak{A} \otimes_R M \longrightarrow R \otimes_R M \longrightarrow (R/\mathfrak{A}) \otimes_R M \longrightarrow 0.$$

Consider the diagram:

$$\begin{array}{ccccccccc} & & \mathfrak{A} \otimes_R M & \longrightarrow & R \otimes_R M & \longrightarrow & (R/\mathfrak{A}) \otimes_R M & \longrightarrow & 0 \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & \mathfrak{A}M & \longrightarrow & M & \longrightarrow & M/\mathfrak{A}M & \longrightarrow & 0. \end{array}$$

The middle vertical arrow is an isomorphism; we claim that there is a map $\mathfrak{A} \otimes_R M \longrightarrow \mathfrak{A}M$. Such a map corresponds to a bilinear map in $\mathrm{Bi}_R(\mathfrak{A}, M; \mathfrak{A}M)$. But, $(\alpha, m) \mapsto \alpha m$ is just such a bilinear map. So, we get our map $\mathfrak{A} \otimes_R M \longrightarrow \mathfrak{A}M$. Now, of course, it is given by $\alpha \otimes m \mapsto \alpha m$. But then, there is induced a

righthand vertical arrow and we get the commutative diagram:



The snake lemma yields an exact sequence

$$\text{Ker } w \longrightarrow \text{Ker } y \xrightarrow{\delta} \text{Coker } \rho \longrightarrow \text{Coker } w \longrightarrow \text{Coker } y \longrightarrow 0.$$

Since ρ is onto (DX), we have Coker $\rho = 0$, and since w is an isomorphism, we have Ker $w =$ Coker $w = 0$. Thus, Ker $y = 0$. As Coker $w \longrightarrow$ Coker $y \longrightarrow 0$ is exact and Coker $w = 0$, we deduce that Coker $y = 0$. Therefore, y is an isomorphism, as claimed. $\square$ (One can also use the five lemma in the proof.)

(3) Compute $\mathbb{Z}/r\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/s\mathbb{Z}$.

We claim that the answer is $\mathbb{Z}/t\mathbb{Z}$, where $t = \text{g.c.d.}(r, s)$.

We know (DX) that $\otimes_R$ is an additive functor. From the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{r} \mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z} \longrightarrow 0,$$

we get the exact sequence

$$\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/s\mathbb{Z}) \xrightarrow{r} \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/s\mathbb{Z}) \longrightarrow (\mathbb{Z}/r\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/s\mathbb{Z}) \longrightarrow 0.$$

Write X for $(\mathbb{Z}/r\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/s\mathbb{Z})$. Hence,

$$\mathbb{Z}/s\mathbb{Z} \xrightarrow{r} \mathbb{Z}/s\mathbb{Z} \longrightarrow X \longrightarrow 0 \quad \text{is exact.}$$

Pick $\overline{z} \in \mathbb{Z}/s\mathbb{Z}$, and say $r\overline{z} = 0$, i.e., $rz \equiv 0 \pmod{s}$. We have $r = \rho t$ and $s = \sigma t$, with g.c.d.$(\rho, \sigma) = 1$. Now, $rz \equiv 0 \pmod{s}$ means that $rz = sk$, for some k; so, we have $\rho tz = \sigma tk$, for some k, and so, $\rho z = \sigma k$, for some k. We see that $\sigma \mid \rho z$, and since g.c.d.$(\rho, \sigma) = 1$, we conclude that $\sigma \mid z$. As a consequence, $\sigma t \mid tz$; so, $s\,(= \sigma t) \mid tz$ and we conclude that $t\overline{z} = 0$ in $\mathbb{Z}/s\mathbb{Z}$. Conversely, if $t\overline{z} = 0$, we get $\rho t\overline{z} = 0$, i.e., $r\overline{z} = 0$ in $\mathbb{Z}/s\mathbb{Z}$. Therefore, we have shown that

$$\text{Ker}\,(\text{mult. by } r) = \text{Ker}\,(\text{mult. by } t) \text{ in } \mathbb{Z}/s\mathbb{Z};$$

consequently (as this holds for no further divisor of t)

$$\text{Im}\,(\text{mult. by } r) = \text{Im}\,(\text{mult. by } t) \text{ in } \mathbb{Z}/s\mathbb{Z}.$$

Thus,

$$X \cong (\mathbb{Z}/s\mathbb{Z})/(t\mathbb{Z}/s\mathbb{Z}) \cong \mathbb{Z}/t\mathbb{Z}.$$

(4) Say M is an S-module and an R^{op}-module. If

$$(sm)r = s(mr), \quad \text{for all } s \in S \text{ and all } r \in R,$$

then M is called an (S, R^{op})-*bimodule*, or simply a *bimodule* when reference to S and R are clear. We will always assume that if M is an S-module and an R^{op}-module, then it is a bimodule.

If M is a (S, R^{op})-bimodule and N is an R-module, we claim that $M \otimes_R N$ has a natural structure of S-module.

Illegal procedure: $s(m \otimes_R n) = (sm) \otimes_R n$.

The correct way to proceed is to pick any $s \in S$ and to consider the map, φ_s, from $M \times N$ to $M \otimes_R N$ defined by

$$\varphi_s(m, n) = (sm) \otimes n.$$

It is obvious that this map is bilinear (in m and n).

Remark: (The reader should realize that the bimodule structure of M is used here to check property (3) of bilinearity. We have

$$\varphi_s(mr, n) = (s(mr)) \otimes n = ((sm)r \otimes n = (sm) \otimes rn = \varphi_s(m, rn).)$$

So, we get a map $M \otimes_R N \longrightarrow M \otimes_R N$, corresponding to s. Check that this gives the (left) action of S on $M \otimes_R N$. Of course, it is

$$s(m \otimes_R n) = (sm) \otimes_R n.$$

Similarly, if M is an R^{op}-module and N is a (R, S^{op})-bimodule, then $M \otimes_R N$ is an S^{op}-module; the (right) action of S is

$$(m \otimes_R n)s = m \otimes_R (ns).$$

Remark: If M is an R-module, N is an (R, S^{op})-bimodule, and Z is an S^{op}-module, then any S^{op}-linear map $f\colon M \otimes_R N \longrightarrow Z$ satisfies the property:

$$f(m \otimes_R (ns)) = f(m \otimes_R n)s, \quad \text{for all } s \in S,$$

since $f(m \otimes_R (ns)) = f((m \otimes_R n)s) = f(m \otimes_R n)s$. Thus, the corresponding bilinear map $\varphi\colon M \times N \longrightarrow Z$ defined by

$$\varphi(m, n) = f(m \otimes_R n)$$

satisfies the property:

$$\varphi(m, ns) = \varphi(m, n)s, \quad \text{for all } s \in S.$$

This suggests defining a set, $S^{\mathrm{op}}\text{-Bi}_R(M, N; Z)$, by

$$S^{\mathrm{op}}\text{-Bi}_R(M, N; Z) = \left\{ \varphi\colon M \times N \longrightarrow Z \;\middle|\; \begin{array}{l} (1)\ (\forall m, m' \in M)(\forall n \in N) \\ \quad (\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)) \\ (2)\ (\forall m \in M)(\forall n, n' \in N) \\ \quad (\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')) \\ (3)\ (\forall m \in M)(\forall n \in N)(\forall r \in R)(\varphi(mr, n) = \varphi(m, rn)) \\ (4)\ (\forall m \in M)(\forall n \in N)(\forall s \in S)(\varphi(m, ns) = \varphi(m, n)s) \end{array} \right\}.$$

Then, we have

Theorem 2.45 *Let M be an R-module and N be an (R, S^{op})-bimodule. The functor $Z \rightsquigarrow S^{\mathrm{op}}\text{-Bi}_R(M, N; Z)$ from $\mathcal{M}\mathrm{od}(S^{\mathrm{op}})$ to $\mathcal{S}\mathrm{ets}$ is representable by $(M \otimes_R N, \Phi)$, where Φ is given by $\Phi(m, n) = m \otimes_R n$.*

Note that the above statement includes the fact that $M \otimes_R N$ is an S^{op}-module.

Similarly, if M is an (S, R^{op})-bimodule, N is an R-module and Z is an S-module, then we can define the set, $S\text{-Bi}_R(M, N; Z)$, in an analogous way (replace (4) by $\varphi(sm, n) = s\varphi(m, n)$), and we find

Theorem 2.46 *Let M be an (S, R^{op})-bimodule and N be an R-module. The functor $Z \rightsquigarrow S\text{-Bi}_R(M, N; Z)$ from $\mathcal{M}\mathrm{od}(S)$ to $\mathcal{S}\mathrm{ets}$ is representable by $(M \otimes_R N, \Phi)$, where Φ is given by $\Phi(m, n) = m \otimes_R n$.*

Associativity of tensor: Let M be an R^{op}-module, N an (R, S^{op})-bimodule, and Z an S-module. Then,

$$(M \otimes_R N) \otimes_S Z \cong M \otimes_R (N \otimes_S Z).$$

For any test group, T, the left hand side represents the functor

$$T \rightsquigarrow \mathrm{Bi}_S(M \otimes_R N, Z; T)$$

and the righthand side represents the functor

$$T \rightsquigarrow \mathrm{Bi}_R(M, N \otimes_S Z; T).$$

We easily check that both these are just the trilinear maps, "$\mathrm{Tri}_{R,S}(M, N, Z; T)$;" so, by the uniqueness of objects representing functors, we get our isomorphism. In particular,

(A) $(M \otimes_R S) \otimes_S Z \cong M \otimes_R (S \otimes_S Z) \cong M \otimes_R Z$.

(B) Say $S \longrightarrow R$ is a given *surjective* ring map and say M is an R^{op}-module and N is an R-module. Then, M is an S^{op}-module, N is an S-module and

$$M \otimes_S N \cong M \otimes_R N.$$

To see this, look at $\mathcal{F}/\mathcal{N}$ and see that the same elements are identified.

(C) Say $S \longrightarrow R$ is a ring map. Then, $M \otimes_R N$ is a homomorphic image of $M \otimes_S N$.

Remark: *Adjointness Properties of tensor*: We observed that when M is an (S, R^{op})-bimodule and N is an R-module, then $M \otimes_R N$ is an S-module (resp. when M is an R^{op}-module and N is an (R, S^{op})-bimodule, then $M \otimes_R N$ is an S^{op}-module.) The abelian group $\mathrm{Hom}(M, N)$ also acquires various module structures depending on the bimodule structures of M and N. There are four possible module structures:

(a) The module M is an (R, S^{op})-bimodule and N is an R-module. Define an S-action on $\mathrm{Hom}_R(M, N)$ as follows: For every $f \in \mathrm{Hom}_R(M, N)$ and every $s \in S$,

$$(sf)(m) = f(ms), \quad \text{for all } m \in M.$$

(b) The module M is an (R, S^{op})-bimodule and N is an S^{op}-module. Define an R^{op}-action on $\mathrm{Hom}_{S^{\mathrm{op}}}(M, N)$ as follows: For every $f \in \mathrm{Hom}_{S^{\mathrm{op}}}(M, N)$ and every $r \in R$,

$$(fr)(m) = f(rm), \quad \text{for all } m \in M.$$

(c) The module M is an R^{op}-module and N is an (S, R^{op})-bimodule. Define an S-action on $\mathrm{Hom}_{R^{\mathrm{op}}}(M, N)$ as follows: For every $f \in \mathrm{Hom}_{R^{\mathrm{op}}}(M, N)$ and every $s \in S$,

$$(sf)(m) = s(f(m)), \quad \text{for all } m \in M.$$

(d) The module M is an S-module and N is an (S, R^{op})-bimodule. Define an R^{op}-action on $\mathrm{Hom}_S(M, N)$ as follows: For every $f \in \mathrm{Hom}_S(M, N)$ and every $r \in R$,

$$(fr)(m) = (f(m))r, \quad \text{for all } m \in M.$$

The reader should check that the actions defined in (a), (b), (c), (d) actually give corresponding module structures. Note how the contravariance in the left argument, M, of $\mathrm{Hom}(M,N)$ flips a left action into a right action, and conversely. As an example, let us check (a). For all $r,t \in S$,

$$((st)f)(m) = f(m(st)) = f((ms)t) = (tf)(ms) = (s(tf))(m).$$

We also need to check that sf is R-linear. This is where we use the bimodule structure of M. We have

$$(sf)(rm) = f((rm)s) = f(r(ms)) = rf(ms) = r((sf)(m)).$$

We are now ready to state an important adjointness relationship between Hom and $\otimes$.

Proposition 2.47 *If M is an R^{op}-module, N is an (R, S^{op})-bimodule, and Z is an S^{op}-module, then there is a natural functorial isomorphism*

$$\mathrm{Hom}_{S^{\mathrm{op}}}(M \otimes_R N, Z) \cong \mathrm{Hom}_{R^{\mathrm{op}}}(M, \mathrm{Hom}_{S^{\mathrm{op}}}(N, Z)).$$

When M is an R-module, N is an (S, R^{op})-bimodule, and Z is an S-module, then there is a natural functorial isomorphism

$$\mathrm{Hom}_S(N \otimes_R M, Z) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, Z)).$$

Proof. Using Theorem 2.45, it is enough to prove that

$$S^{\mathrm{op}}\text{-}\mathrm{Bi}_R(M, N; Z) \cong \mathrm{Hom}_{R^{\mathrm{op}}}(M, \mathrm{Hom}_{S^{\mathrm{op}}}(N, Z))$$

and using Theorem 2.46, to prove that

$$S\text{-}\mathrm{Bi}_R(N, M; Z) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, Z)).$$

We leave this as a (DX). □

Proposition 2.47 states that the functor $- \otimes_R N$ is left adjoint to the functor $\mathrm{Hom}_{S^{\mathrm{op}}}(N, -)$ when N is an (R, S^{op})-bimodule (resp. $N \otimes_R -$ is left adjoint to $\mathrm{Hom}_S(N, -)$ when N is an (S, R^{op})-bimodule).

Commutativity of tensor: If R is commutative, then $M \otimes_R N \cong N \otimes_R M$. The easy proof is just to consider $(m, n) \mapsto n \otimes m$. It is bilinear; so, we get a map $M \otimes_R N \longrightarrow N \otimes_R M$. Interchange M and N, then check the maps are mutually inverse.

(5) Let G be a torsion abelian group and Q a divisible abelian group. Then,

$$Q \otimes_{\mathbb{Z}} G = (0).$$

Look at $\mathrm{Hom}_{\mathbb{Z}}(Q \otimes_{\mathbb{Z}} G, T) \cong \mathrm{Bi}_{\mathbb{Z}}(Q, G; T)$, for any test group, T. Take $\varphi \in \mathrm{Bi}_{\mathbb{Z}}(Q, G; T)$ and look at $\varphi(q, \sigma)$. Since G is torsion, there is some n so that $n\sigma = 0$. But, Q is divisible, so $q = n\widetilde{q}$, for some $\widetilde{q} \in Q$. Thus,

$$\varphi(q, \sigma) = \varphi(n\widetilde{q}, \sigma) = \varphi(\widetilde{q}n, \sigma) = \varphi(\widetilde{q}, n\sigma) = 0.$$

As this holds for all q and σ, we have $\varphi \equiv 0$, and so, $Q \otimes_{\mathbb{Z}} G = (0)$.

(6) Free modules (again). Let $F = \coprod_S R$, an R^{op}-module and $G = \coprod_T R$, an R-module (with both S and T finite). We know that

$$F \otimes_R G = \coprod_{S \times T} R.$$

We want to look at this tensor product more closely. Pick a basis, $e_1, \ldots, e_s$, in F and a basis, $f_1, \ldots, f_t$, in G, so that

$$F = \coprod_{j=1}^{s} e_j R \quad \text{and} \quad G = \coprod_{l=1}^{t} R f_l.$$

Then, we get

$$F \otimes_R G = \coprod_{j=1,l=1}^{s,t} (e_j R) \otimes_R (R f_l).$$

Thus, we get copies of R indexed by elements $e_j \otimes f_l$. Suppose that F is also an R-module. This means that $\rho e_j \in F$ makes sense. We assume $\rho e_j \in e_j R$, that is the left action of R commutes with the coproduct decomposition. Then $F \otimes_R G$ is an R-module and it is free of rank st if the left action, ρe_j, has obvious properties (and similarly if G is also an R^{op}-module).

It is not true in general that $\rho e_j = e_j \rho$. Call a free module a *good free module* iff it possesses a basis $e_1, \ldots, e_s$ so that $\rho e_j = e_j \rho$, for all $\rho \in R$. (This is not standard terminology.)

It is not generally true even here, that

$$\rho m = m \rho \quad (m \in F).$$

Say $m = \sum_{j=1}^{s} e_j \lambda_j$. Then, we have

$$\rho m = \sum_{j=1}^{s} \rho(e_j \lambda_j) = \sum_{j=1}^{s} \rho(\lambda_j e_j) = \sum_{j=1}^{s} (\rho \lambda_j) e_j,$$

and

$$m \rho = \sum_{j=1}^{s} (e_j \lambda_j) \rho = \sum_{j=1}^{s} e_j (\lambda_j \rho) = \sum_{j=1}^{s} (\lambda_j \rho) e_j.$$

In general, $\rho \lambda_j \neq \lambda_j \rho$, and so, $\rho m \neq m \rho$.

Consider the special example in which $R = k =$ a field. Then, all modules are free and good. Let V be a k-vector space of dimension d, and let $e_1, \ldots, e_d$ be some basis for V. We know that the dual space, V^D, has the dual basis, $f_1, \ldots, f_d$, characterized by

$$f_i(e_j) = \delta_{ij}.$$

Every $v \in V$ can be uniquely written as $v = \sum \lambda_i e_i$, and every $f \in V^D$ can be uniquely written as $f = \sum \mu_i f_i$. Consider the space

$$\underbrace{V \otimes_k \cdots \otimes_k V}_{a} \otimes_k \underbrace{V^D \otimes_k \cdots \otimes_k V^D}_{b}.$$

Elements of this space, called (a,b)-*tensors*, have the unique form

$$\sum_{j_1,\ldots,j_b}^{i_1,\ldots,i_a} c^{i_1,\ldots,i_a}_{j_1,\ldots,j_b} e_{i_1} \otimes_k \cdots \otimes_k e_{i_a} \otimes_k f_{j_1} \otimes_k \cdots \otimes_k f_{j_b}.$$

So, $V \otimes_k \cdots \otimes_k V \otimes_k V^D \otimes_k \cdots \otimes_k V^D$ may be identified with tuples $(c^{i_1,\ldots,i_a}_{j_1,\ldots,j_b})$, of elements of k, doubly-multiply indexed. They transform as ... (change of basis). A tensor in $V \otimes_k \cdots \otimes_k V \otimes_k V^D \otimes_k \cdots \otimes_k V^D$ is *cogredient of rank (or degree) a and contragredient of rank (or degree) b*. A *tensor field* on a space, X, is a function (of some class, C^∞, C^k, holomorphic, etc.) from X to a tensor vector space, as above. More generally, it is a section of a tensor bundle over X. Also, we can apply f_{j_m} to e_{i_k} and reduce the cogredient and contragredient ranks by one each. This gives a map $V^{\otimes a} \otimes_R V^{D \otimes b} \longrightarrow V^{\otimes (a-1)} \otimes_R V^{D \otimes (b-1)}$, called *contraction*.

Remark: Let M be an R-module, N be an S-module, and Z be an (R, S^{op})-bimodule. Then, we know that $\mathrm{Hom}_R(M, Z)$ is an S^{op}-module and that $Z \otimes_S N$ is an R-module. We can define a canonical homomorphism of $\mathbb{Z}$-modules,

$$\theta\colon \mathrm{Hom}_R(M, Z) \otimes_S N \longrightarrow \mathrm{Hom}_R(M, Z \otimes_S N).$$

For this, for every $n \in N$ and $u \in \mathrm{Hom}_R(M, Z)$, consider the map from M to $Z \otimes_S N$ given by

$$\theta'(u, n)\colon\ m \mapsto u(m) \otimes n.$$

The reader will check (DX) that $\theta'(u, n)$ is R-linear and that $\theta' \in \mathrm{Bi}_S(\mathrm{Hom}_R(M, Z), N; \mathrm{Hom}_R(M, Z \otimes_S N))$. Therefore, we get the desired homomorphism, θ, such that $\theta(u \otimes n)$ is the R-linear map $\theta'(u, n)$. The following proposition holds:

Proposition 2.48

(i) If N is a projective S-module (resp. a f.g. projective S-module), then the $\mathbb{Z}$-homomorphism, $\theta\colon \mathrm{Hom}_R(M, Z) \otimes_S N \longrightarrow \mathrm{Hom}_R(M, Z \otimes_S N)$, is injective (resp. bijective).

(ii) If M is a f.g. projective R-module, then the $\mathbb{Z}$-homomorphism, θ, is bijective.

Proof. In both cases, the proof reduces to the case where M (resp. N) is a free module, and it proceeds by induction on the number of basis vectors in the case where the free module is f.g. (DX). □

The following special case is of special interest: $R = S$ and $Z = R$. In this case, $\mathrm{Hom}_R(M, R) = M^D$, the dual of M, and the $\mathbb{Z}$-homomorphism, θ, becomes

$$\theta\colon M^D \otimes_R N \longrightarrow \mathrm{Hom}_R(M, N),$$

where $\theta(u \otimes n)$ is the R-linear map, $m \mapsto u(m)n$.

Corollary 2.49 *Assume that M and N are R-modules.*

(i) If N is a projective R-module (resp. a f.g. projective R-module), then the $\mathbb{Z}$-homomorphism, $\theta\colon M^D \otimes_R N \longrightarrow \mathrm{Hom}_R(M, N)$, is injective (resp. bijective).

(ii) If M is a f.g. projective R-module, then the $\mathbb{Z}$-homomorphism, θ, is bijective.

If the R-module, N, is also an S^{op}-module, then θ is S^{op}-linear. Similarly, if the R-module, M, is also an S^{op}-module, then θ is S-linear. Furthermore, if M is an R^{op}-module (and N is an R-module), then we obtain a canonical $\mathbb{Z}$-homomorphism,

$$\theta\colon M^{DD} \otimes_R N \longrightarrow \mathrm{Hom}_R(M^D, N).$$

Using the canonical homomorphism, $M \longrightarrow M^{DD}$, we get a canonical homomorphism

$$\theta'\colon M \otimes_R N \longrightarrow \mathrm{Hom}_R(M^D, N).$$

Again, if M is a f.g. projective R^{op}-module, then the map θ' is bijective (DX).

Some (very) important algebras:

Suppose that M is both an R and an R^{op}-module, and that $R \in \mathrm{RNG}$. We also assume, as usual, that M is a bimodule, i.e., $(\rho m)\sigma = \rho(m\sigma)$. Then, $M \otimes_R M$ is again a bimodule, so we can form $M \otimes_R M \otimes_R M$, etc. Define $\mathcal{T}_j(M)$ (also denoted $M^{\otimes j}$) by $\mathcal{T}_0(M) = R$, $\mathcal{T}_1(M) = M$, and

$$\mathcal{T}_j(M) = \underbrace{M \otimes_R \cdots \otimes_R M}_{j}, \quad \text{if } j \geq 2.$$

Then, form

$$\mathcal{T}(M) = \coprod_{j \geq 0} \mathcal{T}_j(M) = \coprod_{j \geq 0} M^{\otimes j}.$$

We can make $\mathcal{T}(M)$ into a ring, by concatenation. Define the map $M^r \times M^s \longrightarrow \mathcal{T}_{r+s}(M)$, by

$$\langle (m_1, \ldots, m_r), (n_1, \ldots, n_s) \rangle \mapsto m_1 \otimes \cdots \otimes m_r \otimes n_1 \otimes \cdots \otimes n_s.$$

This map is bilinear in the pair $\langle(\text{r}-\text{tuple}),(\text{s}-\text{tuple})\rangle$ and so, it is multilinear in all the variables. Thus, we get a map $\mathcal{T}_r(M)\otimes_R \mathcal{T}_s(M)\longrightarrow \mathcal{T}_{r+s}(M)$. Therefore, $\mathcal{T}(M)$ is an R, R^{op}-algebra called the *tensor algebra of* M.

If Z is an R-algebra, denote by (Z) the object Z considered just as an R-module (i.e., $Z\rightsquigarrow(Z)$ is the partial stripping functor from R-alg to $\mathcal{M}\text{od}(R)$.)

Proposition 2.50 *There is a natural, functorial isomorphism*

$$\text{Hom}_{R\text{-alg}}(\mathcal{T}(M),Z)\cong \text{Hom}_{\mathcal{M}\text{od}(R)}(M,(Z)),$$

for every R-algebra, Z. That is, the functor $M\rightsquigarrow\mathcal{T}(M)$ is the left-adjoint of $Z\rightsquigarrow(Z)$.

Proof. Given $\varphi\in\text{Hom}_{R\text{-alg}}(\mathcal{T}(M),Z)$, look at $\varphi\restriction\mathcal{T}_1(M)=\varphi\restriction M$. Observe that $\varphi\restriction M\in\text{Hom}_{\mathcal{M}\text{od}(R)}(M,(Z))$, and clearly, as M generates $\mathcal{T}(M)$, the map φ is determined by $\varphi\restriction M$. We get a functorial and injective map $\text{Hom}_{R\text{-alg}}(\mathcal{T}(M),Z)\longrightarrow\text{Hom}_{\mathcal{M}\text{od}(R)}(M,(Z))$. Say $\psi\colon M\to(Z)$, pick $(m_1,\ldots,m_d)\in M^d$ and form

$$\widetilde{\psi}(m_1,\ldots,m_d)=\psi(m_1)\cdots\psi(m_d).$$

This map is R-multilinear in the m_j's and has values in Z; it gives a map

$$\Xi_d(\psi)\colon \underbrace{M\otimes_R\cdots\otimes_R M}_{d}\longrightarrow Z,$$

and so, we get a map $\Xi(\psi)\colon\mathcal{T}(M)\longrightarrow Z$. It is easy to check that $\varphi\mapsto\varphi\restriction M$ and $\psi\mapsto\Xi(\psi)$ are inverse functorial maps. □

In $\mathcal{T}(M)$, look at the two-sided ideal generated by elements

$$(m\otimes_R n)-(n\otimes_R m),$$

call it $\mathfrak{I}$. Now, $\mathcal{T}$ is a *graded ring*, i.e., it is a coproduct, $\coprod_{j\geq 0}\mathcal{T}_j(M)$, of R-modules and multiplication obeys:

$$\mathcal{T}_j(M)\otimes_R\mathcal{T}_l(M)\subseteq\mathcal{T}_{j+l}(M).$$

The ideal, $\mathfrak{I}$, is a *homogeneous ideal*, which means that

$$\mathfrak{I}=\coprod_{j\geq 0}\mathfrak{I}\cap\mathcal{T}_j(M).$$

To see this, we will in fact prove more:

Proposition 2.51 *Suppose $R=\coprod_{n\geq 0}R_n$ is a graded ring and $\mathfrak{I}$ is a two-sided ideal generated by homogeneous elements $\{r_\alpha\}_{\alpha\in\Lambda}$ (i.e., $r_\alpha\in R_{d_\alpha}$, for some d_α). Then, $\mathfrak{I}$ is a homogeneous ideal. Moreover, the ring, $R/\mathfrak{I}$, is again graded and $R\longrightarrow R/\mathfrak{I}$ preserves degrees.*

Proof. Pick $\xi\in\mathfrak{I}$, then $\xi=\sum_\alpha\rho_\alpha r_\alpha$ and each ρ_α is of the form

$$\rho_\alpha=\sum_{n=0}^{\infty}\rho_{\alpha,n},\quad\text{where }\rho_{\alpha,n}\in R_n,$$

all the sums involved being, of course, finite. So, we have

$$\xi=\sum_\alpha\sum_{n=0}^{\infty}\rho_{\alpha,n}r_\alpha;$$

moreover, $\rho_{\alpha,n} r_\alpha \in R_{n+d_\alpha}$ and $\rho_{\alpha,n} r_\alpha \in \mathfrak{I}$. As $\mathfrak{I}$ is a 2-sided ideal, the same argument works for $\xi = \sum_\alpha r_\alpha \rho_\alpha$. It follows that

$$\mathfrak{I} = \coprod_{n \geq 0} \mathfrak{I} \cap R_n,$$

and $\mathfrak{I}$ is homogeneous.

Write $\overline{R}$ for $R/\mathfrak{I}$, and let $\overline{R}_n$ be the image of R_n under the homomorphism $\rho \mapsto \overline{\rho}$. Then,

$$\overline{R} = \Big(\coprod_n R_n\Big) / \Big(\coprod_n \mathfrak{I} \cap R_n\Big) \cong \coprod R_n/(\mathfrak{I} \cap R_n).$$

But, $\overline{R}_n = R_n/(\mathfrak{I} \cap R_n)$, so we are done. □

In $\mathcal{T}(M)$, which is graded by the $\mathcal{T}_n(M)$, we have the two 2-sided ideals: $\mathfrak{I}$, the 2-sided ideal generated by the homogeneous elements (of degree 2)

$$m \otimes n - n \otimes m,$$

and $\mathcal{K}$, the 2-sided ideal generated by the homogeneous elements

$$m \otimes m \quad \text{and} \quad m \otimes n + n \otimes m.$$

Both $\mathfrak{I}$ and $\mathcal{K}$ are homogeneous ideals, and by the proposition, $\mathcal{T}(M)/\mathfrak{I}$ and $\mathcal{T}(M)/\mathcal{K}$ are graded rings.

Remark: For $\mathcal{K}$, look at

$$(m+n) \otimes (m+n) = m \otimes m + n \otimes n + m \otimes n + n \otimes m.$$

We deduce that if $m \otimes m \in \mathcal{K}$ for all m, then $m \otimes n + n \otimes m \in \mathcal{K}$ for all m and n. The converse is true if 2 is invertible.

We define $\mathrm{Sym}(M)$, the *symmetric algebra of* M to be $\mathcal{T}/\mathfrak{I}$ and set $m \cdot n =$ image of $m \otimes n$ in $\mathrm{Sym}(M)$. The module $\mathrm{Sym}_j(M)$ is called the *j-th symmetric power of* M. Similarly, $\bigwedge(M) = \mathcal{T}/\mathcal{K}$ is the *exterior algebra of* M, and we set $m \wedge n =$ image of $m \otimes n$ in $\bigwedge(M)$. The module $\bigwedge^j(M)$ is called the *j-th exterior power of* M.

Observe that $m \cdot n = n \cdot m$ in $\mathrm{Sym}(M)$ and $m \wedge n = -n \wedge m$ in $\bigwedge(M)$, for all $m, n \in M$. Of course, $m \wedge m = 0$, for all $m \in M$. Further, $\mathrm{Sym}(M)$ is a commutative ring. However, we can have $\omega \wedge \omega \neq 0$ in $\bigwedge M$; for this, see the remark before Definition 2.8.

The algebras $\mathrm{Sym}(M)$ and $\bigwedge(M)$ are $\mathbb{Z}$-algebras only, even if M is an R-bimodule, unless R is commutative, and then they are R-algebras.

Why?

We know that $r(m \otimes n) = (rm \otimes n)$ in $\mathcal{T}(M)$. But in $\mathrm{Sym}(M)$, we would have (writing $=$ for equivalence mod $\mathfrak{I}$)

$$\begin{aligned} r(m \otimes n) &= (rm) \otimes n \\ &= n \otimes (rm) \\ &= (nr) \otimes m \\ &= m \otimes (nr) \\ &= (m \otimes n) r. \end{aligned}$$

Then, for any $r, s \in R$, we would have

$$\begin{aligned}(rs)(m \otimes n) &= r(s(m \otimes n)) \\ &= r((m \otimes n)s) \\ &= r(m \otimes (ns)) \\ &= (m \otimes (ns))r \\ &= (m \otimes n)(sr).\end{aligned}$$

But, $(sr)(m \otimes n) = (m \otimes n)(sr)$, and so, we would get

$$(rs)(m \otimes n) = (sr)(m \otimes n), \quad \text{for all } r, s \in R.$$

So, if we insist that $\mathrm{Sym}(M)$ and $\bigwedge(M)$ be R-algebras, then R must act as if it were commutative, i.e., the 2-sided ideal, $\mathfrak{M}$, generated by the elements $rs - sr\ (= [r, s])$ annihilates both our algebras. Yet $R/\mathfrak{M}$ might be the 0-ring. However, in the commutative case, no problem arises.

Proposition 2.52 *Suppose M is an R-bimodule and as R-module it is finitely generated by $e_1, \ldots, e_r$. Then, $\bigwedge^s M = (0)$ if $s > r$.*

Proof. Note that for any $\rho \in M$ and any e_j, we have $e_j\rho \in M$, and so,

$$e_j\rho = \sum_i \lambda_i e_i, \quad \text{for some } \lambda_i\text{'s},$$

in other words, $e_j\rho$ is some linear combination of the e_i's. Elements of $\bigwedge^2 M$ are sums

$$\begin{aligned}\sum_{\beta,\gamma} m_\beta \wedge m_\gamma &= \sum_{\beta,\gamma} \Big(\sum_i \lambda_i^{(\beta)} e_i\Big) \wedge \Big(\sum_j \mu_j^{(\gamma)} e_j\Big) \\ &= \sum_{\beta,\gamma}\sum_{i,j} \lambda_i^{(\beta)}(e_i \wedge \mu_j^{(\gamma)} e_j) \\ &= \sum_{\beta,\gamma}\sum_{i,j} \lambda_i^{(\beta)}(e_i\mu_j^{(\gamma)} \wedge e_j) \\ &= \sum_{l,m} \rho_{lm}(e_l \wedge e_m),\end{aligned}$$

for some ρ_{lm}. An obvious induction shows that $\bigwedge^s M$ is generated by elements of the form $e_{i_1} \wedge \cdots \wedge e_{i_s}$. There are only r distinct e_i's and there are s of the e_i's in our wedge generators; thus, some e_i occurs twice, that is, we have

$$e_{i_1} \wedge \cdots \wedge e_{i_s} = e_{i_1} \wedge \cdots \wedge e_i \wedge \cdots \wedge e_i \wedge \cdots \wedge e_{i_s}.$$

However, we can repeatedly permute the second occurrence of e_i with the term on its left (switching sign each time), until we get two consecutive occurrences of e_i:

$$e_{i_1} \wedge \cdots \wedge e_{i_s} = \pm e_{i_1} \wedge \cdots \wedge e_i \wedge e_i \wedge \cdots \wedge e_{i_s}.$$

As $e_i \wedge e_i = 0$, we get $e_{i_1} \wedge \cdots \wedge e_{i_s} = 0$, and this for every generator. Therefore, $\bigwedge^s M = (0)$. □

Let us now assume that M is a free R-module with basis $e_1, \ldots, e_n$. What are $\mathcal{T}(M)$, $\mathrm{Sym}(M)$ and $\bigwedge(M)$?

The elements of $\mathcal{T}_r(M)$ are sums of terms of the form $m_1 \otimes \cdots \otimes m_r$. Now, each m_i is expressed uniquely as $m_i = \sum_j \lambda_j e_j$. Therefore, in $\mathcal{T}_r(M)$, elements are unique sums of terms of the form

$$(\mu_1 e_{i_1}) \otimes (\mu_2 e_{i_2}) \otimes \cdots \otimes (\mu_r e_{i_r}),$$

where e_{i_l} might be equal to e_{i_k} with $i_l \neq i_k$. Let X_j be the image of e_j in $\mathcal{T}(M)$. Then, we see that the elements of $\mathcal{T}(M)$ are sums of "funny monomials"

$$\mu_1 X_{i_1} \mu_2 X_{i_2} \cdots \mu_d X_{i_d},$$

and in these monomials, we do not have $X\mu = \mu X$ (in general). In conclusion, the general polynomial ring over R in n variables is equal to $\mathcal{T}\Big(\coprod_{j=1}^{n} R\Big)$. If our free module is good (i.e., there exists a basis $e_1, \ldots, e_n$ and $\lambda e_i = e_i \lambda$ for all $\lambda \in R$ and all e_i), then we get our simplified noncommutative polynomial ring $R\langle X_1, \ldots, X_n\rangle$, as in Section 2.2.

For $\mathrm{Sym}\Big(\coprod_{j=1}^{r} R\Big)$, where $\coprod_{j=1}^{r} R$ is good, we just get our polynomial ring $R[X_1, \ldots, X_r]$.

All this presumed that the rank of a free finitely-generated R-module made sense. There are rings where this is false. However, if a ring possesses a homomorphism into a field, then ranks do make sense (DX). Under this assumption and assuming that the free module $M = \coprod_{j=1}^{r} R$ has a good basis, we can determine the ranks of $\mathcal{T}_d(M)$, $\mathrm{Sym}_d(M)$ and $\bigwedge^d(M)$. Since elements of the form

$$e_{i_1} \otimes \cdots \otimes e_{i_d}, \quad \text{where } \{i_1, \ldots, i_d\} \text{ is any subset of } \{1, \ldots, r\}$$

form a basis of $\mathcal{T}_d(M)$, we get $\mathrm{rk}(\mathcal{T}(M)) = r^d$. Linear independence is reduced to the case where R is a field in virtue of our assumption. Here, it is not very difficult linear algebra to prove linear independence. For example, $M \otimes_k N$ is isomorphic to $\mathrm{Hom}_k(M^D, N)$, say by Corollary 2.49.

Elements of the form

$$e_{i_1} \otimes \cdots \otimes e_{i_d}, \quad \text{where } i_1 \leq i_2 \leq \ldots \leq i_d$$

form a basis of $\mathrm{Sym}_d(M)$, so we get $\mathrm{rk}(\mathrm{Sym}_d(M)) = \binom{r+d-1}{d}$ (DX–The linear algebra is the same as before, only the counting is different). Let us check this formula in some simple cases. For $r = d = 2$, the formula predicts dimension 3; indeed, we have the basis of 3 monomials: X_1^2, X_2^2, X_1X_2. For $r = d = 3$, the formula predicts dimension 10; we have the basis of 10 monomials:

$$X_1^3,\ X_2^3,\ X_3^3,\ X_1^2X_2,\ X_1^2X_3,\ X_2^2X_1,\ X_2^2X_3,\ X_3^2X_1,\ X_3^2X_2,\ X_1X_2X_3.$$

Finally, elements of the form

$$e_{i_1} \wedge \cdots \wedge e_{i_d}, \quad \text{where } i_1 < i_2 < \ldots < i_d$$

form a basis of $\bigwedge^d(M)$, so we get $\dim(\bigwedge^d(M)) = \binom{r}{d}$. Again, linear independence follows from the field case. Here, it will be instructive to make a filtration of $\bigwedge^d M$ in terms of lower wedges of M and $\widetilde{M}$, where $\widetilde{M}$ has rank $r-1$. Then, induction can be used. All this will be left to the reader.

And now, an application to a bit of geometry. Let M be a (smooth) manifold of dimension r. For every $x \in M$, we have the *tangent space* to M at x, denoted $T(M)_x$, a rank r vector space. A basis of this vector space is

$$\frac{\partial}{\partial X_1}, \ldots, \frac{\partial}{\partial X_r},$$

where $X_1, \ldots, X_r$ are local coordinates at $x \in M$. A tangent vector is just

$$\sum_{j=1}^{r} a_j \frac{\partial}{\partial X_j},$$

the directional derivative w.r.t. the vector $\overrightarrow{v} = (a_1, \ldots, a_r)$. The dual space, $T(M)_x^D$, is called the *cotangent space at* x or the *space of* 1*-forms at* x, and has the dual basis: $dX_1, \ldots, dX_r$, where

$$(dX_i)\left(\frac{\partial}{\partial X_j}\right) = \delta_{ij}.$$

Every element of $T(M)_x^D$ is a 1-form at x, i.e., an expression $\sum_{j=1}^r b_j dX_j$. We have the two vector space families $\bigcup_{x\in M} T(M)_x$ and $\bigcup_{x\in M} T(M)_x^D$. These vector space families are in fact *vector bundles* (DX), called the *tangent bundle*, $T(M)$, and the *cotangent bundle*, $T(M)^D$, respectively.

Say $\varphi\colon M \to N$ is a map of manifolds, then we get a vector space map,

$$D\varphi_x\colon T(M)_x \longrightarrow T(N)_{\varphi(x)}.$$

This map can be defined as follows: For any tangent vector, $\xi \in T(M)_x$, at x, pick a curve through x (defined near x), say $z\colon I \to M$, and having our chosen ξ as tangent vector at $t = 0$ (with $x = z(0)$). Here, I is a small open interval about 0. Then,

$$I \xrightarrow{z} M \xrightarrow{\varphi} N$$

is a curve in N through $\varphi(x)$, and we take the derivative of $\varphi(z(t))$ at $t = 0$ to be our tangent vector $(D\varphi_x)(\xi)$.

By duality, there is a corresponding map $(D\varphi_x)^*\colon T(N)^D_{\varphi(x)} \longrightarrow T(M)^D_x$ called *pull-back* of differential forms. Given any open subset, V, of N, for any section, $\omega \in \Gamma(V, \bigwedge^d T(N)^D)$, by pullback we get the section $\varphi^*\omega \in \Gamma(\varphi^{-1}(V), \bigwedge^d T(M)^D)$. The reader should explicate this map in terms of the local coordinates on V and $\varphi^{-1}(V)$.

Now, consider some section, $\omega \in \Gamma(U, \bigwedge^d T(M)^D)$, where U is an open in M. In local coordinates, ω looks like

$$\sum_{i_1<\cdots<i_d} a(x) dx_{i_1} \wedge \cdots \wedge dx_{i_d}; \quad x \in U.$$

Here, U is a piece of a chart, i.e., there is a diffeomorphism $\varphi\colon V\ (\subseteq \mathbb{R}^r) \xrightarrow{\sim} U$. If $z\colon I\ (\subseteq \mathbb{R}^d) \longrightarrow V$ is a map of a D-disk to V, the composition $\varphi \circ z$ is called an *elementary d-chain* in $U \subseteq M$, and a *d-chain* is a formal $\mathbb{Z}$-combination of elementary d-chains. Then, we have $(\varphi\circ z)^*\omega$, a d-form on I. Hence, by elementary real calculus in several variables,

$$\int_I (\varphi \circ z)^*\omega$$

makes sense. ((DX), compute $(\varphi\circ z)^*\omega$ in local coordinates.) We define the integral of ω over the elementary d-chain $\varphi(z(I))$ by

$$\int_{\varphi(z(I))} \omega = \int_I (\varphi \circ z)^*\omega,$$

and for d-chains, let

$$\int_{d-\text{chain}} \omega = \sum \int_{\text{elem. pieces}} \omega.$$

An elaboration of these simple ideas gives the theory of integration of forms on manifolds.

We also have the theory of determinants. Suppose R is a commutative ring and M is a free module of rank d over R with basis $e_1, \ldots, e_d$. So,

$$M \cong \coprod_{j=1}^d Re_j.$$

Let N be another free module of the same rank with basis $f_1, \ldots, f_d$. Then, a linear map $\varphi \in \mathrm{Hom}_R(M, N)$ gives a matrix in the usual way ($\varphi(e_j)$ as linear combination of the f_i's *is* the j-th column). By functoriality, we get a linear map $\bigwedge^d \varphi\colon \bigwedge^d M \to \bigwedge^d N$. Now, each of $\bigwedge^d M$ and $\bigwedge^d N$ is free of rank 1, and their bases are $e_1 \wedge \cdots \wedge e_d$ and $f_1 \wedge \cdots \wedge f_d$, respectively. Therefore,

$$\Big(\bigwedge^d \varphi\Big)(e_1 \wedge \cdots \wedge e_d) = \lambda(f_1 \wedge \cdots \wedge f_d),$$

for some unique $\lambda \in R$. This unique λ is the *determinant* of φ, by definition. Now, $\left(\bigwedge^d \varphi\right)(e_1 \wedge \cdots \wedge e_d) = \varphi(e_1) \wedge \cdots \wedge \varphi(e_d)$, and so $\det(\varphi)$ is an alternating multilinear map on the columns of the matrix of φ. If Q is yet a third free module of rank d and if $\psi\colon N \to Q$ is an R-linear map and $g_1, \ldots, g_d$ a chosen basis for the module Q, then we find that $\bigwedge^d \psi$ takes $f_1 \wedge \cdots \wedge f_d$ to $\mu(g_1 \wedge \cdots \wedge g_d)$, where $\mu = \det(\psi)$. Since $\bigwedge^d \psi$ is R-linear, it takes $\lambda(f_1 \wedge \cdots \wedge f_d)$ to $\lambda\mu(g_1 \wedge \cdots \wedge g_d)$, and it follows that

$$\det(\psi \circ \varphi) = \mu\lambda = \det(\psi)\det(\varphi).$$

It might appear that $\det(\varphi)$ depends upon our choice of basis, but this is not entirely so. If one has two choices of bases in each of M and N, say $\{e_i\}$ and $\{\widetilde{e_i}\}$; $\{f_j\}$ and $\{\widetilde{f_j}\}$, and if the matrices of the identity transformations $M \longrightarrow M$ and $N \longrightarrow N$ in the basis pairs are the same, then $\det(\varphi)$ is the same whether computed with e's and f's or with $\widetilde{e}$'s and $\widetilde{f}$'s. This situation holds when we identify M and N as same rank free modules, then we have just one pair of bases: The $\{e_i\}$ and the $\{\widetilde{e_i}\}$. The determinant of the endomomorphism $\varphi\colon M \to M$ is then independent of the choice of basis.

If M and N have different ranks, say M has rank r with chosen basis $e_1, \ldots, e_r$ while N has rank s with chosen basis $f_1, \ldots, f_s$, then for any R-linear $\varphi\colon M \to N$, we have the induced map

$$\bigwedge^d \varphi\colon \bigwedge^d M \longrightarrow \bigwedge^d N.$$

Consider $e_{j_1} \wedge \cdots \wedge e_{j_d}$, an element of the induced basis for $\bigwedge^d M$. We apply the map $\bigwedge^d \varphi$ and find

$$\left(\bigwedge^d \varphi\right)(e_{j_1} \wedge \cdots \wedge e_{j_d}) = \sum_{1 \le i_1 < \cdots < i_d \le s} \lambda_{i_1 \ldots i_d}^{j_1 \cdots j_d} f_{i_1} \wedge \cdots \wedge f_{i_d}.$$

The element $\lambda_{i_1 \ldots i_d}^{j_1 \cdots j_d} \in R$ is exactly the $d \times d$ minor from the rows $i_1, \ldots, i_d$ and columns $j_1, \ldots, j_d$ of the matrix of φ in the given bases. So, the $d \times d$ minors form the entries for $\bigwedge^d \varphi$. Projectives being cofactors of free modules allow the definition of determinants of their endomorphisms as well. For this, one must study $\bigwedge^d(P \amalg \widetilde{P})$. (DX)

For the next two remarks, assume that $R \in \mathrm{CR}$.

Remarks:

(1) Let Z be a commutative R-algebra. Then, the functor, $Z \rightsquigarrow (Z)\,(= Z$ as R-module), has as left-adjoint in CR the functor $M \rightsquigarrow \mathrm{Sym}_R(M)$:

$$\mathrm{Hom}_{R\text{-alg}}(\mathrm{Sym}_R(M), Z) \xrightarrow{\sim} \mathrm{Hom}_R(M, (Z))$$

is a functorial isomorphism (in M and Z).

(2) An *alternating R-algebra* is a $\mathbb{Z}/2\mathbb{Z}$-graded R-algebra (which means that $Z = Z_{\mathrm{even}} \amalg Z_{\mathrm{odd}} = Z_0 \amalg Z_1$, with $Z_i Z_j \subseteq Z_{i+j \,(\mathrm{mod}\, 2)}$), together with the commutativity rule

$$\xi\eta = (-1)^{\deg \xi \cdot \deg \eta}\eta\xi.$$

The left-adjoint property for $\bigwedge M$ is this: The functor $Z \rightsquigarrow (Z_1)\,(= Z_1$ as R-module, where Z is an alternating R-algebra) has $M \rightsquigarrow \bigwedge M$ as left adjoint, i.e.,

$$\mathrm{Hom}_{\text{alt. } R\text{-alg}}(\bigwedge M, Z) \xrightarrow{\sim} \mathrm{Hom}_R(M, (Z_1))$$

is a functorial isomorphism (in M and Z).

Remark: If $\omega \in (\bigwedge M)_{\text{even}}$, then $\omega \wedge \omega$ need **not** be zero. In fact, if $\xi \in \bigwedge^p M$ and $\eta \in \bigwedge^q M$, then (DX)

$$\xi \wedge \eta = (-1)^{pq} \eta \wedge \xi.$$

Example: $M = \mathbb{R}^4$, $\omega = dx_1 \wedge dx_2 + dx_3 \wedge dx_4$ (ω is the standard symplectic form on $\mathbb{R}^4$). We have

$$\omega \wedge \omega = (dx_1 \wedge dx_2 + dx_3 \wedge dx_4) \wedge (dx_1 \wedge dx_2 + dx_3 \wedge dx_4) = 2dx_1 \wedge dx_2 \wedge dx_3 \wedge dx_4 \neq 0.$$

Flat Modules. As with the functor Hom, we single out those modules rendering $\otimes$ an exact functor. Actually, before we study right limits, little of consequence can be done. So, here is an introduction and some first properties; we'll return to flatness in Section 2.8.

Definition 2.8 An R^{op}-module, M, is *flat (over R)* iff the functor $N \rightsquigarrow M \otimes_R N$ is exact. If M is an R-module then M is *flat (over R) iff the functor (on R^{op}-modules) $N \rightsquigarrow N \otimes_R M$ is exact. The module, M, is faithfully flat iff M is flat and $M \otimes_R N = (0)$ (resp. $N \otimes_R M = (0)$) implies $N = (0)$.*

Proposition 2.53 *Say M is an R-module (resp. R^{op}-module) and there is another R-module (resp. R^{op}-module), $\widetilde{M}$, so that $M \amalg \widetilde{M}$ is flat. Then M is flat. Finitely generated free modules are faithfully flat. Finitely generated projective modules are flat. Finite coproducts of flat modules are flat. (The finiteness hypotheses will be removed in Section 2.8, but the proofs require the notion of right limit.)*

Proof. Let $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ be an exact sequence; we treat the case where M is an R^{op}-module. Let $F = M \amalg \widetilde{M}$. As F is flat, the sequence

$$0 \longrightarrow F \otimes_R N' \longrightarrow F \otimes_R N \quad \text{is exact.}$$

We have the diagram

$$\begin{array}{ccccccc} & & M \otimes_R N' & \xrightarrow{\quad\theta\quad} & M \otimes_R N & & \\ & & \downarrow & & \downarrow & & \\ F \otimes_R N' & \xrightarrow{\cong} & M \otimes_R N' \amalg \widetilde{M} \otimes_R N' & \longrightarrow & M \otimes_R N \amalg \widetilde{M} \otimes_R N & \xleftarrow{\cong} & F \otimes_R N. \end{array}$$

The bottom horizontal arrow is injective and the vertical arrows are injective too, as we see by tensoring the split exact sequence

$$0 \longrightarrow M \longrightarrow F \longrightarrow \widetilde{M} \longrightarrow 0$$

on the right with N and N'. A trivial diagram chase shows that θ is injective, as contended.

Assume F is free and f.g., that is, $F = \coprod_S R$, where $S \neq \emptyset$ and S is finite. Since $F \otimes_R N \cong \coprod_S N$, we have $F \otimes_R N = (0)$ iff $N = (0)$. If we knew that finite coproducts of flats were flat, all we would need to show is that R itself is flat. But, $R \otimes_R N \cong N$, and so, $R \otimes_R -$ is exact.

Let M and $\widetilde{M}$ be flat and consider their coproduct, $F = M \amalg \widetilde{M}$. Then, for any exact sequence

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

the maps $f\colon M \otimes_R N' \to M \otimes_R N$ and $g\colon \widetilde{M} \otimes_R N' \to \widetilde{M} \otimes_R N$ are injective, as M and $\widetilde{M}$ are flat. Since the coproduct functor is exact, $f \amalg g$ is injective and so

$$(M \otimes_R N') \amalg (\widetilde{M} \otimes_R N') \cong F \otimes_R N' \longrightarrow F \otimes_R N \cong (M \otimes_R N) \amalg (\widetilde{M} \otimes_R N)$$

is injective as well, which proves that F is flat.

If P is projective and f.g., then $P \amalg \widetilde{P} \cong F$, for some module $\widetilde{P}$ and some f.g. free module, F. The first part of the proof shows that P is flat. $\square$

Proposition 2.54 *If $R \in$ CR is an integral domain (or $R \in$ RNG has no zero divisors) then every flat module is torsion-free. The converse is true if R is a P.I.D. (the proof will be given in Section 2.8).*

Proof. If $\xi \in R$, then $0 \longrightarrow R \xrightarrow{\xi} R$ is an injective R^{op}-homomorphism ($(\xi m)\rho = \xi(m\rho)$). The diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & R \otimes_R M & \xrightarrow{\xi} & R \otimes_R M \\ & & \downarrow & & \downarrow \\ & & M & \xrightarrow{\xi} & M \end{array}$$

commutes, the vertical arrows are isomorphisms, and the upper row is exact, since M is flat. This shows that $m \mapsto \xi m$ is injective; so, if $\xi m = 0$, then $m = 0$. □

Remark: The module $\mathbb{Q}$ is a flat $\mathbb{Z}$-module. However, $\mathbb{Q}$ is **not** free, **not** projective (DX) and **not** faithfully flat ($\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = (0)$).

2.7 Limit Processes in Algebra

Let Λ be a partially ordered set (with partial order $\leq$) and assume Λ has the *Moore–Smith property* (Λ is a *directed* set), which means that for all $\alpha, \beta \in \Lambda$, there is some $\gamma \in \Lambda$ so that $\alpha \leq \gamma$ and $\beta \leq \gamma$.

Examples of Directed Sets: (1) Let X be a topological space, and pick $x \in X$; take
$\Lambda = \{U \mid (1)\, U \text{ open in } X; (2)\, x \in U\}$, with $U \leq V$ iff $V \subseteq U$.

(2) $\Lambda = \mathbb{N}$, and $n \leq m$ iff $n \mid m$ (Artin ordering).

To introduce right and left limits, we consider the following set-up: We have a category, $\mathcal{C}$, a collection of objects of $\mathcal{C}$ indexed by Λ, say C_α. Consider the two conditions (R) and (L) stated below:

(R) For all $\alpha \leq \beta$, there is a morphism, $\varphi_\alpha^\beta \colon C_\alpha \to C_\beta$, and there is compatibility: For all $\alpha \leq \beta \leq \gamma$, the diagram

$$\begin{array}{ccc} & C_\gamma & \\ {\scriptstyle \varphi_\alpha^\gamma}\nearrow & & \nwarrow{\scriptstyle \varphi_\beta^\gamma} \\ C_\alpha & \xrightarrow[\varphi_\alpha^\beta]{} & C_\beta \end{array}$$

commutes and $\varphi_\alpha^\alpha = \mathrm{id}_{C_\alpha}$.

(L) For all $\alpha \leq \beta$, there is a morphism, $\psi_\beta^\alpha \colon C_\beta \to C_\alpha$, and there is compatibility: For all $\alpha \leq \beta \leq \gamma$, the diagram

$$\begin{array}{ccc} & C_\gamma & \\ {\scriptstyle \psi_\gamma^\alpha}\swarrow & & \searrow{\scriptstyle \psi_\gamma^\beta} \\ C_\alpha & \xleftarrow[\psi_\beta^\alpha]{} & C_\beta \end{array}$$

commutes and $\psi_\alpha^\alpha = \mathrm{id}_{C_\alpha}$.

Definition 2.9 A *right (direct, inductive) mapping family, $(C_\alpha, \varphi_\alpha^\beta)$, of $\mathcal{C}$* is a family of objects, C_α, and *morphisms*, φ_α^β, satisfying axiom (R). *Mutatis mutandis* for a *left (inverse, projective) mapping family*, $(C_\alpha, \psi_\beta^\alpha)$ and axiom (L).

Examples of Right and Left Mapping Families:

(1L) Let $\Lambda = \mathbb{N}$ with the usual ordering, $\mathcal{C} = \mathcal{A}\mathrm{b}$ and $C_n = \mathbb{Z}$. Pick a prime, p; for $m \leq n$, define $\psi_n^m \colon \mathbb{Z} \to \mathbb{Z}$ as multiplication by p^{n-m}.

(1R) Same Λ, same $\mathcal{C}$, same C_n, and $\varphi_m^n \colon \mathbb{Z} \to \mathbb{Z}$ is multiplication by p^{n-m}.

(2L) Same Λ, Artin ordering, same $\mathcal{C}$, same C_n. If $n \leq m$, then $n \mid m$, so $m\mathbb{Z} \subseteq n\mathbb{Z}$, define $\psi_m^n \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ as the projection map.

(2R) Same Λ, Artin ordering, same $\mathcal{C}$, $C_n = \mathbb{Z}/n\mathbb{Z}$. If $n \leq m$, then $r = m/n \in \mathbb{Z}$, define $\varphi_n^m \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ as multiplication by r.

Look at the functor (from $\mathcal{C}$ to $\mathcal{S}\mathrm{ets}$)

$$T \rightsquigarrow \left\{ (f_\alpha \colon C_\alpha \longrightarrow T)_\alpha \;\middle|\; \begin{array}{ccc} & T & \\ {\scriptstyle f_\alpha}\nearrow & & \nwarrow{\scriptstyle f_\beta} \\ C_\alpha & \xrightarrow[\varphi_\alpha^\beta]{} & C_\beta \end{array} \quad \text{commutes whenever } \alpha \leq \beta \right\},$$

denoted $\varinjlim_\alpha (C_\alpha, \varphi_\alpha^\beta)(T)$, and the cofunctor (from $\mathcal{C}$ to $\mathcal{S}\mathrm{ets}$)

$$T \rightsquigarrow \left\{ (g_\alpha \colon T \longrightarrow C_\alpha)_\alpha \;\middle|\; \begin{array}{ccc} & T & \\ {\scriptstyle c_\alpha}\swarrow & & \searrow{\scriptstyle c_\beta} \\ C_\alpha & \xleftarrow[\psi_\beta^\alpha]{} & C_\beta \end{array} \quad \text{commutes whenever } \alpha \leq \beta \right\},$$

denoted $\varprojlim_\beta (C_\beta, \psi_\beta^\alpha)(T)$.

Question: *Are either (or both) of these representable?*

Definition 2.10 The *right (direct, inductive) limit* of a right mapping family, $(C_\alpha, \varphi_\alpha^\beta)$, is the pair, $(C, \{c_\alpha\})$, representing the functor $\varinjlim_\alpha (C_\alpha, \varphi_\alpha^\beta)$ and is denoted $\varinjlim_\alpha (C_\alpha, \varphi_\alpha^\beta)$. The *left (inverse, projective) limit* of a left mapping family, $(C_\beta, \psi_\beta^\alpha)$, is the pair, $(C, \{c_\beta\})$, representing the functor $\varprojlim_\beta (C_\beta, \psi_\beta^\alpha)$, denoted $\varprojlim_\beta (C_\beta, \psi_\beta^\alpha)$.

Let us explicate this definition. First, consider right mapping families. The tuple $\{c_\alpha\}_\alpha$ is to lie in $\varinjlim_\alpha (C_\alpha, \varphi_\alpha^\beta)(C)$, the set of tuples of morphisms, $c_\alpha \colon C_\alpha \to C$, so that the diagram

$$\begin{array}{ccc} & T & \\ {\scriptstyle c_\alpha}\nearrow & & \nwarrow{\scriptstyle c_\beta} \\ C_\alpha & \xrightarrow[\varphi_\alpha^\beta]{} & C_\beta \end{array}$$

commutes whenever $\alpha \leq \beta$. We seek an object, $C \in \mathcal{C}$, and a family of morphisms, $c_\alpha \colon C_\alpha \to C$, so that

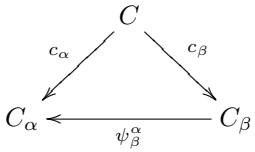
$$\mathrm{Hom}_{\mathcal{C}}(C, T) \cong \varinjlim_\alpha (C_\alpha, \varphi_\alpha^\beta)(T),$$

for every $T \in \mathcal{C}$, *via* the isomorphism $u \mapsto \{u \circ c_\alpha\}_\alpha$. Thus, the above functorial isomorphism says that for every family of morphisms, $\{f_\alpha \colon C_\alpha \to T\}_\alpha \in \varinjlim_\alpha (C_\alpha, \varphi_\alpha^\beta)(T)$, there is a *unique* morphism, $u \colon C \to T$, so that

$$f_\alpha = u \circ c_\alpha, \quad \text{for all } \alpha \in \Lambda.$$

This is the *universal mapping property* of $\varinjlim_\alpha C_\alpha$.

Next, consider left mapping families. This time, the tuple $\{c_\beta\}_\beta$ is to lie in $\varprojlim_\beta (C_\beta, \psi_\beta^\alpha)(C)$, the set of tuples of morphisms, $c_\beta \colon C \to C_\beta$, so that the diagram



commutes whenever $\alpha \leq \beta$. We seek an object, $C \in \mathcal{C}$, and a family of morphisms, $c_\beta \colon C \to C_\beta$, so that

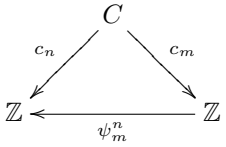
$$\mathrm{Hom}_{\mathcal{C}}(T, C) \cong \varprojlim_\beta (C_\beta, \psi_\beta^\alpha)(T),$$

for every $T \in \mathcal{C}$, *via* the isomorphism $u \mapsto \{c_\beta \circ u\}_\beta$. The *universal mapping property* of $\varprojlim_\alpha C_\alpha$ is that for every family of morphisms, $\{g_\alpha \colon T \to C_\alpha\}_\alpha \in \varprojlim_\beta (C_\beta, \psi_\beta^\alpha)(T)$, there is a *unique* morphism, $u \colon T \to C$, so that

$$g_\alpha = c_\alpha \circ u, \quad \text{for all } \alpha \in \Lambda.$$

Remark: A right (resp. left) mapping family in $\mathcal{C}$ is the same as a left (resp. right) mapping family in the dual category $\mathcal{C}^D$. Thus, $\varinjlim_\alpha (C_\alpha)$ exists in $\mathcal{C}$ iff $\varprojlim_\alpha (C_\alpha)$ exists in $\mathcal{C}^D$.

Let us examine Example (1L). If we assume that its inverse limit exists, then we can find out what this is. By definition, whenever $n \leq m$, the map $\psi_m^n \colon \mathbb{Z} \to \mathbb{Z}$ is multiplication by p^{m-n}. Pick $\xi \in C$, hold n fixed and look at $c_n(\xi) \in \mathbb{Z}$. For all $m \geq n$, the commutativity of the diagram



shows that $p^{m-n} c_m(\xi) = c_n(\xi)$, and so, p^{m-n} divides $c_n(\xi)$ for all $m \geq n$. This can only be true if $c_n \equiv 0$. Therefore, all the maps, c_n, are the zero map. As there is a unique homomorphism from any abelian group, T, to (0) and as the tuple of maps, $\{c_\alpha\}_\alpha$, is the tuple of zero maps, the group (0) with the zero maps is $\varprojlim_\alpha C_\alpha$. In fact, this argument with T replacing C *proves* the existence of the left limit for the family (1L) and exhibits it as (0).

Theorem 2.55 *(Existence Theorem) If $\mathcal{C}$ is any one of the categories: $\mathcal{S}$ets, Ω-groups (includes R-modules, vector spaces, $\mathcal{A}$b, $\mathcal{G}$r), topological spaces, topological groups,* CR, RNG, *then both $\varinjlim_\alpha$ and $\varprojlim_\alpha$ are representable (we say that $\mathcal{C}$ possesses arbitrary right and left limits).*

Proof. We give a complete proof for $\mathcal{S}$ets and indicate the necessary modifications for the other categories. Let Λ be a directed index set.

(1) *Right limits*: For every $\alpha \in \Lambda$, we have a set, S_α, and we have set maps, $\varphi_\alpha^\beta \colon S_\alpha \to S_\beta$, whenever $\alpha \leq \beta$. Let $\mathcal{S} = \bigcup\!\!\cdot\, S_\alpha$, the coproduct of the S_α's in $\mathcal{S}$ets (their disjoint union). Define an equivalence relation on $\mathcal{S}$ as follows: For all $x, y \in \mathcal{S}$,

$$\text{if } x \in S_\alpha \text{ and } y \in S_\beta \text{ then} \quad x \sim y \quad \text{iff} \quad (\exists \gamma \in \Lambda)(\alpha \leq \gamma,\ \beta \leq \gamma)(\varphi_\alpha^\gamma(x) = \varphi_\beta^\gamma(y)).$$

We need to check that $\sim$ is an equivalence relation. It is obvious that $\sim$ is reflexive and symmetric.

Say $x \sim y$ and $y \sim z$. This means that $x \in S_\alpha$, $y \in S_\beta$, $z \in S_\gamma$ and there exist $\delta_1, \delta_2 \in \Lambda$ so that $\alpha \leq \delta_1$; $\beta \leq \delta_1$; $\beta \leq \delta_2$; $\gamma \leq \delta_2$, and

$$\varphi_\alpha^{\delta_1}(x) = \varphi_\beta^{\delta_1}(y);\ \varphi_\beta^{\delta_2}(y) = \varphi_\gamma^{\delta_2}(z).$$

As Λ is directed, there is some $\delta \in \Lambda$, with $\delta_1 \leq \delta$ and $\delta_2 \leq \delta$; so, we may replace δ_1 and δ_2 by δ. Therefore, $\varphi_\alpha^\delta(x) = \varphi_\gamma^\delta(z)$, and transitivity holds. Let $S = \mathcal{S}/\sim$. We have the maps

$$s_\alpha \colon S_\alpha \longrightarrow \bigcup_\lambda\!\!\cdot\, S_\lambda = \mathcal{S} \xrightarrow{pr} \mathcal{S}/\sim = S,$$

and the pair $(S, \{s_\alpha\})$ represents $\varinjlim_\alpha S_\alpha$, as is easily checked.

(2) *Left Limits*: We have sets, S_α, for every $\alpha \in \Lambda$, and maps, $\psi_\beta^\alpha \colon S_\beta \to S_\alpha$. Let

$$P = \Big\{(\xi_\alpha) \in \prod_\alpha S_\alpha \ \Big|\ (\forall \alpha \leq \beta)(\psi_\beta^\alpha(\xi_\beta) = \xi_\alpha)\Big\},$$

be the collection of consistent tuples from the product. The set P might be empty.

We have the maps

$$p_\alpha \colon P \hookrightarrow \prod_\alpha S_\alpha \xrightarrow{pr_\alpha} S_\alpha.$$

The pair $(P, \{p_\alpha\})$ represents the cofunctor $\varprojlim_\alpha S_\alpha$ (DX).

Modifications: Look first at the category of groups (this also works for Ω-groups and rings).

(1′) *Right limits*. Write G_α for each group ($\alpha \in \Lambda$). We claim that $G = \varinjlim_\alpha G_\alpha$ (in $\mathcal{S}$ets) is already a group (etc., in a natural way) and as a group, it represents our functor. All we need to do is to define the group operation on $\varinjlim_\alpha G_\alpha$. If $x, y \in G = \varinjlim_\alpha G_\alpha$, then $x = c_\alpha(\xi)$ and $y = c_\beta(\eta)$, for some $\xi \in G_\alpha$ and some $\eta \in G_\beta$. Since Λ is directed, there is some $\gamma \in \Lambda$ with $\alpha, \beta \leq \gamma$; consider $\xi' = \varphi_\alpha^\gamma(\xi)$ and $\eta' = \varphi_\beta^\gamma(\eta)$. (Obviously, $c_\gamma(\xi') = x$ and $c_\gamma(\eta') = y$.) So, we have $\xi', \eta' \in G_\gamma$, and we set

$$xy = c_\gamma(\xi'\eta').$$

Check (DX) that such a product is well-defined and that G is a group. Also, the maps c_α are group homomorphisms.

The existence of right limits now holds for all the algebraic categories.

Now, consider the category, TOP, of topological spaces. Observe that when each S_α is a topological space, then the disjoint union, $\mathcal{S} = \bigcup\!\!\cdot\, S_\alpha$, is also a topological space (using the disjoint union topology); in fact, it is the coproduct in TOP. Give $S = \mathcal{S}/\sim$ the quotient topology, and then check that the maps s_α are continuous and that $(S, \{s_\alpha\})$ represents $\varinjlim_\alpha S_\alpha$ in TOP.

For the category of topological groups, TOPGR, check that $G = \varinjlim_{\alpha} G_\alpha$ is also a topological space as above and (DX) that the group operations are continuous. Thus, $(G, \{s_\alpha\}_\alpha)$ represents $\varinjlim_{\alpha} G_\alpha$ in TOPGR.

(2′) *Left Limits*. Again, first assume each G_α is a group and the ψ_β^α are homomorphisms. Check that P (= consistent tuples) is a group (in particular, note that $(1, 1, \ldots, 1, \ldots)$ is consistent so that $P \neq \emptyset$) and that the p_α's are homomorphisms (DX); hence, $(P, \{p_\alpha\})$ represents $\varprojlim_{\alpha} G_\alpha$. Now, similar reasoning shows left limits exist for all the algebraic categories.

For TOP, we make $\prod_\alpha S_\alpha$ into a topological space with the product topology. Check (DX) that the continuity of the ψ_β^α's implies that P is closed in $\prod_\alpha S_\alpha$. Then, the p_α's are also continuous and $(P, \{p_\alpha\})$ represents $\varprojlim_{\alpha} S_\alpha$ in TOP.

For TOPGR, similar remarks, as above for TOP and as in the discussion for groups, imply that $(P, \{p_\alpha\})$ represents $\varprojlim_{\alpha} G_\alpha$ in TOPGR. □

Remark: Say Λ is a directed index set. We can make Λ a category as follows: $\mathcal{O}\mathrm{b}(\Lambda) = \Lambda$, and

$$\mathrm{Hom}(\alpha, \beta) = \begin{cases} \emptyset & \text{if } \alpha \not\leq \beta; \\ \{\cdot\} & \text{if } \alpha \leq \beta. \end{cases}$$

(Here, $\{\cdot\}$ denotes a one-point set.) Given a right mapping family, $(C_\alpha, \varphi_\alpha^\beta)$, where $\varphi_\alpha^\beta \in \mathrm{Hom}_{\mathcal{C}}(C_\alpha, C_\beta)$, we define the functor, RF, by

$$\begin{aligned} \mathrm{RF}(\alpha) &= C_\alpha \\ \mathrm{RF}(\cdot\colon \alpha \to \beta) &= \varphi_\alpha^\beta. \end{aligned}$$

Similarly, there is a one-to-one correspondence between left-mapping families, $(C_\beta, \psi_\beta^\alpha)$, and cofunctors, LF, defined by

$$\begin{aligned} \mathrm{LF}(\alpha) &= C_\alpha \\ \mathrm{LF}(\cdot\colon \alpha \to \beta) &= \psi_\beta^\alpha. \end{aligned}$$

If we now think of RF and LF as "functions" on Λ and view the Moore–Smith property as saying that the α's "grow without bound", then we can interpret $\varinjlim_{\alpha} C_\alpha$ and $\varprojlim_{\alpha} C_\alpha$ as: "limits, as $\alpha \to \infty$, of our 'functions' RF and LF",

$$\varinjlim_{\alpha} C_\alpha = \lim_{\alpha \to \infty} \mathrm{RF}(\alpha) \quad \text{and} \quad \varprojlim_{\alpha} C_\alpha = \lim_{\alpha \to \infty} \mathrm{LF}(\alpha).$$

Indeed, there is a closer analogy. Namely, we are taking the limit of $\mathrm{RF}(\alpha)$ and $\mathrm{LF}(\alpha)$ as *nets* in the sense of general topology.

Say $\Gamma \subseteq \Lambda$ is a subset of our index set, Λ. We say that Γ is *final* in Λ (old terminology, *cofinal*) iff for every $\alpha \in \Lambda$, there is some $\beta \in \Gamma$ with $\alpha \leq \beta$. Check (DX),

$$\varinjlim_{\alpha \in \Gamma} C_\alpha = \varinjlim_{\alpha \in \Lambda} C_\alpha; \quad \varprojlim_{\alpha \in \Gamma} C_\alpha = \varprojlim_{\alpha \in \Lambda} C_\alpha.$$

Examples of Right and Left Limits:

(1R) Recall that $\Lambda = \mathbb{N}$ with the ordinary ordering, $C_n = \mathbb{Z}$ and for $m \geq n$, φ_n^m is multiplication by p^{m-n}. Consider the isomorphism, $\theta_n \colon \mathbb{Z} \to (1/p^n)\mathbb{Z} \subseteq \mathbb{Q}$, defined by $\theta_n(1) = 1/p^n$. The diagram

$$\begin{array}{ccccc} C_n = \mathbb{Z} & \xrightarrow{\theta_n} & \dfrac{1}{p^n}\mathbb{Z} & \hookrightarrow & \mathbb{Q} \\ \Big\downarrow{\scriptstyle p^{m-n}} & & \Big\downarrow{\scriptstyle \text{incl}} & & \Big\| \\ C_m = \mathbb{Z} & \xrightarrow[\theta_m]{} & \dfrac{1}{p^m}\mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

commutes, and so, the direct limit on the left is equal to the direct limit in the middle. There, the direct limit is

$$\varinjlim_m C_m = \left\{ \frac{k}{p^t} \;\middle|\; k \in \mathbb{Z},\ p \not| k \right\} \subseteq \mathbb{Q}.$$

This subgroup, $\varinjlim_m C_m$, of $\mathbb{Q}$ is usually denoted $\dfrac{1}{p^\infty}\mathbb{Z}$.

Generalization: $\Lambda = \mathbb{N}$, Artin ordering ($n \leq m$ iff $n \mid m$), $C_n = \mathbb{Z}$, and for $n \leq m$, define, $\varphi_n^m =$ multiplication by m/n. We get

$$\varinjlim_n C_n = \mathbb{Q}. \tag{$*$}$$

(2R) What is $\varinjlim_{n|m} \mathbb{Z}/n\mathbb{Z}$? If we observe that $\mathbb{Z}/n\mathbb{Z} \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, by $(*)$, we get

$$\varinjlim_{n|m} \mathbb{Z}/n\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

Say X and Y are topological spaces and pick $x \in X$. Let

$$\Lambda_x = \{U \mid U \text{ open in } X \text{ and } x \in U\};$$

Partially order Λ_x so that $U \leq V$ iff $V \subseteq U$ (usual ordering on Λ_x). Clearly, Λ_x has Moore–Smith. Let

$$\mathcal{C}(U) = \left\{ f \;\middle|\; \begin{array}{l} (1)\ f \colon U \to Y \\ (2)\ f \text{ is continuous on } U \text{ (or perhaps has better properties)} \end{array} \right\}$$

Look at $\varinjlim_{\Lambda_x} \mathcal{C}(U)$, denoted temporarily C_x. We have $\xi \in C_x$ iff there is some open subset, U, of X, with $x \in U$, some continuous function, $f \colon U \to Y$, and ξ is the class of f.

Two functions, $f \colon U \to Y$ and $g \colon V \to Y$, where $U, V \subseteq X$ are open and contain x, give the same ξ iff there is some open, $W \subseteq U \cap V$, with $x \in W$, so that $f \restriction W = g \restriction W$. Therefore, C_x is the set of germs of continuous functions on X at x. (The usual notation for C_x is $\mathcal{O}_{X,x}$.)

(2L) Consider the left limit, $\varprojlim_{n|m} \mathbb{Z}/n\mathbb{Z}$, where $\psi_m^n \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is projection. The elements of $\varprojlim_{n|m} \mathbb{Z}/n\mathbb{Z}$ are tuples, (ξ_n), with $\xi_n \in \mathbb{Z}$, such that

(1) $(\xi_n) = (\eta_n)$ iff $(\forall n)(\xi_n \equiv \eta_n \pmod n)$ and

(2) (consistency): If $n \mid m$, then $\xi_m \equiv \xi_n \pmod n$.

We obtain a new object, denoted $\widehat{\mathbb{Z}}$. We have an injective map, $\mathbb{Z} \longrightarrow \widehat{\mathbb{Z}}$, given by $n \mapsto (n, n, \ldots, n, \ldots)$. You should check that the following two statements are equivalent:

(1) Chinese Remainder Theorem.

(2) $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$.

Proposition 2.56 *Say $C = \varinjlim_{\alpha} C_\alpha$ and let $x \in C_\alpha$ and $y \in C_\beta$, with $c_\alpha(x) = c_\beta(y)$. Then, there is some $\gamma \geq \alpha, \beta$, so that $\varphi_\alpha^\gamma(x) = \varphi_\beta^\gamma(y)$. In particular, if all the φ_α^β are injections, so are the canonical maps, c_α.*

Proof. Clear. □

Corollary 2.57 *Say $\mathcal{C} = \Omega$-modules and each C_α is Ω-torsion-free. Then, $\varinjlim_{\alpha} C_\alpha$ is torsion-free.*

Proof. Pick $x \in C = \varinjlim_{\alpha} C_\alpha$; $\lambda \in \Omega$, with $\lambda \neq 0$. Then, $\lambda x = \lambda c_\alpha(x_\alpha)$, for some α and some $x_\alpha \in C_\alpha$. So, $0 = \lambda x = c_\alpha(\lambda x_\alpha)$ implies that there is some $\gamma \geq \alpha$, with $\varphi_\alpha^\gamma(\lambda x_\alpha) = 0$. Consequently, $\lambda \varphi_\alpha^\gamma(x_\alpha) = \lambda x_\gamma = 0$. But C_γ is torsion-free, so $x_\gamma = 0$. Therefore, $x = c_\alpha(x_\alpha) = c_\gamma(x_\gamma) = 0$. This proves that C is torsion-free. □

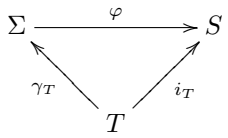
Corollary 2.58 *Say $\mathcal{C} = \Omega$-modules and each C_α is Ω-torsion. Then, $\varinjlim_{\alpha} C_\alpha$ is torsion.*

Proof. If $x \in C$, then there is some α and some $x_\alpha \in C_\alpha$, with $c_\alpha(x_\alpha) = x$. But, there is some $\lambda \in \Omega$, with $\lambda \neq 0$, so that $\lambda x_\alpha = 0$, since C_α is torsion. So, $\lambda x = \lambda c_\alpha(x_\alpha) = c_\alpha(\lambda x_\alpha) = 0$. □

Proposition 2.59 *Let Λ be an index set and $\mathcal{C} = \mathcal{S}$ets. Then, every set is the right-limit of its finite subsets (under inclusion). The same conclusion holds if $\mathcal{C} = \mathcal{G}$r, Ω-groups, RNG, then each object of $\mathcal{C}$ is equal to the right limit of its finitely generated subobjects.*

Proof. Let $\Lambda = \{T \subseteq S \mid T \text{ finite}\}$. Order Λ, *via* $T \leq W$ iff $T \subseteq W$. Clearly, Λ has Moore–Smith. Let $\Sigma = \varinjlim_{T \in \Lambda} T$.

For a given $T \in \Lambda$, we have an injective map, $i_T \colon T \hookrightarrow S$. Hence, by the universal mapping property, these maps factor through the canonical maps, $\gamma_T \colon T \to \Sigma$, *via* a fixed map, $\varphi \colon \Sigma \to S$:



Pick some $\xi \in S$. Then, $\{\xi\} \in \Lambda$; so we get a map, $\gamma_{\{\xi\}} \colon \{\xi\} \to \Sigma$. Let $\psi(\xi) = \gamma_{\{\xi\}}(\xi) \in \Sigma$. This gives a map, $\psi \colon S \to \Sigma$. Check (DX), φ and ψ are inverse maps.

Modifications: $\Lambda = \{T \subseteq S \mid T \text{ is a finitely generated subobject of } S\}$ and proceed analogously. □

Corollary 2.60 *An abelian group is torsion iff it is a right-limit of finite abelian groups.*

Corollary 2.61 *Say $\mathcal{C}$ is a category with finite coproducts (or finite products). If $\mathcal{C}$ has right limits (resp. left limits) then $\mathcal{C}$ has arbitrary coproducts (resp. arbitrary products).*

Proof. Cf. Problem 62. □

Proposition 2.62 *Say $\{G_\alpha\}_\alpha$ is a left-mapping family of finite groups (not necessarily abelian). Then, the left limit, $\varprojlim_\alpha G_\alpha = G$, is a compact topological group. (Such a G is called a profinite group.) Similarly, if the G_α are compact topological groups and form a left-mapping family with continuous homomorphisms, then $\varprojlim_\alpha G_\alpha = G$ is a compact topological group.*

Proof. Observe that the second statement implies the first. Now, G is the group of consistent tuples in $\prod_\alpha G_\alpha$. By Tychonov's theorem, $\prod_\alpha G_\alpha$ is compact. As the ψ_β^α are continuous, the subgroup of consistent tuples is *closed*; therefore, this subgroup is compact. □

It follows from Proposition 2.62 that $\widehat{\mathbb{Z}}$ is compact.

2.8 Flat Modules (Again)

Proposition 2.63 *Say $\{\Omega_\alpha\}_\alpha$ is a right-mapping family of rings, $\{M_\alpha\}_\alpha$, $\{N_\alpha\}_\alpha$ are "right-mapping families" of $\Omega_\alpha^{\mathrm{op}}$ (resp. Ω_α)-modules, then $\{M_\alpha \otimes_{\Omega_\alpha} N_\alpha\}_\alpha$ forms a right-mapping family (in $\mathcal{A}\mathrm{b}$) and*

$$\varinjlim_\alpha (M_\alpha \otimes_{\Omega_\alpha} N_\alpha) = \Big(\varinjlim_\alpha M_\alpha\Big) \otimes_{\varinjlim_\alpha \Omega_\alpha} \Big(\varinjlim_\alpha N_\alpha\Big).$$

Proof. The hypothesis (within quotes) means that for all $\alpha \le \beta$, we have

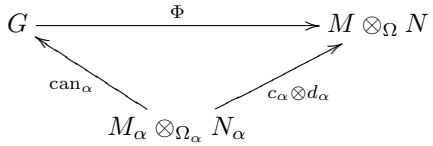
$$\psi_\alpha^\beta(\lambda_\alpha n_\alpha) = \theta_\alpha^\beta(\lambda_\alpha)\psi_\alpha^\beta(n_\alpha), \quad \text{for all } \lambda_\alpha \in \Omega_\alpha \text{ and all } n_\alpha \in N_\alpha,$$

where $\psi_\alpha^\beta\colon N_\alpha \to N_\beta$ and $\theta_\alpha^\beta\colon \Omega_\alpha \to \Omega_\beta$, and similarly with the M_α's.

Let $M = \varinjlim_\alpha M_\alpha$; $N = \varinjlim_\alpha N_\alpha$; $\Omega = \varinjlim_\alpha \Omega_\alpha$ and $G = \varinjlim_\alpha (M_\alpha \otimes_{\Omega_\alpha} N_\alpha)$. Write $c_\alpha\colon M_\alpha \to M$; $d_\alpha\colon N_\alpha \to N$ and $t_\alpha\colon \Omega_\alpha \to \Omega$, for the canonical maps. We have the maps

$$c_\alpha \otimes d_\alpha\colon M_\alpha \otimes_{\Omega_\alpha} N_\alpha \longrightarrow M \otimes_\Omega N,$$

hence, by the universal mapping property of right limits, there is a unique map, $\Phi\colon G \to M \otimes_\Omega N$, so that the following diagram commutes for every α:



We also need a map, $M \otimes_\Omega N \longrightarrow G$. Pick $m \in M$ and $n \in N$, since the index set is directed we may assume that there is some α so that $m = c_\alpha(m_\alpha)$ and $n = d_\alpha(n_\alpha)$. Thus, we have $m_\alpha \otimes_{\Omega_\alpha} n_\alpha \in M_\alpha \otimes_{\Omega_\alpha} N_\alpha$ and so, $\mathrm{can}_\alpha(m_\alpha \otimes_{\Omega_\alpha} n_\alpha) \in G$. Define Ψ by

$$\Psi(m, n) = \mathrm{can}_\alpha(m_\alpha \otimes_{\Omega_\alpha} n_\alpha).$$

Check (DX) that

(1) Ψ is well-defined,

(2) Ψ is bilinear; thus, by the universal mapping property of tensor, there is a map, $\Psi\colon M \otimes_\Omega N \to G$,

(3) Φ and Ψ are inverse homomorphisms. □

Proposition 2.64 *Suppose $\mathcal{C} = \mathcal{M}\mathrm{od}(\Omega)$ and N'_α, N_α, N''_α, are all right-mapping families of Ω-modules. If for every α, the sequence*

$$0 \longrightarrow N'_\alpha \longrightarrow N_\alpha \longrightarrow N''_\alpha \longrightarrow 0 \quad \textit{is exact,}$$

then the sequence

$$0 \longrightarrow \varinjlim_\alpha N'_\alpha \longrightarrow \varinjlim_\alpha N_\alpha \longrightarrow \varinjlim_\alpha N''_\alpha \longrightarrow 0 \quad \textit{is again exact.}$$

Proof. (DX) □

Corollary 2.65 *The right-limit of flat modules is flat.*

Proof. The operation $\varinjlim_\alpha$ commutes with tensor and preserves exactness, as shown above. □

Corollary 2.66 *Tensor product commutes with arbitrary coproducts. An arbitrary coproduct of flat modules is flat.*

Proof. Look at $\coprod_{\alpha\in S} M_\alpha$. We know from the Problems that $\coprod_{\alpha\in S} M_\alpha = \varinjlim_T M_T$, where $T \subseteq S$, with T finite and $M_T = \coprod_{\beta\in T} M_\beta$. So, given N, we have

$$\begin{aligned} N \otimes_\Omega \Big(\coprod_S M_\alpha\Big) &= N \otimes_\Omega \varinjlim_T M_T \\ &= \varinjlim_T (N \otimes_\Omega M_T) \\ &= \varinjlim_T \coprod_{\beta\in T} (N \otimes_\Omega M_\beta) \\ &= \coprod_{\beta\in S} (N \otimes_\Omega M_\beta). \end{aligned}$$

The second statement follows from Corollary 2.65 and the fact that finite coproducts of flat modules are flat (Proposition 2.53). □

Remark: Corollary 2.66 extends the last part of Proposition 2.44 that only asserts that tensor commutes with finite coproducts. It also proves that Proposition 2.53 holds for arbitrary modules, not just f.g. modules. Thus, free modules are flat and so, projective modules are flat, too.

Proposition 2.67 *Say Ω is a ring and M is an Ω^{op}-module (resp. Ω-module). Then, M is flat iff for every exact sequence*

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

of Ω (resp. Ω^{op})-modules in which all three modules are f.g., the induced sequence

$$0 \longrightarrow M \otimes_\Omega N' \longrightarrow M \otimes_\Omega N \longrightarrow M \otimes_\Omega N'' \longrightarrow 0$$

(*resp.*
$$0 \longrightarrow N' \otimes_\Omega M \longrightarrow N \otimes_\Omega M \longrightarrow N'' \otimes_\Omega M \longrightarrow 0)$$

remains exact.

Proof. Given

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0,$$

an arbitrary exact sequence of Ω-modules, write $N = \varinjlim_\alpha N_\alpha$, where the N_α's are f.g. submodules of N. Let N''_α be the image of N_α in N''. So, N''_α is f.g., too. We get the exact sequence

$$0 \longrightarrow N' \cap N_\alpha \longrightarrow N_\alpha \longrightarrow N''_\alpha \longrightarrow 0. \qquad (*)$$

Now, $N' \cap N_\alpha = \varinjlim_\beta \mathcal{N}_\beta^{(\alpha)}$, where $\mathcal{N}_\beta^{(\alpha)}$ ranges over the f.g. submodules of $N' \cap N_\alpha$. We get the exact sequence

$$0 \longrightarrow \mathcal{N}_\beta^{(\alpha)} \longrightarrow N_\alpha \longrightarrow N''_{\alpha,\beta} \longrightarrow 0, \tag{$\dagger$}$$

where $N''_{\alpha,\beta} = N_\alpha/\mathcal{N}_\beta^{(\alpha)}$, and all the modules in ($\dagger$) are f.g. The right limit of ($\dagger$) is ($*$). By hypothesis, $M \otimes_\Omega$ ($\dagger$) is still exact, and the right limit of an exact sequence is exact; so

$$0 \longrightarrow M \otimes_\Omega (N' \cap N_\alpha) \longrightarrow M \otimes_\Omega N_\alpha \longrightarrow M \otimes_\Omega N''_\alpha \longrightarrow 0 \quad \text{is exact.}$$

Now, if we pass to the right limit, this time over α, we get

$$0 \longrightarrow M \otimes_\Omega N' \longrightarrow M \otimes_\Omega N \longrightarrow M \otimes_\Omega N'' \longrightarrow 0 \quad \text{is exact.}$$ □

Theorem 2.68 *(FGI-Test)*[1] *An Ω-module, M, is flat iff for all sequences*

$$0 \longrightarrow \mathfrak{A} \longrightarrow \Omega^{\mathrm{op}} \longrightarrow \Omega^{\mathrm{op}}/\mathfrak{A} \longrightarrow 0$$

in which $\mathfrak{A}$ is a finitely generated Ω^{op}-ideal, the sequence

$$0 \longrightarrow \mathfrak{A} \otimes_\Omega M \longrightarrow \Omega^{\mathrm{op}} \otimes_\Omega M \longrightarrow (\Omega^{\mathrm{op}}/\mathfrak{A}) \otimes_\Omega M \longrightarrow 0 \quad \textit{is still exact.}$$

Proof. ($\Rightarrow$) is trivial.

($\Leftarrow$). We proceed in two steps.

Step 1. I claim: For every exact sequence of Ω^{op}-modules of the form

$$0 \longrightarrow K \longrightarrow \coprod_S \Omega^{\mathrm{op}} \longrightarrow N \longrightarrow 0, \tag{$*$}$$

in which $\#(S)$ is finite, we have an exact sequence

$$0 \longrightarrow K \otimes_\Omega M \longrightarrow \Big(\coprod_S \Omega^{\mathrm{op}}\Big) \otimes_\Omega M \longrightarrow N \otimes_\Omega M \longrightarrow 0.$$

We prove this by induction on the *minimal number, r, of generators of N*. (Note that $\#(S) \geq r$.) The case $r = 1$ has all the ingredients of the general proof as we will see. When $r = 1$, look first at the base case: $\#(S) = 1$, too. Sequence ($*$) is then:

$$0 \longrightarrow K \longrightarrow \Omega^{\mathrm{op}} \longrightarrow N \longrightarrow 0. \tag{$*_1$}$$

This means that K is an ideal of Ω^{op} and we know $K = \varinjlim_\alpha K_\alpha$, where the K_α's are f.g. Ω^{op}-ideals. Then, ($*$)$_1$ is the right limit of

$$0 \longrightarrow K_\alpha \longrightarrow \Omega^{\mathrm{op}} \longrightarrow N_\alpha \longrightarrow 0, \tag{$*_\alpha$}$$

where $N_\alpha = \Omega^{\mathrm{op}}/K_\alpha$. Our hypothesis shows that

$$0 \longrightarrow K_\alpha \otimes_\Omega M \longrightarrow \Omega^{\mathrm{op}} \otimes_\Omega M \longrightarrow N_\alpha \otimes_\Omega M \longrightarrow 0 \quad \text{is exact.}$$

Pass the latter sequence to the limit over α and obtain

$$0 \longrightarrow K \otimes_\Omega M \longrightarrow \Omega^{\mathrm{op}} \otimes_\Omega M \longrightarrow N \otimes_\Omega M \longrightarrow 0 \quad \text{is exact.}$$

[1] FGI stands for finitely generated ideal.

Thus, the base case $\#(S) = r = 1$ is proved.

We now use induction on $\#(S)$ to establish the case $\#(S) > r = 1$. (So, our claim involves an induction inside an induction.) The induction hypothesis is: For all exact sequences

$$0 \longrightarrow K \longrightarrow \coprod_S \Omega^{\mathrm{op}} \longrightarrow N \longrightarrow 0,$$

in which $\#(S) = s$ *and* $r\,(=$ minimal number of generators of $N) = 1$, tensoring with M leaves the sequence exact. Say it is true for all sequences with $\#(S) < s$. Given

$$0 \longrightarrow K \longrightarrow \coprod_S \Omega^{\mathrm{op}} \longrightarrow N \longrightarrow 0, \quad \#(S) = s,$$

pick some $\sigma \in S$ and let $\Sigma = S - \{\sigma\}$. We have the map $\Omega^{\mathrm{op}} = \Omega_\sigma^{\mathrm{op}} \hookrightarrow \coprod_S \Omega^{\mathrm{op}} \longrightarrow N$, and we let N_σ be the image of this map in N. This gives the commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K_\sigma & \longrightarrow & \Omega = \Omega_\sigma & \longrightarrow & N_\alpha & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K & \longrightarrow & \coprod_S \Omega & \longrightarrow & N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K'' & \longrightarrow & \coprod_\Sigma \Omega & \longrightarrow & N'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

(where $N'' = N/N_\sigma$) with exact rows and columns and the middle column split-exact. Note that N'' and N_σ have $r \leq 1$ and when $r = 0$ the above argument is trivial. Tensor the diagram on the right with M. So, the top and bottom rows remain exact (by the induction hypothesis and the base case), the middle column remains exact (in fact, split) and all other rows and columns are exact:

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
0 & \longrightarrow & K_\sigma \otimes_\Omega M & \longrightarrow & \Omega \otimes_\Omega M & \longrightarrow & N_\alpha \otimes_\Omega M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \nu} & & \downarrow & & \downarrow & & \\
 & & K \otimes_\Omega M & \xrightarrow{\alpha} & \left(\coprod_S \Omega\right) \otimes_\Omega M & \longrightarrow & N \otimes_\Omega M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \theta} & & \downarrow & & \\
0 & \longrightarrow & K'' \otimes_\Omega M & \longrightarrow & \left(\coprod_\Sigma \Omega\right) \otimes_\Omega M & \longrightarrow & N'' \otimes_\Omega M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} .$$

We must show that α is an injection. Take $x \in K \otimes_\Omega M$. If $\alpha(x) = 0$, then $\theta(\alpha(x)) = 0$, which implies that $\pi(x)$ goes to zero under the injection $(K'' \otimes_\Omega M \longrightarrow \left(\coprod_\Sigma \Omega\right) \otimes_\Omega M)$, and so, $\pi(x) = 0$. Then, there is some

$y \in K_\sigma \otimes_\Omega M$ with $\nu(y) = x$. But the map $K_\sigma \otimes_\Omega M \longrightarrow \Omega \otimes_\Omega M \longrightarrow \left(\coprod_S \Omega\right) \otimes_\Omega M$ is injective and y goes to zero under it. So, we must have $y = 0$, and thus, $x = 0$. This proves that α is injective, and completes the interior induction (case: $r = 1$). By the way, α is injective by the five lemma with the two left vertical sequences considered horizontal and read backwards!

There remains the induction on r. The case $r = 1$ is proved. If the statement is true for modules N with $< r$ minimal generators, we take an N with exactly r as its number of minimal generators. Then, for any finite S, and any sequence

$$0 \longrightarrow K \longrightarrow \coprod_S \Omega^{\mathrm{op}} \longrightarrow N \longrightarrow 0,$$

we choose, as above, $\sigma \in S$ and set $\Sigma = S - \{\sigma\}$ and let N_σ, N'' be as before. Now redo the argument involving the 9 term diagram; it shows α is, once again, injective and the claim is proved.

Step 2. I claim that for every sequence

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

of Ω^{op}-modules, all of which are f.g., the sequence

$$0 \longrightarrow N' \otimes_\Omega M \longrightarrow N \otimes_\Omega M \longrightarrow N'' \otimes_\Omega M \longrightarrow 0$$

remains exact. By the previous proposition, this will finish the proof.

Since N', N and N'' are all f.g., we have the commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K' & \longrightarrow & \coprod_S \Omega & \longrightarrow & N' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K & \longrightarrow & \coprod_{S\cup T} \Omega & \longrightarrow & N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K'' & \longrightarrow & \coprod_T \Omega & \longrightarrow & N'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array},$$

in which the middle column is split-exact. By tensoring this diagram with M (on the right), we get the

following commutative diagram with all exact rows (by Step 1) and columns:

$$\begin{array}{ccccccccc}
 & & & & 0 & & \operatorname{Ker}\alpha & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K'\otimes_\Omega M & \longrightarrow & \left(\coprod_S \Omega\right)\otimes_\Omega M & \longrightarrow & N'\otimes_\Omega M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & K\otimes_\Omega M & \longrightarrow & \left(\coprod_{S\cup T} \Omega\right)\otimes_\Omega M & \longrightarrow & N\otimes_\Omega M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K''\otimes_\Omega M & \xrightarrow{\beta} & \left(\coprod_T \Omega\right)\otimes_\Omega M & \longrightarrow & N''\otimes_\Omega M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & .
\end{array}$$

We must show that α is injective. Apply the snake lemma to the first two rows: We get

$$0 \longrightarrow \operatorname{Ker}\alpha \xrightarrow{\delta} K''\otimes_\Omega M \xrightarrow{\beta} \left(\coprod_T \Omega\right)\otimes_\Omega M \quad \text{is exact.}$$

But, $\operatorname{Ker}\beta = (0)$ implies that $\operatorname{Im}\delta = (0)$, and so, $\operatorname{Ker}\alpha = (0)$. □

The second (unproven) assertion of Proposition 2.54 now follows from Theorem 2.68.

Corollary 2.69 *If Ω is a P.I.D., more generally, a nonzero-divisor ring all of whose f.g. Ω^{op}-ideals are principal, then M is flat over Ω iff M is Ω-torsion-free.*

Proof. The implication ($\Rightarrow$) is always true when Ω has no zero divisors.

($\Leftarrow$). By the previous theorem, we only need to test against exact sequences of the form

$$0 \longrightarrow \mathfrak{A} \longrightarrow \Omega^{\mathrm{op}} \longrightarrow \Omega^{\mathrm{op}}/\mathfrak{A} \longrightarrow 0,$$

where $\mathfrak{A}$ is a f.g. (hence, *principal*) Ω^{op}-ideal. So, there is some $\lambda \in \Omega$ with $\mathfrak{A} = \lambda\Omega$. We have the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega & \xrightarrow{\lambda} & \Omega & \longrightarrow & \Omega/\lambda\Omega & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \theta} & & \| & & \| & & \\
0 & \longrightarrow & \mathfrak{A} & \hookrightarrow & \Omega & \longrightarrow & \Omega/\mathfrak{A} & \longrightarrow & 0
\end{array}$$

(with $\mathfrak{A}$ considered as right ideal and where $\theta(\mu) = \lambda\mu$) and all the vertical maps are isomorphisms. Consequently, we may assume that our exact sequence is

$$0 \longrightarrow \Omega \xrightarrow{\lambda} \Omega \longrightarrow \Omega/\lambda\Omega \longrightarrow 0.$$

By tensoring with M, we get the exact sequence

$$\Omega\otimes_\Omega M \xrightarrow{\lambda} \Omega\otimes_\Omega M \longrightarrow (\Omega/\lambda\Omega)\otimes_\Omega M \longrightarrow 0,$$

which, in view of the isomorphisms $\Omega\otimes_\Omega M \cong M$ and $(\Omega/\lambda\Omega)\otimes_\Omega M \cong M/\lambda M$, is equivalent to

$$M \xrightarrow{\lambda} M \longrightarrow M/\lambda M \longrightarrow 0.$$

Since M has no torsion, multiplication by λ is injective and the sequence is exact. □

The corollary is false if Ω is not a P.I.D. Here is an example:

Consider the ring, $A = \mathbb{C}[X, Y]$ ($A \in \mathrm{CR}$). The ring A is a domain; so, it is torsion-free. (It's even a UFD.) Let $\mathfrak{M}$ be the ideal of A generated by X and Y. We can write

$$\begin{aligned}\mathfrak{M} &= \{f \in \mathbb{C}[X,Y] \mid f(X,Y) = g(X,Y)X + h(X,Y)Y, \text{ with } g(X,Y), h(X,Y) \in \mathbb{C}[X,Y]\} \\ &= \{f \in \mathbb{C}[X,Y] \mid f(0,0) = 0, \text{ i.e., } f \text{ has no constant term}\}.\end{aligned}$$

Since $\mathfrak{M} \subseteq A$, we see that $\mathfrak{M}$ is torsion-free.

Claim: $\mathfrak{M}$ is not flat.

Now, $A/\mathfrak{M} \cong \mathbb{C}$, so $\mathbb{C}$ is an A-module; how?

The A-module structure on $\mathbb{C}$ is as follows: For any $f(X,Y) \in A$ and any $\lambda \in \mathbb{C}$,

$$f(X,Y) \cdot \lambda = f(0,0)\lambda.$$

Note that $X \cdot \lambda = Y \cdot \lambda = 0$. When we consider $\mathfrak{M}$ as an A-module, write its generators as e_1 and e_2. Under the map $\mathfrak{M} \longrightarrow A$, we have $e_1 \mapsto X$ and $e_2 \mapsto Y$. There is a unique nontrivial relation:

$$Y \cdot e_1 - X \cdot e_2 = 0.$$

We claim that $e_1 \otimes e_2 \neq e_2 \otimes e_1$ in $\mathfrak{M} \otimes_A \mathfrak{M}$. To see this, define a map, $B\colon \mathfrak{M} \times \mathfrak{M} \to \mathbb{C}$.

(a) First, define B on the generators e_1, e_2, by setting

$$B(e_1, e_1) = B(e_2, e_2) = 0, \quad B(e_1, e_2) = 1, \quad B(e_2, e_1) = -1.$$

(b) We need to check that B is well-defined. Let's check it for the left hand side argument:

$$B\left(Y \cdot e_1 - X \cdot e_2, \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}\right) = Y \cdot B\left(e_1, \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}\right) - X \cdot B\left(e_2, \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}\right).$$

In the case of e_1, we get $X \cdot 1 = 0$, and in the case of e_2, we get $Y \cdot 1 = 0$. The reader should check similarly that there is no problem for the righthand side argument.

Consequently, we get a linear map, $\theta\colon \mathfrak{M} \otimes \mathfrak{M} \longrightarrow \mathbb{C}$. For this linear map,

$$\theta(e_1 \otimes e_1) = \theta(e_2 \otimes e_2) = 0, \quad \theta(e_1 \otimes e_2) = 1, \quad \theta(e_2 \otimes e_1) = -1.$$

So, $e_1 \otimes e_2 \neq e_2 \otimes e_1$, as contended. Now we will see that $\mathfrak{M}$ is **not** flat as A-module. Look at the exact sequence

$$0 \longrightarrow \mathfrak{M} \longrightarrow A \longrightarrow \mathbb{C} \longrightarrow 0$$

and tensor it with $\mathfrak{M}$. We get

$$\mathfrak{M} \otimes_A \mathfrak{M} \longrightarrow A \otimes_A \mathfrak{M} \longrightarrow \mathbb{C} \otimes_A \mathfrak{M} \longrightarrow 0 \quad \text{is exact.}$$

However, $\mathfrak{M} \otimes_A \mathfrak{M} \longrightarrow A \otimes_A \mathfrak{M}$ is not injective. To see this, use the isomorphism $\mu\colon A \otimes_A \mathfrak{M} \cong \mathfrak{M}$, *via* $\alpha \otimes m \mapsto \alpha \cdot m$ and examine the composed homomorphism

$$\varphi\colon \mathfrak{M} \otimes_A \mathfrak{M} \longrightarrow A \otimes_A \mathfrak{M} \xrightarrow{\mu} \mathfrak{M}.$$

Since μ is an isomorphism, all we must prove is that φ is not injective. But,

$$\begin{aligned}\varphi(e_1 \otimes e_2) &= \mu(X \otimes e_2) = X \cdot e_2 \\ \varphi(e_2 \otimes e_1) &= \mu(Y \otimes e_1) = Y \cdot e_1.\end{aligned}$$

Yet, $X \cdot e_2 = Y \cdot e_1$ and $e_1 \otimes e_2 \neq e_2 \otimes e_1$, so φ is not injective and $\mathfrak{M}$ is not flat.

Say Ω is a Λ-algebra and M is a Λ^{op}-module, then $M \otimes_\Lambda \Omega$ is an Ω^{op}-module. The module $M \otimes_\Lambda \Omega$ is called the *base extension* of M to Ω.

Proposition 2.70 *Say M is a flat Λ-module, then its base extension, $\Omega \otimes_\Lambda M$, is again a flat Ω-module. If N is a flat Ω-module and Ω is a flat Λ-algebra, then N considered as Λ-module (via $\Lambda \longrightarrow \Omega$), is again flat over Λ.*

Proof. Assume M is flat as Λ-module. Then, we know that for any exact sequence of Λ^{op}-modules,

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0,$$

the sequence

$$0 \longrightarrow N' \otimes_\Lambda M \longrightarrow N \otimes_\Lambda M \quad \text{is exact.}$$

Now, take any exact sequence of Ω-modules, say

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0, \tag{$\dagger$}$$

it is still exact as a sequence of Λ-modules. Hence,

$$0 \longrightarrow N' \otimes_\Lambda M \longrightarrow N \otimes_\Lambda M \quad \text{is exact.}$$

Tensoring ($\dagger$) with $\Omega \otimes_\Lambda M$ over Ω, we get

$$N' \otimes_\Omega (\Omega \otimes_\Lambda M) \longrightarrow N \otimes_\Omega (\Omega \otimes_\Lambda M) \longrightarrow \cdots . \tag{$\dagger\dagger$}$$

We want to show that ($\dagger\dagger$) is exact on the left. But $Z \otimes_\Omega (\Omega \otimes_\Lambda M) \cong Z \otimes_\Lambda M$, for any Ω^{op}-module, Z. Hence, ($\dagger\dagger$) becomes

$$N' \otimes_\Lambda M \longrightarrow N \otimes_\Lambda M \longrightarrow \cdots ,$$

and we already observed that this sequence is exact on the left.

For the second part, take an exact sequence of Λ^{op}-modules,

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0. \tag{$*$}$$

We need to show that

$$0 \longrightarrow M' \otimes_\Lambda N \longrightarrow M \otimes_\Lambda N \quad \text{is exact.}$$

Tensor ($*$) over Λ with Ω. The resulting sequence

$$0 \longrightarrow M' \otimes_\Lambda \Omega \longrightarrow M \otimes_\Lambda \Omega \longrightarrow \cdots \tag{$**$}$$

is still exact as Ω is flat. Tensor ($**$) with N over Ω; again, as N is flat over Ω, we get

$$0 \longrightarrow (M' \otimes_\Lambda \Omega) \otimes_\Omega N \longrightarrow (M \otimes_\Lambda \Omega) \otimes_\Omega N \longrightarrow \cdots \quad \text{is exact.}$$

But the latter exact sequence is just

$$0 \longrightarrow M' \otimes_\Lambda N \longrightarrow M \otimes_\Lambda N \longrightarrow \cdots ,$$

as required. □

Harder question: Let $P(\Lambda)$ be a property of Λ-modules. Say Ω is a Λ-algebra and M is a Λ-module. Then, we get the Ω-module, $\Omega \otimes_\Lambda M$, the base extension of M to Ω. Suppose, $\Omega \otimes_\Lambda M$ has $P(\Omega)$. Does M have $P(\Lambda)$?

If so, one says that *P descends in the extension Ω over Λ*. This matter is a question of descent.

A more realistic question is: Given P, or a collection of interesting P's, for which Λ-algebras, Ω, does (do) $P(\Omega)$ descend?

Examples:

1. $P_1(\Lambda)$: M is a torsion-free Λ-module.
2. $P_2(\Lambda)$: M is a flat Λ-module.
3. $P_3(\Lambda)$: M is a free Λ-module.
4. $P_4(\Lambda)$: M is an injective Λ-module.
5. $P_5(\Lambda)$: M is a torsion Λ-module.

Take $\Lambda = \mathbb{Z}$ (a very good ring: commutative, P.I.D), $\Omega = \mathbb{Q}$ (a field, a great ring), $\mathbb{Q}$ is flat over $\mathbb{Z}$ (and $\mathbb{Z} \hookrightarrow \mathbb{Q}$). Let $M = \mathbb{Z} \amalg (\mathbb{Z}/2\mathbb{Z})$. (The module M is f.p.) The module M, has, **none** of $P_j(\mathbb{Z})$ for $j = 1, 2, 3, 4$. On the other hand, $\mathbb{Q} \otimes_{\mathbb{Z}} M \cong \mathbb{Q}$, and $\mathbb{Q}$ has all of $P_j(\mathbb{Q})$ for $j = 1, 2, 3, 4$. However, P_5 descends in the extension $\mathbb{Q}$ over $\mathbb{Z}$. This follows from

Proposition 2.71 *The module, M, is a torsion $\mathbb{Z}$-module iff $\mathbb{Q} \otimes_{\mathbb{Z}} M = (0)$.*

Proof. ($\Rightarrow$). This has already been proved.

($\Leftarrow$). First, let M be f.g. We know that there is an exact sequence

$$0 \longrightarrow t(M) \longrightarrow M \longrightarrow M/t(M) \longrightarrow 0 \qquad (\dagger)$$

where $t(M)$ is the torsion submodule of M and $M/t(M)$ is torsion-free; hence (since M is f.g.), $M/t(M)$ is free. If we tensor ($\dagger$) with $\mathbb{Q}$, we get

$$\mathbb{Q} \otimes_{\mathbb{Z}} M \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} (M/t(M)) \longrightarrow 0.$$

Since $\mathbb{Q} \otimes_{\mathbb{Z}} M = (0)$, by hypothesis, we get $\mathbb{Q} \otimes_{\mathbb{Z}} (M/t(M)) = (0)$. Yet, $M/t(M) = \amalg_S \mathbb{Z}$ where S is finite; consequently, $S = \emptyset$ and so, $M/t(M) = (0)$, i.e., $M = t(M)$. Therefore, M is torsion.

For an arbitrary M, we can write $M = \varinjlim_{\alpha} M_\alpha$, where M_α ranges over the f.g. submodules of M. We have an exact sequence

$$0 \longrightarrow M_\alpha \longrightarrow M, \quad \text{for all } \alpha,$$

and $\mathbb{Q}$ is flat; so,

$$0 \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} M_\alpha \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} M \quad \text{is still exact.}$$

But, $\mathbb{Q} \otimes_{\mathbb{Z}} M = (0)$ implies $\mathbb{Q} \otimes_{\mathbb{Z}} M_\alpha = (0)$. As the M_α's are f.g., the previous argument shows that M_α is torsion. Then, $M = \varinjlim_{\alpha} M_\alpha$ is torsion as the right limit of torsion modules is torsion. □

We now go back to the question. Given the $\mathbb{Z}$-module M, we assume that $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is torsion. Since $\mathbb{Q}$ is a field, $\mathbb{Q} \otimes_{\mathbb{Z}} M = (0)$. Proposition 2.71 implies that M is torsion and P_5 descends in the extension $\mathbb{Q}$ over $\mathbb{Z}$.

2.9 Further Readings

Rings and modules are covered in most algebra texts, so we shall nor repeat the references given in Section 1.8. Other references include Atiyah MacDonald [3], Lafon [32, 33], Eisenbud [13], Matsumura [39], Malliavin [38] and Bourbaki [8].

Chapter 3

Commutative Rings

3.1 Introduction

The ordinary arithmetic of the integers and simple generalizations (such as the Gaussian Integers) as well as of analogues like the polynomial ring in one variable over a field gave rise to the study of number theory and then to the study of commutative rings. The assumption of commutativity in multiplication makes possible a much deeper theory with more satisfying applications. Nowadays, a thorough knowledge of this Chapter is essential in order to do Algebraic Geometry and Algebraic Number Theory (and their mixture: Arithmetic Algebraic Geometry); one also needs to know the material here for Algebraic Topology. Many of the results are direct consequences of prodding from geometry, physics and number theory. A modern problem is to use our physical knowledge (quantum theory), our knowledge of modules and representation theory, and the hints from the forefront of number theory to augment these results to a new and better theory of not necessarily commutative rings. This endeavor will probably be a big part of the twenty-first century in mathematics.

3.2 Classical Localization

All rings in this chapter are commutative with unity.

Definition 3.1 Let $A \in \mathrm{CR}$ and $S \subseteq A$ be a subset of A. We say that S *is a multiplicative subset in* A iff

(1) $1 \in S$

(2) If $x, y \in S$, then $xy \in S$

(3) $0 \notin S$.

Examples:

(1) $S = \mathbb{G}_m(A) =$ the units of A; the idea is to abstract this case.

(2) $S = \{\alpha \in A \mid \alpha \text{ is not a zero divisor in } A\}$.

(3) $S = \{x \in \mathbb{R} \mid x > 0\} \subseteq \mathbb{G}_m(\mathbb{R})$.

(3a) S has property (1) and (2) and is contained in $\mathbb{G}_m(A)$.

(4) Given $f \in A$, let $S = \{f^n \mid n \in \mathbb{Z},\ n \geq 0\}$ and assume that $f \notin \mathcal{N}(A)$ (i.e., $f^n \neq 0$ for all $n \geq 0$).

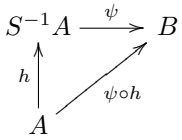
Fix a base ring, C, and look at C-algebras in CR (we get CR when $C = \mathbb{Z}$). Let A and B be C-algebras, where B varies, and let S be a multiplicative subset in A. Look at

$$\mathrm{Hom}_{C-\mathrm{alg}}(A, B; S) = \{\varphi \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B) \mid \varphi(S) \subseteq \mathbb{G}_m(B)\}.$$

Check that $B \rightsquigarrow \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$ is a functor from C-algebras to $\mathcal{S}$ets. Is it representable? This means, is there a C-algebra, $S^{-1}A$, and a map (of C-algebras), $h\colon A \to S^{-1}A$, so that

$$\theta_B\colon \mathrm{Hom}_{C-\mathrm{alg}}(S^{-1}A, B) \cong \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$$

functorially, where $\theta_B(\psi) = \psi \circ h \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$, as illustrated below:



Proposition 3.1 *The functor $B \rightsquigarrow \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$ is representable. The representing object, $S^{-1}A$, is called the fraction ring of A w.r.t. S (or the localization of A w.r.t. S). The C-algebra map, $h\colon A \to S^{-1}A$, is the canonical map.*

Proof. Look at $A \times S$ (in $\mathcal{S}$ets) and form the equivalence relation, $\sim$, given by:

$$(a, s) \sim (b, t) \quad \text{iff} \quad (\exists u \in S)(u(at - sb) = 0 \quad \text{in } A).$$

Write $\dfrac{a}{s}$ for the equivalence class of (a, s). So,

$$\frac{a}{s} = \frac{b}{t} \quad \text{iff} \quad (\exists u \in S)(u(at - sb) = 0).$$

Define addition and multiplication by:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + sb}{st} \quad \text{and} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Check that these operations are well defined and that $S^{-1}A$ is a C-algebra $\left(c \cdot \dfrac{a}{s} = \dfrac{f(c)a}{s}\right)$;[1] the C-algebra map, $h\colon A \to S^{-1}A$, is given by $h(a) = \dfrac{a}{1}$.

Functorial part. Given $\psi \in \mathrm{Hom}_{C-\mathrm{alg}}(S^{-1}A, B)$, form $\psi \circ h$ taking A to B. Now, elements of S become units in $S^{-1}A$, because

$$\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1}, \quad \text{the unit element of } S^{-1}A.$$

But, ψ maps units of $S^{-1}A$ to units of B, so $\psi \circ h \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$. Next, given $\varphi \in \mathrm{Hom}_{C-\mathrm{alg}}(A, B; S)$, define

$$[\varphi]\left(\frac{a}{s}\right) = \varphi(s)^{-1}\varphi(a) \in B.$$

Check

(a) The homomorphism $[\varphi]\colon S^{-1}A \to B$ is well defined.

(b) θ_B and $\varphi \mapsto [\varphi]$ are inverse maps. □

[1] Here, $f\colon C \to A$ is the ring homomorphism making A into a C-algebra.

We can do the same thing with modules. Let M be an A-module and S a multiplicative set in A. Make $(M \times S)/\sim$, where $\sim$ is given by

$$(m,s) \sim (n,t) \quad \text{iff} \quad (\exists u \in S)(u(tm - sn) = 0 \quad \text{in } M).$$

Write $\dfrac{m}{s}$ for the equivalence class of (m,s). Define addition and the action of A by

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \quad \text{and} \quad a \cdot \frac{m}{s} = \frac{am}{s}.$$

This gives the A-module, $S^{-1}M$. We have the canonical map, $h\colon M \to S^{-1}M$, given by $h(m) = m/1$.

To discuss what this means, look at the general case of a ring homomorphism, $\psi\colon A \to B$. We have two functors: $\psi^\bullet\colon \mathcal{M}\mathrm{od}(B) \rightsquigarrow \mathcal{M}\mathrm{od}(A)$ (*the backward image functor*) and $\psi_\bullet\colon \mathcal{M}\mathrm{od}(A) \rightsquigarrow \mathcal{M}\mathrm{od}(B)$ (*the forward image functor*). Here, $\psi^\bullet(M) = M$ as an A-module *via* ψ; that means $a \cdot m = \psi(a) \cdot m$. The functor $\psi^\bullet$ is an exact functor. Also, the functor $\psi_\bullet$ is given by: $\psi_\bullet(M) = B \otimes_A M$. The forward image functor is only right-exact, in general. These functors form a pair of adjoint functors:

$$\mathrm{Hom}_B(\psi_\bullet(M), N) \cong \mathrm{Hom}_A(M, \psi^\bullet(N)).$$

Proposition 3.2 *The module $S^{-1}M$ is, in a natural way, an $S^{-1}A$-module. The map $M \rightsquigarrow S^{-1}M$ is a functor from $\mathcal{M}\mathrm{od}(A)$ to $\mathcal{M}\mathrm{od}(S^{-1}A)$ and is left-adjoint to $h^\bullet$. That is,*

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, N) \cong \mathrm{Hom}_A(M, h^\bullet(N)).$$

Consequently,

$$S^{-1}M \cong S^{-1}A \otimes_A M \cong M \otimes_A S^{-1}A = h_\bullet(M).$$

Proof. Let $\dfrac{a}{t} \cdot \dfrac{m}{s} = \dfrac{am}{ts}$, this is well-defined and makes $S^{-1}M$ into an $S^{-1}A$-module. If $\varphi\colon M \to \widetilde{M}$ in $\mathcal{M}\mathrm{od}(A)$, the assignment $\dfrac{m}{s} \mapsto \dfrac{\varphi(m)}{s}$ yields $S^{-1}\varphi\colon S^{-1}M \to S^{-1}\widetilde{M}$. Check this makes $M \rightsquigarrow S^{-1}M$ a functor.

Say $\theta \in \mathrm{Hom}_{S^{-1}A}(S^{-1}M, N)$, set

$$\Theta(m) = \theta\left(\frac{m}{1}\right) \in h^\bullet(N).$$

Now,

$$\Theta(am) = \theta\left(\frac{am}{1}\right) = \theta\left(\frac{a}{1}\frac{m}{1}\right) = \frac{a}{1} \cdot \theta\left(\frac{m}{1}\right) = \left(a \cdot \theta\left(\frac{m}{1}\right) \text{ in } h^\bullet(N)\right) = a \cdot \Theta(m).$$

So, we have a map from $\mathrm{Hom}_{S^{-1}A}(S^{-1}M, N)$ to $\mathrm{Hom}_A(M, h^\bullet(N))$ given by $\theta \mapsto \Theta$. Now, say $\varphi \in \mathrm{Hom}_A(M, h^\bullet(N))$; then, $S^{-1}\varphi \in \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}h^\bullet(N))$. But, if $N \in \mathcal{M}\mathrm{od}(S^{-1}A)$, then $S^{-1}h^\bullet(N) = N$, and we get the map in the opposite direction, $\varphi \mapsto S^{-1}\varphi$. These maps are mutually inverse. Each of $S^{-1}-$; $S^{-1}A \otimes_A -$; $- \otimes_A S^{-1}A$, are left adjoint to $h^\bullet$; so, they are all isomorphic. □

Proposition 3.3 *The functor $M \rightsquigarrow S^{-1}M$ is exact, hence, $S^{-1}A$ is a flat A-algebra.*

Proof. Given any exact sequence $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$, we will show that $S^{-1}M_1 \xrightarrow{S^{-1}\varphi} S^{-1}M_2 \xrightarrow{S^{-1}\psi} S^{-1}M_3$ is again exact. Clearly, as $M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$ is exact, we have $\psi \circ \varphi = 0$; and so, $(S^{-1}\psi) \circ (S^{-1}\varphi) = 0$. This shows that $\mathrm{Im}\,(S^{-1}\varphi) \subseteq \mathrm{Ker}\,(S^{-1}\psi)$. Say $\xi \in S^{-1}M_2$ and $S^{-1}\psi(\xi) = 0$. As $\xi = m/s$, for some $m \in M_2$ and some $s \in S$, and as $S^{-1}\psi(\xi) = \psi(m)/s = 0$ in $S^{-1}M_3$, there is some $u \in S$ with $u\psi(m) = 0$, i.e., $\psi(um) = 0$. By exactness, there is some $m' \in M_1$ so that $um = \varphi(m')$. Consider the element $m'/(su)$; we have

$$S^{-1}\varphi\left(\frac{m'}{su}\right) = \frac{\varphi(m')}{su} = \frac{um}{su} = \frac{m}{s} = \xi.$$

Therefore, $\xi \in \mathrm{Im}\,(S^{-1}\varphi)$, as required. □

Examples:

(1) $S = \mathrm{G}_m(A)$ or more generally, $S \subseteq \mathrm{G}_m(A)$. Then, $S^{-1}A = A$.

(2) $S =$ all nonzero divisors of A. Here, $S^{-1}A$ is a bigger ring if we are not in case (1). The ring $S^{-1}A$ is called the *total fraction ring of* A and it is denoted $\mathrm{Frac}(A)$. If A is a domain, then $\mathrm{Frac}(A)$ is a field, the *fraction field of* A. For example, $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. The field, $\mathrm{Frac}(k[X_1, \ldots, X_n])$, denoted $k(X_1, \ldots, X_n)$, is the *rational function field* in n variables (where k is a field). If A is the ring of entire (holomorphic) functions, then $\mathrm{Frac}(A)$ is the field of meromorphic functions on $\mathbb{C}$. If $A = \mathrm{Hol}(U)$, the ring of holomorphic functions on an open, $U \subseteq \mathbb{C}$, then $\mathrm{Frac}(A) = \mathcal{M}\mathrm{er}(U) =$ the field of meromorphic functions on U.

(3) $S = \{f^n \mid f \in A\,(f \text{ fixed}); f \notin \mathcal{N}(A)\}$. The ring $S^{-1}A$ has the special notation A_f. Observe that

$$A_f = \left\{ \frac{\alpha}{f^n} \;\middle|\; \alpha \in A, n \geq 0 \right\},$$

while, in general,

$$\mathrm{Ker}\,(h\colon A \longrightarrow S^{-1}A) = \left\{\alpha \in A \;\middle|\; \frac{\alpha}{1} = 0\right\} = \{\alpha \in A \mid (\exists u \in S)(u\alpha = 0)\}.$$

In cases (1) and (2), the map, h, is injective. In case (3), $\mathrm{Ker}\ h = \{\alpha \in A \mid (\exists n \geq 0)(f^n\alpha = 0)\}$. Consider the map $A[X] \longrightarrow A_f$, *via* $X \mapsto 1/f$ ($a \mapsto h(a)$, for $a \in A$). Since $aX^n \mapsto a/f^n$, our map is surjective. What is its kernel?

Consider the diagram

$$\begin{array}{ccc} A_f[X] & \xrightarrow{X \mapsto 1/f} & A_f \\ {\scriptstyle h}\uparrow & & \| \\ A[X] & \xrightarrow{X \mapsto 1/f} & A_f. \end{array}$$

The kernel of the top arrow is: $(X - 1/f)$. The answer to our question is now easily seen to be

$$\{P(X) \in A[X] \mid (\exists r \geq 0)(f^r P(X) \in (Xf - 1)\} = (Xf - 1)^{ec}.$$

Here, $(Xf - 1)^{ec}$ is, for the moment, just a notation for the left hand side. So,

$$A[X]/(Xf - 1)^{ec} \cong A_f.$$

Generalities on extension (e) and contraction (c).

Let $\psi\colon A \to B$ be a map of rings. Say $\mathfrak{A}$ is an ideal in A. Let $\mathfrak{A}^e =$ (*the extended ideal*) be the ideal of B generated by $\psi(\mathfrak{A})$. If $\mathfrak{B}$ is an ideal in B, then let $\mathfrak{B}^c =$ (*the contracted ideal*) be the ideal of A given by

$$\mathfrak{B}^c = \psi^{-1}(\mathfrak{B}) = \{x \in A \mid \psi(x) \in \mathfrak{B}\}.$$

Take $B = S^{-1}A$. If $\mathfrak{A} \subseteq A$, what is $\mathfrak{A}^e$?

Claim: $\mathfrak{A}^e = \left\{ \alpha/s \mid \alpha \in \mathfrak{A},\, s \in S \right\}$. Indeed, we have

$$\mathfrak{A}^e = \left\{ \sum_{i=1}^{n} \frac{b_i}{s_i}\frac{a_i}{1} \;\middle|\; a_i \in \mathfrak{A},\, b_i \in A,\, s_i \in S \right\}.$$

Such a sum is of the form $\dfrac{1}{\sigma}\sum_{i=1}^{n} c_i a_i$, where $\sigma = s_1 \cdots s_n$; $c_i \in A$ and $a_i \in \mathfrak{A}$. Since $\mathfrak{A}$ is an ideal, this sum is of the form α/σ, where $\alpha \in \mathfrak{A}$. We have proved part of

Proposition 3.4 *For any commutative ring, A, and any multiplicative subset, S, of A we have:*

(1) $\mathbb{G}_m(S^{-1}A) = \{\alpha/s \mid (\exists b \in A)(b\alpha \in S)\}$.

(2) If $\mathfrak{A} \subseteq A$ *then* $\mathfrak{A}^e = \{\alpha/s \mid \alpha \in \mathfrak{A},\ s \in S\}$.

(3) $\mathfrak{A}^e = (1) = S^{-1}A$ *iff* $\mathfrak{A} \cap S \neq \emptyset$.

Proof. (1) We have $\alpha/s \in \mathbb{G}_m(S^{-1}A)$ iff there is some β/t with $\dfrac{\beta\alpha}{ts} = 1 = \dfrac{1}{1}$ iff $(\exists u \in S)((u\beta)\alpha = ust)$. But, $ust \in S$; so, if we set $b = u\beta$, we get $b\alpha \in S$. The converse is clear.

(2) Already done.

(3) We have $\mathfrak{A}^e = (1)$ iff some element of $\mathfrak{A}^e$ is a unit iff α/s is a unit for some $\alpha \in \mathfrak{A}$ iff there is some $b \in A$ with $b\alpha \in S$. But, $\alpha \in \mathfrak{A}$, so $b\alpha \in \mathfrak{A}$, yet $b\alpha \in S$; so, $\mathfrak{A} \cap S \neq \emptyset$. Conversely, if $\mathfrak{A} \cap S \neq \emptyset$, then $\{s/1 \mid s \in S\} \cap \mathfrak{A}^e \neq \emptyset$. Consequently, $\mathfrak{A}^e$ has a unit in it, and so, $\mathfrak{A}^e = (1)$. □

Say $\mathfrak{A} \subseteq A$, when is $\mathfrak{A}$ contracted? First an easier question: What is $\mathfrak{A}^{ec}$?

Note: for all $v \in A$, we have $\mathfrak{A} \subseteq (v \longrightarrow \mathfrak{A})$ (this only uses the fact that $\mathfrak{A}$ is a two-sided ideal).

Claim: $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$ iff v is not a zero divisor mod $\mathfrak{A}$, i.e., $\overline{v} \in A/\mathfrak{A}$ is not a zero divisor. (Terminology: v is *regular* w.r.t, $\mathfrak{A}$).

We have $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$ iff $(v \longrightarrow \mathfrak{A}) \subseteq \mathfrak{A}$ iff for every $\xi \in A$, when $\xi v \in \mathfrak{A}$, then $\xi \in \mathfrak{A}$. Reading this mod $\mathfrak{A}$, we find the above statement is equivalent to

$$(\forall \overline{\xi} \in A/\mathfrak{A})(\overline{\xi}\overline{v} = 0 \implies \overline{\xi} = 0),$$

which holds iff $\overline{v}$ is not a zero divisor in $A/\mathfrak{A}$.

Going back to the question: What is $\mathfrak{A}^{ec}$?, we have $\xi \in \mathfrak{A}^{ec}$ iff $h(\xi) \in \mathfrak{A}^e$ iff $h(\xi) = \alpha/s$, for some $\alpha \in \mathfrak{A}$ and some $s \in S$, iff $\xi/1 = \alpha/s$ iff there is some $u \in S$ so that $u(\xi s - \alpha) = 0$, i.e. $u\xi s = u\alpha \in \mathfrak{A}$. As $us \in S$, this implies that there is some $v \in S$ with $v\xi \in \mathfrak{A}$. Conversely, if $v\xi \in \mathfrak{A}$ for some $v \in S$, then

$$\frac{v}{1}\frac{\xi}{1} \in \mathfrak{A}^e \implies \frac{1}{v}\frac{v}{1}\frac{\xi}{1} \in \mathfrak{A}^e \implies \frac{\xi}{1} \in \mathfrak{A}^e \implies h(\xi) \in \mathfrak{A}^e,$$

and so, $\xi \in \mathfrak{A}^{ec}$. Therefore,

$$\begin{aligned} \mathfrak{A}^{ec} &= \{\xi \mid (\exists v \in S)(v\xi \in \mathfrak{A})\} \\ &= \{\xi \mid (\exists v \in S)(\xi \in (v \longrightarrow \mathfrak{A}))\} \\ &= \bigcup_{v \in S} (v \longrightarrow \mathfrak{A}). \end{aligned}$$

Now, $\mathfrak{A} = (1 \longrightarrow \mathfrak{A}) \subseteq \bigcup_{s \in S}(s \longrightarrow \mathfrak{A}) = \mathfrak{A}^{ec}$.

When is $\mathfrak{A}$ contracted, i.e., when is it of the form $\mathfrak{A} = \mathfrak{B}^c$, for some $\mathfrak{B} \subseteq S^{-1}A$?

Of course, if $\mathfrak{A} = \mathfrak{A}^{ec}$, then $\mathfrak{B} = \mathfrak{A}^e$ will do. In fact, we shall prove that $\mathfrak{A} = \mathfrak{B}^c$ for some $\mathfrak{B} \subseteq S^{-1}A$ iff $\mathfrak{A} = \mathfrak{A}^{ec}$. First, we claim that $\mathfrak{B} = \mathfrak{B}^{ce}$ for *every* $\mathfrak{B} \subseteq S^{-1}A$; that is, every ideal, $\mathfrak{B}$, of $S^{-1}A$ is an extended ideal. For, any ξ in $\mathfrak{B}$ is of the form $\xi = \alpha/s$, for some $\alpha \in A$ and some $s \in S$. But, $s\xi \in \mathfrak{B}$, too, and so, $\alpha/1 \in \mathfrak{B}$, which implies that $\alpha \in \mathfrak{B}^c$. Consequently, $\xi = \alpha/s \in \mathfrak{B}^{ce}$. Conversely, if $\xi \in \mathfrak{B}^{ce}$, then $\xi = \beta/t$, with $\beta \in \mathfrak{B}^c$; it follows that $\xi = (1/t)(\beta/1) \in \mathfrak{B}$, and so, $\mathfrak{B} = \mathfrak{B}^{ce}$.

But now, $\mathfrak{A} = \mathfrak{B}^c$ implies that $\mathfrak{A}^e = \mathfrak{B}^{ce} = \mathfrak{B}$; so, $\mathfrak{A}^{ec} = \mathfrak{B}^c = \mathfrak{A}$. These remarks prove most of the

Proposition 3.5 *If* $A \in \mathrm{CR}$ *and* S *is a multiplicative system in* A, *then*

(1) An ideal, $\mathfrak{A}$, of A is contracted iff $\mathfrak{A} = \mathfrak{A}^{ec}$ iff every element of S is regular for $\mathfrak{A}$.

(2) Every ideal, $\mathfrak{B} \subseteq S^{-1}A$, is extended.

(3) The map, $\mathfrak{A} \mapsto \mathfrak{A}^e$, is a one-to-one inclusion-preserving correspondence between all the contracted ideals of A and **all** *ideals of $S^{-1}A$.*

(4) If A is noetherian, then $S^{-1}A$ is noetherian.

Proof. (1) We proved earlier that $\mathfrak{A}^{ec} = \bigcup_{v \in S}(v \longrightarrow \mathfrak{A})$ and we know that $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$ iff v is regular for $\mathfrak{A}$. So, (1) is now clear.

(2) This has already been proved.

(3) Assume that $\mathfrak{A}$ and $\widetilde{\mathfrak{A}}$ have the same extension and both are contracted. Then, by (1) $\mathfrak{A} = \mathfrak{A}^{ec}$ and $\widetilde{\mathfrak{A}} = \widetilde{\mathfrak{A}}^{ec}$, and since, by hypothesis $\mathfrak{A}^e = \widetilde{\mathfrak{A}}^e$, we get $\mathfrak{A} = \widetilde{\mathfrak{A}}$. It is also clear that if $\mathfrak{A} \subseteq \widetilde{\mathfrak{A}}$, then $\mathfrak{A}^e \subseteq \widetilde{\mathfrak{A}}^e$.

(4) (DX) from (1), (2), (3). □

The same argument shows the corresponding proposition for modules.

Proposition 3.6 *If $A \in$ CR and S is a multiplicative system in A, for any module, $M \in \mathcal{M}\mathrm{od}(A)$,*

(1) A submodule, N, of M is contracted iff it is equal to its S-saturation. The S-saturation of N is the submodule given by

$$\{\xi \in M \mid (\exists v \in S)(v\xi \in N)\} = \bigcup_{v \in S}(v \longrightarrow N),$$

where $(v \longrightarrow N) = \{\xi \in M \mid v\xi \in N\}$.

(2) Every submodule of $S^{-1}M$ is extended, i.e., has the form $S^{-1}N$, for some submodule, N, of M.

(3) The map, $N \mapsto S^{-1}N$, is a one-to-one inclusion-preserving correspondence between all the S-saturated submodules of M and **all** *submodules of $S^{-1}M$.*

(4) If M is a noetherian module, then $S^{-1}M$ is a noetherian module.

Proposition 3.7 *Say $A \in$ CR and S is a multiplicative system in A. For any ideal, $\mathfrak{A} \subseteq A$, we have*

(a) The image, $\overline{S}$, of S in $A/\mathfrak{A}$, is a multiplicative subset provided that $S \cap \mathfrak{A} = \emptyset$.

(b) $S^{-1}A/\mathfrak{A}^e \xrightarrow{\sim} \overline{S}^{-1}(A/\mathfrak{A})$.

Proof. (a) This is trivial.

(b) We have $A \longrightarrow A/\mathfrak{A} \longrightarrow \overline{S}^{-1}(A/\mathfrak{A})$. The elements of S become units in $\overline{S}^{-1}(A/\mathfrak{A})$. By the universal mapping property, we have the map $S^{-1}A \longrightarrow \overline{S}^{-1}(A/\mathfrak{A})$. This map is $a/s \mapsto \overline{a}/\overline{s}$; so, it is surjective. We have $\overline{a}/\overline{s} = 0$ in $\overline{S}^{-1}(A/\mathfrak{A})$ iff there is some $\overline{u} \in \overline{S}$ so that $\overline{u}\,\overline{a} = \overline{0}$ iff $a/1 \in \mathfrak{A}^e$ iff $a/s \in \mathfrak{A}^e$. Therefore, the kernel of our map is $\mathfrak{A}^e$, and so, $S^{-1}A/\mathfrak{A}^e \xrightarrow{\sim} \overline{S}^{-1}(A/\mathfrak{A})$. □

3.3 Prime and Maximal Ideals

Recall that an ideal, $\mathfrak{p}$, of $A \in \mathrm{CR}$ is a *prime ideal* iff $\mathfrak{p} \neq (1)$ and for all $a, b \in A$, if $ab \in \mathfrak{p}$, then one of $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ holds.

Proposition 3.8 *Given a commutative ring, A, for any ideal, $\mathfrak{A} \subseteq A$, the following are equivalent:*

(1) The ideal, $\mathfrak{A}$, is a prime ideal.

(2) The ring $A/\mathfrak{A}$ is an integral domain.

(3) The set $S = A - \mathfrak{A} =$ the complement of $\mathfrak{A}$ is a multiplicative subset of A.

(4) If $\mathfrak{B}$ and $\widetilde{\mathfrak{B}}$ are two ideals of A and if $\mathfrak{B}\widetilde{\mathfrak{B}} \subseteq \mathfrak{A}$, then one of $\mathfrak{B} \subseteq \mathfrak{A}$ or $\widetilde{\mathfrak{B}} \subseteq \mathfrak{A}$ holds.

(5) There is a ring, B, a homomorphism, $\varphi\colon A \to B$ and a maximal ideal, $\mathfrak{m}$, of B, so that $\varphi^{-1}(\mathfrak{m}) = \mathfrak{A}$.

(6) There is a multiplicative set, $S \subseteq A$, so that

(i) $\mathfrak{A} \cap S = \emptyset$ and

(ii) $\mathfrak{A}$ is maximal among the ideals having (i).

Proof. Equivalence of (1)–(4) is known and clear. Now, the inverse image of a prime ideal is *always* a prime ideal (DX). Every maximal ideal is prime, so it follows that (5) $\Rightarrow$ (1). Moreover, (1) implies (6) because take $S = A - \mathfrak{p}$. This is a multiplicative set by (3) and (6) follows tautologically.

(1) $\Rightarrow$ (5). Given a prime, $\mathfrak{A}$, let $S = A - \mathfrak{A}$, a multiplicative set by (3) and let $B = S^{-1}A$ and $\varphi = h$. We claim that $\mathfrak{A}^e$ is a maximal ideal of $S^{-1}A$. This is because $S^{-1}A/\mathfrak{A}^e \xrightarrow{\sim} \overline{S}^{-1}(A/\mathfrak{A})$, but $A/\mathfrak{A}$ is an integral domain and $\overline{S} =$ nonzero elements of $A/\mathfrak{A}$. Consequently, $\overline{S}^{-1}(A/\mathfrak{A}) = \mathrm{Frac}(A/\mathfrak{A})$ is a field; so, $\mathfrak{A}^e$ is a maximal ideal. Now, $h^{-1}(\mathfrak{A}^e) = \mathfrak{A}^{ec} = \bigcup_{v \in S}(v \longrightarrow \mathfrak{A})$. Now, $\xi \in (v \longrightarrow \mathfrak{A})$ iff $v\xi \in \mathfrak{A}$, where $v \notin \mathfrak{A}$. But, $\mathfrak{A}$ is prime, so $\xi \in \mathfrak{A}$. Therefore, $(v \longrightarrow \mathfrak{A}) = \mathfrak{A}$, for all $v \in S$; and so, $\mathfrak{A}^{ec} = h^{-1}(\mathfrak{A}^e) = \mathfrak{A}$ and (5) follows.

(6) $\Rightarrow$ (1). Given any $a, b \notin \mathfrak{A}$, we must show that $ab \notin \mathfrak{A}$. The hypotheses imply that $\mathfrak{A} + (a) > \mathfrak{A}$ and $\mathfrak{A} + (b) > \mathfrak{A}$, and by (6) (i) and (ii), we have $(\mathfrak{A} + (a)) \cap S \neq \emptyset$ and $(\mathfrak{A} + (b)) \cap S \neq \emptyset$. So, there are some $s, t \in S$, where $s = \alpha + \rho a$, $t = \beta + \sigma b$, with $\alpha, \beta \in \mathfrak{A}$, $\rho, \sigma \in A$. Since $st \in S$, it follows that

$$\alpha\beta + \rho a\beta + \sigma b\alpha + \rho\sigma(ab) \in S.$$

If $ab \in \mathfrak{A}$, then $st \in \mathfrak{A} \cap S$, a contradiction. Therefore, $ab \notin \mathfrak{A}$. □

Corollary 3.9 *Given any multiplicative set, S, in A, there exists a prime ideal, $\mathfrak{p}$, so that $\mathfrak{p} \cap S = \emptyset$.*

Proof. Look at $\mathcal{S} = \{\mathfrak{A} \mid \mathfrak{A} \text{ an ideal and } \mathfrak{A} \cap S = \emptyset\}$. We have $(0) \in \mathcal{S}$, partially order $\mathcal{S}$ by inclusion and check that $\mathcal{S}$ is inductive. By Zorn's lemma, $\mathcal{S}$ has some maximal element, $\mathfrak{p}$. By (6), the ideal $\mathfrak{p}$ is prime. □

Notation: If $S = A - \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal, write $A_{\mathfrak{p}}$ instead of $S^{-1}A$; the ring $A_{\mathfrak{p}}$ is called the *localization of A at $\mathfrak{p}$*. Recall that a *local ring* is a ring that has a unique maximal ideal.

Corollary 3.10 *For any prime ideal, $\mathfrak{p}$, in A, the ring $A_{\mathfrak{p}}$ is always a local ring and its maximal ideal is just $\mathfrak{p}^e$.*

Proof. Say $\mathfrak{A}$ is an ideal of A. Ideals of $A_{\mathfrak{p}} = S^{-1}A$ are extended ideals, i.e., they are of the form $\mathfrak{A}^e$. We have $\mathfrak{A}^e = (1)$ iff $\mathfrak{A} \cap S \neq \emptyset$ iff $\mathfrak{A} \not\subseteq \mathfrak{p}$. Thus, $\mathfrak{A}^e$ is a proper ideal iff $\mathfrak{A} \subseteq \mathfrak{p}$; the latter implies that $\mathfrak{A}^e \subseteq \mathfrak{p}^e$. So, $\mathfrak{p}^e$ is *the* maximal ideal of $A_{\mathfrak{p}}$, as contended. □

Remark: We have $\mathfrak{p}^{ec} = \mathfrak{p}$. We saw this above in the proof that (1) $\Rightarrow$ (5).

Proposition 3.11 *Let $A \in \mathrm{CR}$ be a commutative ring, S be a multiplicative set in A and let $\mathfrak{P}$ be a prime ideal of A. Then,*

(1) The ideal $\mathfrak{P}^e$ is a prime ideal of $S^{-1}A$ iff $\mathfrak{P}^e \neq (1)$ iff $\mathfrak{P} \cap S = \emptyset$.

(2) Every prime ideal of $S^{-1}A$ has the form $\mathfrak{P}^e$, for some prime ideal, $\mathfrak{P}$, of A.

(3) There is a one-to-one, inclusion-preserving, correspondence between the prime ideals of $S^{-1}A$ and the prime ideals, $\mathfrak{P}$, of A for which $\mathfrak{P} \cap S = \emptyset$.

When $S = A - \mathfrak{p}$ for some prime, $\mathfrak{p}$, of A, we have

(1′) The ideal $\mathfrak{P}^e$ is a prime of $A_\mathfrak{p}$ iff $\mathfrak{P}$ is a prime in A and $\mathfrak{P} \subseteq \mathfrak{p}$.

(2′) Every prime ideal of $A_\mathfrak{p}$ is $\mathfrak{P}^e$, for some prime, $\mathfrak{P}$, of A with $\mathfrak{P} \subseteq \mathfrak{p}$.

(3′) There is a one-to-one, inclusion-preserving, correspondence between all primes of $A_\mathfrak{p}$ and the primes of A contained in $\mathfrak{p}$.

Proof. (1) We know that $\mathfrak{P}^e \neq (1)$ iff $\mathfrak{P} \cap S = \emptyset$. By definition, a prime ideal is never equal to (1), so, all we must show is: If $\mathfrak{P}$ is prime in A, then $\mathfrak{P}^e$ is prime in $S^{-1}A$ (of course, $\mathfrak{P}^e \neq (1)$). Say $(\alpha/s)(\beta/t) \in \mathfrak{P}^e$. Then, $(\alpha\beta)/1 \in \mathfrak{P}^e$, and so, $\alpha\beta \in \mathfrak{P}^{ec}$. But, $\mathfrak{P}^{ec} = \bigcup_{v \in S}(v \longrightarrow \mathfrak{P})$ and $\xi \in (v \longrightarrow \mathfrak{P})$ iff $v\xi \in \mathfrak{P}$; moreover, $v \notin \mathfrak{P}$ since $\mathfrak{P} \cap S = \emptyset$, so, $\xi \in \mathfrak{P}$. Therefore, $\mathfrak{P}^{ec} = \mathfrak{P}$, and so, $\alpha\beta \in \mathfrak{P}$. Since $\mathfrak{P}$ is prime, either $\alpha \in \mathfrak{P}$ or $\beta \in \mathfrak{P}$; it follows that either $\alpha/s \in \mathfrak{P}^e$ or $\beta/t \in \mathfrak{P}^e$.

(2) If $\mathfrak{q}$ is a prime in $S^{-1}A$, then $\mathfrak{q} = \mathfrak{q}^{ce}$ and $\mathfrak{q}^c$ is a prime, as $\mathfrak{q}^c = h^{-1}(\mathfrak{q})$. Take $\mathfrak{P} = \mathfrak{q}^c$ to satisfy (2). Conversely, $\mathfrak{P}^e$ is prime iff $\mathfrak{P} \cap S = \emptyset$.

(3) follows from (1) and (2) and previous work.

Finally, (1′), (2′) and (3′) are special cases of (1), (2) and (3), respectively. □

Definition 3.2 If $\mathfrak{p}$ is a prime ideal of $A \in \mathrm{CR}$, look at chains of prime ideals

$$\mathfrak{p} = \mathfrak{p}_0 > \mathfrak{p}_1 > \cdots > \mathfrak{p}_n,$$

where each $\mathfrak{p}_j$ is prime ideal of A. Call n the *length* of this chain and define the *height of* $\mathfrak{p}$ by

$$\mathrm{ht}(\mathfrak{p}) = \sup\{\text{length of all chains } \mathfrak{p} = \mathfrak{p}_0 > \mathfrak{p}_1 > \cdots > \mathfrak{p}_n\}.$$

Observe that $\mathrm{ht}(\mathfrak{p})$ might be infinite. Since there is a one-to-one inclusion-preserving correspondence between the set of all primes, $\mathfrak{P}$, contained in $\mathfrak{p}$ and the set of all prime ideals of $A_\mathfrak{p}$, we get

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\text{maximal ideal of } A_\mathfrak{p}).$$

Definition 3.3 The *Krull dimension* of a commutative ring, A, denoted $\dim(A)$, is the supremum of the set $\{\mathrm{ht}(\mathfrak{m}) \mid \mathfrak{m} \text{ is a maximal ideal of } A\}$.

Hence, we see that $\mathrm{ht}(\mathfrak{p}) = \dim(A_\mathfrak{p})$, and

$$\dim(A) = \sup\{\dim(A_\mathfrak{m}) \mid \mathfrak{m} \text{ is a maximal ideal of } A\}.$$

Examples.

(1) Say $\dim(A) = 0$. This holds iff every prime ideal is maximal iff every maximal ideal is a minimal prime ideal. An example is a field, or $\mathbb{Z}/n\mathbb{Z}$.

(2) $\dim(A) = 1$. Here, A = a P.I.D. will do. For example, $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[T]$, more generally, $k[T]$, for any field, k. Also, $\mathbb{Z}[\sqrt{-5}]$, a non-P.I.D., has dimension 1.

(3) $\mathbb{C}[T_1, \ldots, T_n]$ has dimension n (this is not obvious, try it!) Given a commutative ring, A, for applications to algebraic geometry and number theory, it is useful to introduce two important sets, $\operatorname{Spec} A$ and $\operatorname{Max} A$, and to make these sets into topological spaces. Let

$$\begin{aligned} \operatorname{Spec} A &= \{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime ideal of } A\} \\ \operatorname{Max} A &= \{\mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal of } A\}. \end{aligned}$$

The set, $X = \operatorname{Spec} A$, is given a topology (the *Zariski topology* or *spectral topology*) for which a basis of open sets consists of the sets

$$X_f = \{\mathfrak{p} \in \operatorname{Spec} A \mid f \notin \mathfrak{p}\} \quad (f \in A),$$

and $\operatorname{Max} A \subseteq \operatorname{Spec} A$ is given the relative topology.

Remarks:

(1) $X_{f^n} = X_f$, for all $n \geq 1$. This is because $f^n \notin \mathfrak{p}$ iff $f \notin \mathfrak{p}$, as $\mathfrak{p}$ is prime.

(2) $X_{fg} = X_f \cap X_g$. This is because $\mathfrak{p} \in X_{fg}$ iff $fg \notin \mathfrak{p}$ iff $(f \notin \mathfrak{p})$ and $(g \notin \mathfrak{p})$.

(3) $X_f = \operatorname{Spec} A = X$ iff $f \notin \mathfrak{p}$, for every prime $\mathfrak{p}$ iff $f \in \mathbb{G}_m(A)$ iff $X_f = X_1$.

(4) $X_f = \emptyset$ iff $f \in \mathfrak{p}$, for all primes, $\mathfrak{p}$.

The open sets in $X = \operatorname{Spec} A$ are just the sets of the form $\bigcup_{f \in T} X_f$, for any subset, T, of A. So, a set, C, is closed in X iff it is of the form $C = \bigcap_T X_f^{\mathrm{c}}$, where

$$X_f^{\mathrm{c}} = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \notin X_f\} = \{\mathfrak{p} \in \operatorname{Spec} A \mid f \in \mathfrak{p}\} = \{\mathfrak{p} \in \operatorname{Spec} A \mid (f) \subseteq \mathfrak{p}\}.$$

Thus, $\mathfrak{p} \in C$ iff the ideal generated by the set T is contained in $\mathfrak{p}$. This suggests the following definition: For any ideal, $\mathfrak{A}$, in A, let

$$V(\mathfrak{A}) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supseteq \mathfrak{A}\}$$

be the *variety defined by* $\mathfrak{A}$. Then, we have

$$V(\mathfrak{A}) = \bigcap_{f \in \mathfrak{A}} X_f^{\mathrm{c}} = \bigcap \{X_f^{\mathrm{c}} \mid f \text{ is part of a generating set for } \mathfrak{A}\}.$$

The dual properties to (1)–(4) are:

(1′) $V(\mathfrak{A} \cap \mathfrak{B}) = V(\mathfrak{A}\mathfrak{B}) = V(\mathfrak{A}) \cup V(\mathfrak{B})$

(2′) $V(\sum_\alpha \mathfrak{A}_\alpha) = \bigcap_\alpha V(\mathfrak{A}_\alpha)$ $\quad$ ($\sum_\alpha \mathfrak{A}_\alpha$ = the ideal generated by the $\mathfrak{A}_\alpha$'s).

(3′) $V(\mathfrak{A}) = \emptyset$ iff $\mathfrak{A} = (1)$.

(4′) $V(\mathfrak{A}) = X = \operatorname{Spec} A$ iff $(\forall \mathfrak{p} \in \operatorname{Spec} A)(\mathfrak{A} \subseteq \mathfrak{p})$.

From now on, when we refer to $\operatorname{Spec} A$ and $\operatorname{Max} A$, we mean these as *topological spaces*.

To give a more informative criterion for (4) and (4′), we need to study $\mathcal{N}(A)$ = the *nilradical of* A, defined by

$$\mathcal{N}(A) = \{x \in A \mid x^n = 0, \text{ for some integer } n > 0\}.$$

This is an ideal of A. Indeed, if $x \in \mathcal{N}(A)$ and $y \in A$, since A is commutative, we have $(yx)^n = y^n x^n = 0$. Also, if $x, y \in \mathcal{N}(A)$, then there is some integer $n \geq 0$ so that $x^n = y^n = 0$, and by the binomial formula,

$$(x \pm y)^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} x^j (\pm 1)^{2n-j} y^{2n-j} = 0,$$

since $y^{2n-j} = 0$ if $j \leq n$ and $x^j = 0$ if $j \geq n$. Therefore, $x \pm y \in \mathcal{N}(A)$ and $\mathcal{N}(A)$ is an ideal.

More generally, if $\mathfrak{A}$ is an ideal, the *radical* of $\mathfrak{A}$, denoted $\sqrt{\mathfrak{A}}$, is

$$\sqrt{\mathfrak{A}} = \{x \in A \mid (\exists n \geq 0)(x^n \in \mathfrak{A})\}.$$

It is easy to check that $\sqrt{\mathfrak{A}}$ is an ideal and that $\mathfrak{A} \subseteq \sqrt{\mathfrak{A}}$. Note: $\sqrt{(0)} = \mathcal{N}(A)$.

That $\sqrt{\mathfrak{A}}$ is an ideal can also be seen as follows: Consider the projection map, $A \xrightarrow{\text{bar}} A/\mathfrak{A}$, and look at $\mathcal{N}(A/\mathfrak{A})$. Then, $\sqrt{\mathfrak{A}}$ is the inverse image of $\mathcal{N}(A/\mathfrak{A})$ under bar, and so, $\sqrt{\mathfrak{A}}$ is an ideal. Furthermore, by the first homomorphism theorem,

$$A/\sqrt{\mathfrak{A}} \cong (A/\mathfrak{A})/\mathcal{N}(A/\mathfrak{A}).$$

Observe that $A/\mathcal{N}(A)$ is a ring without nonzero nilpotent elements. Such a ring is called a *reduced ring* and $A/\mathcal{N}(A)$ is reduced. We write A_{red} for $A/\mathcal{N}(A)$. Note: $(A/\mathfrak{A})_{\text{red}} = A/\sqrt{\mathfrak{A}}$. For example, $(\mathbb{Z}/p^n\mathbb{Z})_{\text{red}} = \mathbb{Z}/p\mathbb{Z}$, for any prime p.

The following facts are easy to prove (DX):

(a) $\sqrt{\sqrt{\mathfrak{A}}} = \sqrt{\mathfrak{A}}$.

(b) $\sqrt{\mathfrak{A} \cap \mathfrak{B}} = \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}}$.

(c) If $\mathfrak{A}^k \subseteq \mathfrak{B}$, for some $k \geq 1$, then $\sqrt{\mathfrak{A}} \subseteq \sqrt{\mathfrak{B}}$.

There is another radical, the *Jacobson radical*, $\mathcal{J}(A)$, given by

$$\mathcal{J}(A) = \bigcap_{\mathfrak{m} \in \text{Max}(A)} \mathfrak{m}.$$

Proposition 3.12 *For any ring, $A \in$ CR, we have*

(1) $x \notin \mathbb{G}_m(A)$ iff there is some maximal ideal, $\mathfrak{m}$, so that $x \in \mathfrak{m}$.

(2) If $x \in \mathcal{J}(A)$, then $1 + x \in \mathbb{G}_m(A)$.

(3) $\mathcal{N}(A) = \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$; hence $\mathcal{N}(A) \subseteq \mathcal{J}(A)$.

Proof. (1) is clear (use Zorn's lemma).

(2) Assume $(1 + x) \notin \mathbb{G}_m(A)$. By (1), there is some $\mathfrak{m} \in \text{Max } A$, so that $1 + x \in \mathfrak{m}$. So, $x \notin \mathfrak{m}$ (else, $1 \in \mathfrak{m}$, a contradiction). As $\mathcal{J}(A)$ is contained in every maximal ideal, we get $x \notin \mathcal{J}(A)$.

(3) Suppose $x \in \mathcal{N}(A)$; then, $x^n = 0$, for some $n \geq 0$. Consequently, $x^n \in \mathfrak{p}$, for every prime $\mathfrak{p}$; so, $x \in \mathfrak{p}$, as $\mathfrak{p}$ is prime. Conversely, assume $x \in \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}$. Look at the set $S = \{x^n \mid n \geq 0\}$. Were S a multiplicative set, then there would be some prime ideal, $\mathfrak{p}$, with $\mathfrak{p} \cap S = \emptyset$. As $x \in \mathfrak{p}$, this is impossible. Therefore, S is not a multiplicative set, which happens iff x is nilpotent. □

Now, we can give the criteria for (4) and (4′).

(4) $X_f = \emptyset$ iff $f \in \mathcal{N}(A)$.

(4′) $V(\mathfrak{A}) = X = \operatorname{Spec} A$ iff $\mathfrak{A} \subseteq \mathcal{N}(A)$.

Corollary 3.13 *Given any ideal, $\mathfrak{A}$,*

$$\sqrt{\mathfrak{A}} = \bigcap\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supseteq \mathfrak{A}\} = \bigcap\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \in V(\mathfrak{A})\}.$$

Proof. There is a one-to-one correspondence between the set of prime ideals, $\mathfrak{p}$, containing $\mathfrak{A}$ and the set of prime ideals, $\overline{\mathfrak{p}}$, in $A/\mathfrak{A}$. So, $\bigcap\{\mathfrak{p} \mid \mathfrak{p} \supseteq \mathfrak{A}\}$ is the inverse image of $\mathcal{N}(A/\mathfrak{A})$, but this inverse image is $\sqrt{\mathfrak{A}}$. □

The minimal elements among primes, $\mathfrak{p}$, such that $\mathfrak{p} \supseteq \mathfrak{A}$ are called the *isolated primes* of $\mathfrak{A}$. Therefore,

$$\sqrt{\mathfrak{A}} = \bigcap\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \text{ is an isolated prime of } \mathfrak{A}\}.$$

Proposition 3.14 *The space $X = \operatorname{Spec} A$ is always quasi-compact (i.e., compact but not necessarily Hausdorff).*

Proof. Say $\bigcup_\alpha U_\alpha = X$ is an open cover of X. Each open U_α has the form $U_\alpha = \bigcup_\beta X_{f_\beta^{(\alpha)}}$. Therefore, we get an open cover $\bigcup_{\alpha,\beta} X_{f_\beta^{(\alpha)}} = X$. If we prove that this cover has a finite subcover, we are done (DX). The hypothesis implies that $\bigcap_{\alpha,\beta} X^{\mathrm{c}}_{f_\beta^{(\alpha)}} = \emptyset$. However the left hand side is $V((f_\beta^{(\alpha)}))$ and so $(f_\beta^{(\alpha)}) = (1)$, by previous work. We find

$$1 = c_{\alpha_1,\beta_1} f_{\beta_1}^{(\alpha_1)} + \cdots + c_{\alpha_s,\beta_s} f_{\beta_s}^{(\alpha_s)}, \quad \text{for some } c_{\alpha_j,\beta_j} \in A.$$

Thus, already, $(f_{\beta_j}^{(\alpha_j)})_{j=1}^s = (1)$, and so, $\bigcap_{j=1}^s X^{\mathrm{c}}_{f_{\beta_j}^{(\alpha_j)}} = \emptyset$. Thus, $\bigcup_{j=1}^s X_{f_{\beta_j}^{(\alpha_j)}} = X$, a finite cover. □

Remark: The space, $\operatorname{Spec} A$, is almost never Hausdorff. For example,
$\operatorname{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), (7), (11), \ldots\}$, and $\{(0)\}$ is dense in $\operatorname{Spec}(\mathbb{Z})$, i.e., every open set contains (0).

Another geometric example of $\operatorname{Spec} A$ and $\operatorname{Max} A$ is this:

Proposition 3.15 *Let X be a compact, Hausdorff space and write $A = \mathcal{C}(X)$ (the ring of real-valued (or complex-valued) continuous functions on X). For each $x \in X$, write $\mathfrak{m}_x = \{f \in A \mid f(x) = 0\}$. Then*

(1) Each $\mathfrak{m}_x$ is a maximal ideal of A and

(2) The map $x \mapsto \mathfrak{m}_x$ is a bijection of X with $\operatorname{Max} A$. (In fact, $x \mapsto \mathfrak{m}_x$ is a homeomorphism).

Proof. Note that the map $f \mapsto f(x)$ is a homomorphism of $\mathcal{C}(X)$ *onto* $\mathbb{R}$ (resp. $\mathbb{C}$). Its kernel is $\mathfrak{m}_x$, and so, $\mathfrak{m}_x$ is maximal. By Urysohn's lemma, if $x \neq y$, there is some continuous function, $f \in A$, so that $f(x) = 0$ and $f(y) = 1$. Thus, $f \in \mathfrak{m}_x$ and $f \notin \mathfrak{m}_y$; it follows that $\mathfrak{m}_x \neq \mathfrak{m}_y$; so, our map is an injection (of sets). Take any $\mathfrak{m}$ in $\operatorname{Max} A$. Say, $\mathfrak{m} \neq \mathfrak{m}_x$ for all $x \in X$. Given $x \in X$, since $\mathfrak{m} \neq \mathfrak{m}_x$, there is some $f_x \in \mathfrak{m}$ and $f_x \notin \mathfrak{m}_x$, Therefore, $f_x(x) \neq 0$. Since f is continuous, there is some open subset, U_x, with $x \in U_x$, and $f \restriction U_x \neq 0$. Then, the family $\{U_x\}$ is an open cover of X, and by compactness, it contains a finite subcover, say $\{U_{x_j}\}_{j=1}^t$. We have a function, $f_{x_j} \in \mathfrak{m}$, for each $j = 1, \ldots, t$. Let

$$F = \sum_{j=1}^t f_{x_j}^2 \quad \Big(F = \sum_{j=1}^t |f_{x_j}|^2, \quad \text{in the complex case}\Big).$$

Clearly, $F \geq 0$. Pick any $\xi \in X$. Then, there is some j, with $1 \leq j \leq t$, so that $\xi \in U_{x_j}$, and so, $f_{x_j}(\xi) \neq 0$. It follows that $F(\xi) > 0$. Thus, F is *never* zero on X; consequently, $1/F \in A$. But now, F is a unit and yet, $F \in \mathfrak{m}$, a contradiction. Therefore, the map $x \mapsto \mathfrak{m}_x$ is surjective. We leave the fact that it is a homeomorphism as a (DX). □

Here are some useful lemmas on primes.

Lemma 3.16 *If $\mathfrak{p}$ is a prime of A and $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ are some given ideals, then $\mathfrak{p} \supseteq \bigcap_{j=1}^t \mathfrak{A}_j$ iff $\mathfrak{p} \supseteq \mathfrak{A}_j$, for some j.*

Proof. ($\Leftarrow$). This is a tautology.

($\Rightarrow$). Observe that $\mathfrak{p} \supseteq \bigcap_{j=1}^t \mathfrak{A}_j \supseteq \prod_{j=1}^t \mathfrak{A}_j$, and since $\mathfrak{p}$ is prime, we must have $\mathfrak{p} \supseteq \mathfrak{A}_j$, for some j. □

Lemma 3.17 *(Prime avoidance lemma) Let $\mathfrak{A}$ be an ideal and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be some prime ideals. If $\mathfrak{A} \subseteq \bigcup_{j=1}^t \mathfrak{p}_j$, then $\mathfrak{A} \subseteq \mathfrak{p}_j$, for some j. (The lemma says that if $\mathfrak{A}$ avoids all the $\mathfrak{p}_j$, in the sense that $\mathfrak{A} \not\subseteq \mathfrak{p}_j$, then it avoids $\bigcup_{j=1}^t \mathfrak{p}_j$).*

Proof. We proceed by induction on t. The case $t = 1$ is obvious. Assume the induction hypothesis for $t < n$. Given n prime ideals, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, by the induction hypothesis, we may assume that $\mathfrak{A} \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$, for $i = 1, \ldots, n$. Since, by hypothesis, $\mathfrak{A} \subseteq \bigcup_{j=1}^n \mathfrak{p}_j$, for every $i = 1, \ldots, n$, there is some $x_i \in \mathfrak{A}$ with

$$x_i \in \mathfrak{p}_i \quad \text{and} \quad x_i \notin \mathfrak{p}_j, \quad \text{for all } j \neq i. \tag{$\dagger$}$$

Let k be given and form

$$y_k = x_1 \cdots x_{k-1} \widehat{x_k} x_{k+1} \cdots x_n,$$

where, as usual, the hat over x_k means that x_k is omitted. Then, $y_k \in \mathfrak{p}_i$, for all $i \neq k$. We claim that $y_k \notin \mathfrak{p}_k$. Indeed, were it not the case, then we would have $y_k = x_1 \cdots \widehat{x_k} \cdots x_n \in \mathfrak{p}_k$; since $\mathfrak{p}_k$ is prime, there would be some $x_j \in \mathfrak{p}_k$ for some $j \neq k$, a contradiction of ($\dagger$).

Of course, $y_k \in \mathfrak{A}$, for all k. Now, take $a = y_1 + \cdots + y_n$.

Claim. $a \notin \bigcup_{j=1}^n \mathfrak{p}_j$.

Suppose that $a \in \mathfrak{p}_k$, for some k. We can write

$$a = y_k + \sum_{j \neq k} y_j \in \mathfrak{p}_k, \tag{$*$}$$

and since we proved that $y_j \in \mathfrak{p}_k$ for all $j \neq k$, the fact that $a \in \mathfrak{p}_k$ implies that $y_k \in \mathfrak{p}_k$, a contradiction. □

Lemma 3.18 *Say $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals in A, then $S = A - \bigcup_{j=1}^n \mathfrak{p}_j$ is a multiplicative subset of A.*

Proof. We have $0 \notin S$ and $1 \in S$. Suppose that $s, t \in S$ and $st \notin S$. Then, $st \in \bigcup_{j=1}^n \mathfrak{p}_j$, and so, $st \in \mathfrak{p}_j$ for some j; as $\mathfrak{p}_j$ is prime, either $s \in \mathfrak{p}_j$ or $t \in \mathfrak{p}_j$, a contradiction. □

Now, I.S. Cohen (1950) showed that noetherian-ness of a ring is controlled by its prime ideals.

Lemma 3.19 *(Cohen, 1950) If $\mathfrak{A}$ is an ideal in a commutative ring, A, and if b is an element of A for which $\mathfrak{A} + (b)$ is f.g. and $(b \longrightarrow \mathfrak{A})$ is also f.g., then $\mathfrak{A}$ is f.g.*

Proof. Say $\mathfrak{A} + (b)$ is generated by $\beta_1, \ldots, \beta_t$. Each β_j is of the form $a_j + \rho_j b$, for some $a_j \in \mathfrak{A}$ and some $\rho_j \in A$. So, the elements $a_1, \ldots, a_t$ and b generate $\mathfrak{A} + (b)$. Let $c_1, \ldots, c_s$ generate $(b \longrightarrow \mathfrak{A})$. Then, $c_j b \in \mathfrak{A}$, for $j = 1, \ldots, s$.

We claim that the elements $a_1, \ldots, a_t, c_1 b, \ldots, c_s b$ generate $\mathfrak{A}$.

Pick $\alpha \in \mathfrak{A}$, then $\alpha \in \mathfrak{A} + (b)$, and so, $\alpha = \sum_{j=1}^t v_j a_j + \rho b$, with a_j as above, for $j = 1, \ldots, t$. But,

$$\rho b = \alpha - \sum_{j=1}^t v_j a_j \in \mathfrak{A},$$

and so, $\rho \in (b \longrightarrow \mathfrak{A})$. Consequently, we can write $\rho = \sum_{j=1}^s u_j c_j$, as the c_j's generate $(b \longrightarrow \mathfrak{A})$. It follows that

$$\alpha = \sum_{j=1}^t v_j a_j + \sum_{j=1}^s u_j (c_j b),$$

as contended. □

Proposition 3.20 *Let A be a commutative ring, then the following are equivalent:*

(1) A is noetherian (A has the ACC).

(2) Every ideal of A is f.g.

(3) A has the maximal condition on ideals.

(4) A has the ACC on f.g. ideals.

(5) (I.S. Cohen, 1950) Every prime ideal of A is f.g.

Proof. We already proved the equivalence (1)–(3) (c.f. Proposition 2.9). Obviously, (1) implies (4) and (2) implies (5).

(4) $\Rightarrow$ (1). Suppose

$$\mathfrak{A}_1 < \mathfrak{A}_2 < \mathfrak{A}_3 < \cdots$$

is a strictly ascending chain of ideals of A. By the axiom of choice, we can find a tuple, $(a_j)_{j=1}^{\infty}$, of elements in A so that $a_j \in \mathfrak{A}_j$ and $a_j \notin \mathfrak{A}_{j-1}$. Look at the ascending chain

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots \subseteq (a_1, \ldots, a_n) \subseteq \cdots .$$

This is a strictly ascending sequence, by the choice of the a_j's, a contradiction.

(5) $\Rightarrow$ (2). Take $\mathcal{F} = \{\mathfrak{A} \text{ an ideal of } A \mid \mathfrak{A} \text{ is not f.g.}\}$ and partially order $\mathcal{F}$ by inclusion. If $\mathcal{F}$ is not empty, it is inductive (DX). By Zorn's lemma, $\mathcal{F}$ has a some maximal element, $\mathfrak{A}$. Since $\mathfrak{A} \in \mathcal{F}$, it is not f.g. and by (5), the ideal $\mathfrak{A}$ is not prime. So, there exist $a, b \in A$ with $a, b \notin \mathfrak{A}$ and yet, $ab \in \mathfrak{A}$. Since $b \notin \mathfrak{A}$, we have $\mathfrak{A} + (b) > \mathfrak{A}$. Now, $a \in (b \longrightarrow \mathfrak{A})$ (since $ab \in \mathfrak{A}$), yet, $a \notin \mathfrak{A}$, and so, $(b \longrightarrow \mathfrak{A}) > \mathfrak{A}$. As $\mathfrak{A}$ is maximal in $\mathcal{F}$, it follows that both $\mathfrak{A} + (b)$ and $(b \longrightarrow \mathfrak{A})$ are f.g. By Cohen's lemma, the ideal $\mathfrak{A}$ is f.g., a contradiction. Therefore, $\mathcal{F} = \emptyset$, and (2) holds. $\square$

We now move back to modules. Given an A-module, M, we make the definition

Definition 3.4 The *support* of an A-module, M, denoted $\mathrm{Supp}(M)$ is that subset of $\mathrm{Spec}\, A$ given by

$$\mathrm{Supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}\, A \mid M_{\mathfrak{p}} \neq (0)\}.$$

Proposition 3.21 *If M is an A-module, then*

$$\mathrm{Supp}(M) \subseteq V((M \longrightarrow (0))) = V(\mathrm{Ann}(M)).$$

If M is f.g., then

$$\mathrm{Supp}(M) = V((M \longrightarrow (0))).$$

So, the support of a f.g. module is **closed** *in* $\mathrm{Spec}\, A$.

Proof. Pick $\mathfrak{p}$ in $\mathrm{Supp}(M)$, i.e., $M_{\mathfrak{p}} \neq (0)$. We need to show that $\mathfrak{p} \in V((M \longrightarrow (0)))$, i.e., $\mathfrak{p} \supseteq (M \longrightarrow (0))$. We will show that if $\mathfrak{p} \not\supseteq (M \longrightarrow (0))$ then $M_{\mathfrak{p}} = (0)$. But, $\mathfrak{p} \not\supseteq (M \longrightarrow (0))$ implies that there is some $s \notin \mathfrak{p}$ with $s \in (M \longrightarrow (0))$. In $M_{\mathfrak{p}}$,

$$\frac{s}{1}\frac{m}{t} = \frac{sm}{t} = 0, \quad \text{as } s \text{ kills } M$$

But, $s/1$ is a unit in $A_{\mathfrak{p}}$, and so, $m/t = 0$ already, and $M_{\mathfrak{p}} = (0)$.

Now, say M is f.g. with $m_1, \ldots, m_t$ as generators. Pick $\mathfrak{p} \in V((M \longrightarrow (0)))$, we need to show that $\mathfrak{p} \in \mathrm{Supp}(M)$. This means, if $\mathfrak{p} \supseteq \mathrm{Ann}(M)$, then $M_{\mathfrak{p}} \neq (0)$. We will prove that if $M_{\mathfrak{p}} = (0)$, then $\mathfrak{p} \not\supseteq \mathrm{Ann}(M)$.

If $M_{\mathfrak{p}} = (0)$, then $m/1 = 0$. So, there is some $s = s(m) \in S$ with $sm = 0$ in M. If we repeat this process for each of the $m_1, \ldots, m_t$ that generate M, we get $s_1, \ldots, s_t \in S$ such that $s_j m_j = 0$, for $j = 1, \ldots, t$. Write $\sigma = s_1 \cdots s_t \in S$. We get $\sigma m_j = 0$ for all $j = 1, \ldots, t$; so, $\sigma \in \mathrm{Ann}(M)$. But, $\sigma \in S$ implies that $\sigma \notin \mathfrak{p}$; consequently, $\mathfrak{p} \not\supseteq \mathrm{Ann}(M)$. $\square$

Proposition 3.22 *Say M is an A-module (where $A \in \mathrm{CR}$). Then, the following are equivalent:*

(1) $M = (0)$.

(2) $\mathrm{Supp}(M) = \emptyset$.

(2a) $M_{\mathfrak{p}} = (0)$, *for all* $\mathfrak{p} \in \mathrm{Spec}\, A$.

(3) $\mathrm{Supp}(M) \cap \mathrm{Max}\, A = \emptyset$.

(3a) $M_{\mathfrak{m}} = (0)$, *for all* $\mathfrak{m} \in \mathrm{Max}\, A$.

Proof. The implications (2) $\Leftrightarrow$ (2a) and (3) $\Leftrightarrow$ (3a) are obvious. Similarly, (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) are trivial. So, we need to show (3) $\Rightarrow$ (1). Let us first assume that M is f.g., Then, we know that $\mathrm{Supp}(M) = V((M \longrightarrow (0)))$. The hypothesis (3) implies that $\mathfrak{m} \supseteq (M \longrightarrow (0))$ for **no** maximal ideal, $\mathfrak{m}$. This implies that $(M \longrightarrow (0)) = (1)$, the unit ideal. Consequently, $1 \in (M \longrightarrow (0))$, and so, $M = (0)$.

Let us now consider the case where M is not f.g. We can write $M = \varinjlim_{\alpha} M_\alpha$, where the M_α's range over the f.g. submodules of M. Now, $M_\alpha \subseteq M$ and localization being exact, $(M_\alpha)_{\mathfrak{m}} \subseteq M_{\mathfrak{m}}$; so, $(M_\alpha)_{\mathfrak{m}} = (0)$ for all $\mathfrak{m} \in \mathrm{Max}\, A$. By the f.g. case, we get $M_\alpha = (0)$ for all α, and thus, $M = (0)$. □

Remark: The implication (3) $\Rightarrow$ (1) can also be proved without using right limits. Here is the proof. Assume $M \neq (0)$. Then, there is some $m \in M$ with $m \neq 0$, and let $\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$; we have $\mathrm{Ann}(m) \neq (1)$; so, $\mathrm{Ann}(m) \subseteq \mathfrak{m}$, for some maximal ideal, $\mathfrak{m}$. Consider $m/1 \in M_{\mathfrak{m}}$. Since $M_{\mathfrak{m}} = (0)$, we have $\lambda m = 0$, for some $\lambda \in A - \mathfrak{m}$; thus, $\lambda \in \mathrm{Ann}(m)$, and yet $\lambda \notin \mathfrak{m} \supseteq \mathrm{Ann}(m)$, a contradiction. Therefore, $M = (0)$. □

Corollary 3.23 *If $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$ is a given sequence of modules and maps, then it is exact iff for all $\mathfrak{p} \in \mathrm{Spec}\, A$, the sequence $M'_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M''_{\mathfrak{p}}$ is exact iff for all $\mathfrak{m} \in \mathrm{Max}\, A$, the sequence $M'_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \longrightarrow M''_{\mathfrak{m}}$ is exact.*

Proof. ($\Rightarrow$). This direction is trivial as localization is an exact functor.

Observe that we need only assume that the sequence $M'_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \longrightarrow M''_{\mathfrak{m}}$ is exact for all $\mathfrak{m} \in \mathrm{Max}\, A$. Then, $(\psi \circ \varphi)_{\mathfrak{m}} = \psi_{\mathfrak{m}} \circ \varphi_{\mathfrak{m}} = 0$; so if N is the image of the map $\psi \circ \varphi$, we find $N_{\mathfrak{m}} = (0)$, for all $\mathfrak{m} \in \mathrm{Max}\, A$. By Proposition 3.22, we get $N = (0)$, and thus $\psi \circ \varphi = 0$.

Let $H = \mathrm{Ker}\ \psi / \mathrm{Im}\ \varphi$. The same argument (using exactness of localization) shows that $H_{\mathfrak{m}} \cong (\mathrm{Ker}\ \psi)_{\mathfrak{m}} / (\mathrm{Im}\ \varphi)_{\mathfrak{m}} = (0)$. Again, Proposition 3.22 implies that $H = (0)$ and $\mathrm{Ker}\ \psi = \mathrm{Im}\ \varphi$, as contended. □

The statement is not that a whole family of local morphisms comes from a global morphism, rather we must have the global morphisms and then exactness is a local property.

Local Terminology: If P is property of A-modules (or morphisms), then a module (or morphism) is *locally P* iff for every $\mathfrak{p} \in \mathrm{Spec}\, A$, the module $M_{\mathfrak{p}}$ has P as $A_{\mathfrak{p}}$-module.[2]

Examples: Locally f.g., locally f.p., locally flat, locally exact, locally free, locally zero. etc.

Sometimes, you get a global result from an everywhere local result.

Proposition 3.24 *(Local flatness criterion) Say M is an A-module (where $A \in \mathrm{CR}$). Then, the following are equivalent:*

(1) M is flat over A.

[2]In reality, this ought to be called "pointwise P".

(2) M is locally flat.

(2a) For every $\mathfrak{p} \in \operatorname{Spec} A$, the module $M_{\mathfrak{p}}$ is flat over A.

(3) For every $\mathfrak{m} \in \operatorname{Max} A$, the module $M_{\mathfrak{m}}$ is flat over $A_{\mathfrak{m}}$.

(3a) For every $\mathfrak{m} \in \operatorname{Max} A$, the module $M_{\mathfrak{m}}$ is flat over A.

Proof. The implications (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) hold, the first by base extension and the second because it is a tautology. We shall prove that (3) $\Rightarrow$ (1) (and along the way, (3) $\Longleftrightarrow$ (3a) and hence, (2) $\Longleftrightarrow$ (2a)). Assume $0 \longrightarrow N' \longrightarrow N$ is exact. Tensoring with M, we get $N' \otimes_A M \longrightarrow N \otimes_A M$. Consider the exact sequence

$$0 \longrightarrow K \longrightarrow N' \otimes_A M \longrightarrow N \otimes_A M,$$

where $K = \operatorname{Ker}(N' \otimes_A M \longrightarrow N \otimes_A M)$. By localizing at $\mathfrak{m}$, we get the exact sequence

$$0 \longrightarrow K \otimes_A A_{\mathfrak{m}} \longrightarrow (N' \otimes_A M) \otimes_A A_{\mathfrak{m}} \longrightarrow (N \otimes_A M) \otimes_A A_{\mathfrak{m}}. \tag{$*$}$$

It follows that the sequence

$$0 \longrightarrow K_{\mathfrak{m}} \longrightarrow N' \otimes_A M_{\mathfrak{m}} \longrightarrow N \otimes_A M_{\mathfrak{m}} \quad \text{is exact.} \tag{$**$}$$

Now, for any module, L,

$$(L \otimes_A M) \otimes_A A_{\mathfrak{m}} \cong (L \otimes_A A_{\mathfrak{m}}) \otimes_{A_{\mathfrak{m}}} (M \otimes A_{\mathfrak{m}}) \cong L_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}},$$

and so, the sequence

$$0 \longrightarrow K_{\mathfrak{m}} \longrightarrow N'_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \quad \text{is also exact.} \tag{$\dagger$}$$

Since, the sequence $0 \longrightarrow N'_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ is exact and

(a) $M_{\mathfrak{m}}$ is $A_{\mathfrak{m}}$-flat; we find $K_{\mathfrak{m}} = (0)$.

(b) $M_{\mathfrak{m}}$ is A-flat; we find $K_{\mathfrak{m}} = (0)$, again.

But, the above holds for all $\mathfrak{m} \in \operatorname{Max} A$, and thus, $K = (0)$, as required. □

This method amounts to studying modules over the $A_{\mathfrak{p}}$'s and the latter are local rings, where matters are usually easier. The basic fact is Nakayama's lemma.

Lemma 3.25 *(Nakayama's lemma) Say A is a commutative ring and $\mathcal{J}(A)$ is its Jacobson radical. Suppose that M is a f.g. A-module and that $\mathcal{J}(A)M = M$. Then, $M = (0)$. That is, if $M \otimes_A (A/\mathcal{J}(A)) = (0)$, then $M = (0)$ (recall that $M \otimes_A (A/\mathcal{J}(A)) \cong M/(\mathcal{J}(A)M)$).*

Proof. Pick a generating set for M of least cardinality. If $M \neq (0)$, this set is nonempty. Write $m_1, \ldots, m_t$ for these generators. As $M = \mathcal{J}(A)M$, we can express $m_t \in M$ as $m_t = \sum_{j=1}^{t} \alpha_j m_j$, where $\alpha_j \in \mathcal{J}(A)$. Consequently,

$$(1 - \alpha_t)m_t = \sum_{j=1}^{t-1} \alpha_j m_j.$$

Now, $1 - \alpha_t \in \mathbb{G}_m(A)$, since $\alpha_t \in \mathcal{J}(A)$. Therefore, $m_t = \sum_{j=1}^{t-1} \alpha_j (1-\alpha_t)^{-1} m_j$, contradicting the minimality of t. □

Corollary 3.26 *(Classical Nakayama) Say A is a local ring and $\mathfrak{m}_A$ is its maximal ideal. Suppose that M is a f.g. A-module and that $\mathfrak{m}_A M = M$. Then, $M = (0)$.*

Corollary 3.27 *On the category of f.g. modules, $A/\mathcal{J}(A)$ is a faithful module. This means if $M \otimes_A (A/\mathcal{J}(A)) = (0)$, then $M = (0)$. (In the local ring case, if $M \otimes_A \kappa(A) = (0)$, then $M = (0)$, with $\kappa(A) = A/\mathfrak{m}_A$.)*

Corollary 3.28 *Let M be an f.g. A-module and say $m_1, \ldots, m_t \in M$ have residues $\overline{m_1}, \ldots, \overline{m_t}$ in $\overline{M} = M \otimes_A (A/\mathcal{J}(A)) \cong M/(\mathcal{J}(A)M)$ which generate $\overline{M}$. Then, $m_1, \ldots, m_t$ generate M.*

Proof. Let N be the submodule of M generated by $m_1, \ldots, m_t$. Look at $\overline{M}/\overline{N} = \overline{M/N}$. Since M is f.g., M/N is f.g. and $\overline{M/N} = \overline{M}/\overline{N} = (0)$. By Corollary 3.27, we get $M/N = (0)$, i.e., $M = N$. □

Corollary 3.29 *Let M be an f.g. A-module and let N be a submodule for which $N + \mathcal{J}(A)M = M$. Then, $N = M$.*

Proof. The hypothesis means $\overline{M} = \overline{N}$; so, $\overline{M/N} = (0)$. We conclude using Corollary 3.27, again. □

Corollary 3.30 *Let A be a local ring and M be a f.g. A-module. Write t for the minimal cardinality of a set of generators for M. Then*

(1) A set of elements $m_1, \ldots, m_r$ generate M iff $\overline{m_1}, \ldots, \overline{m_r}$ span the vector space $M \otimes_A \kappa(A)$.

(2) Every set of generators of M contains a subset generating M with exactly t elements.

The integer t is equal to $\dim_{\kappa(A)}(M \otimes_A \kappa(A))$.

Proof. (1) The implication ($\Rightarrow$) is clear and the implication ($\Leftarrow$) follows from Corollary 3.28.

(2) For vector spaces, each spanning set contains a basis; this implies that each generating set of M contains elements which pass to a basis. So, $t \geq d = \dim_{\kappa(A)}(M \otimes_A \kappa(A))$. As any basis of a vector space spans the vector space, Corollary 3.28 shows that M has a generating set of d elements, and so, $t \leq d$. Therefore, $t = d$. □

Proposition 3.31 *Let A be a local ring and M be an A-module. Assume one of*

(a) A is noetherian and M is f.g.

(b) M is f.p.

Then, the following are equivalent:

(1) M is free over A.

(2) M is projective over A.

(3) M is faithfully flat over A.

(4) M is flat over A.

Proof. The implications (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (4) and (1) $\Rightarrow$ (3), are already known (c.f. Remark (1) after Definition 2.4 for (1) $\Rightarrow$ (2) and c.f. Proposition 2.53 and Proposition 2.66 for (2) $\Rightarrow$ (4) and (1) $\Rightarrow$ (3)). We need only prove (4) $\Rightarrow$ (1). Hypothesis (b) follows from hypothesis (a), so, we assume that M is f.p. and flat. Pick a minimal set of generators for M, having say, having t generators. We have the exact sequence

$$0 \longrightarrow K \longrightarrow A^t \longrightarrow M \longrightarrow 0.$$

As M is f.p. and A^t is f.g., by Proposition 2.41 (or Proposition 2.17), we know that K is also f.g. Since M is flat, when we tensor with $\kappa(A)$, the sequence

$$0 \longrightarrow \overline{K} \longrightarrow \kappa(A)^t \xrightarrow{\Theta} \overline{M} \longrightarrow 0$$

remains exact (a Homework problem, but c.f. below). Since the vector spaces $\overline{M}$ and $\kappa(A)^t$ have the same dimension, Θ is an isomorphism. So, $\overline{K} = (0)$. Since K is f.g., by Nakayama's lemma, $K = (0)$. Therefore, $M \cong A^t$ and M is free over A. $\square$

Remark: For the sake of completeness, here is a proof of the fact referred to during the proof of the previous proposition.

Proposition 3.32 *Let Λ be a ring and consider the exact sequence of Λ-modules*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0. \qquad (*)$$

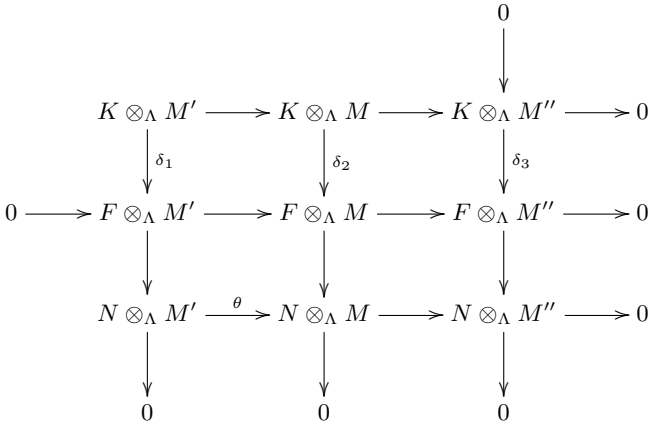
If M'' is flat, then for any Λ^{op}-module, N, the sequence

$$0 \longrightarrow N \otimes_\Lambda M' \longrightarrow N \otimes_\Lambda M \longrightarrow N \otimes_\Lambda M'' \longrightarrow 0 \quad \textit{is still exact.}$$

Proof. We can write N as a factor of some free Λ^{op}-module, F:

$$0 \longrightarrow K \longrightarrow F \longrightarrow N \longrightarrow 0. \qquad (**)$$

Then, by tensoring $(*)$ with K, F and N and by tensoring $(**)$ with M', M and M'' we obtain the following commutative diagram:



The second row is exact because F is free, and thus flat; the third column is exact because M'' is flat, and the other rows and columns are exact because tensor is right-exact. We need to prove that $\theta\colon N \otimes_\Lambda M' \to N \otimes_\Lambda M$ is injective. However, this follows from the snake lemma applied to the first two rows. $\square$

Theorem 3.33 *Let A be a commutative ring and M be an A-module. Assume one of*

(a) A is noetherian and M is f.g.

(b) M is f.p.

Then, the following are equivalent:

(1) M is projective over A.

(2) M is flat over A.

(3) M is locally free over A.

Proof. The implication (1) $\Rightarrow$ (2) is known (c.f. Proposition 2.53 and Proposition 2.66) and (2) $\Rightarrow$ (3) follows from Proposition 3.31. We need to prove (3) $\Rightarrow$ (1). Consider the functor $T\colon N \rightsquigarrow \mathrm{Hom}_A(M, N)$; we must show it is exact. Say

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0 \quad \text{is exact}$$

and apply T. We get

$$0 \longrightarrow \mathrm{Hom}_A(M, N') \longrightarrow \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M, N'') \longrightarrow C \longrightarrow 0, \qquad (\dagger)$$

where C is the cokernel of the map $\mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M, N'')$. We have the lemma (proved in the Problems):

Lemma 3.34 *If B is a flat A-algebra and M is a f.p. A-module, then the canonical map*

$$\mathrm{Hom}_A(M, N) \otimes_A B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$$

is an isomorphism.

Let $B = A_{\mathfrak{p}}$, for any $\mathfrak{p} \in \operatorname{Spec} A$. If we localize $(\dagger)$ at $\mathfrak{p}$, we get

$$0 \longrightarrow \mathrm{Hom}_A(M, N')_{\mathfrak{p}} \longrightarrow \mathrm{Hom}_A(M, N)_{\mathfrak{p}} \longrightarrow \mathrm{Hom}_A(M, N'')_{\mathfrak{p}} \longrightarrow C_{\mathfrak{p}} \longrightarrow 0,$$

and Lemma 3.34 implies, this is

$$0 \longrightarrow \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, N'_{\mathfrak{p}}) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}}) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, N''_{\mathfrak{p}}) \longrightarrow C_{\mathfrak{p}} \longrightarrow 0.$$

Yet, by (3), M is locally free, i.e., $M_{\mathfrak{p}}$ is free over $A_{\mathfrak{p}}$. So, $C_{\mathfrak{p}} = (0)$ (since $\mathrm{Hom}(F, -)$ is exact for F free). As $\mathfrak{p}$ is arbitrary, $C = (0)$. □

Proof of Lemma 3.34. Define the map $\theta\colon \mathrm{Hom}_A(M, N) \times B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$ by

$$\theta(f, b) = b(f \otimes \mathrm{id}_B), \quad \text{for all } f \in \mathrm{Hom}_A(M, N) \text{ and all } b \in B.$$

The map θ is clearly bilinear, so, it induces a canonical linear map

$$\Theta\colon \mathrm{Hom}_A(M, N) \otimes_A B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B).$$

Since M is an f.p. A-module, there is an exact sequence

$$\coprod_q A \longrightarrow \coprod_p A \longrightarrow M \longrightarrow 0,$$

for some integers $p, q \geq 0$. Since $\mathrm{Hom}_A(-, N)$ is a left-exact cofunctor, we get

$$0 \longrightarrow \mathrm{Hom}_A(M, N) \longrightarrow \prod_p \mathrm{Hom}_A(A, N) \longrightarrow \prod_q \mathrm{Hom}_A(A, N) \quad \text{is exact.}$$

Tensoring with B, since B is a flat A-algebra, we get

$$0 \longrightarrow \mathrm{Hom}_A(M, N) \otimes_A B \longrightarrow \prod_p \mathrm{Hom}_A(A, N) \otimes_A B \longrightarrow \prod_q \mathrm{Hom}_A(A, N) \otimes_A B \quad \text{is exact.}$$

Similarly, the sequence

$$\Big(\coprod_q A\Big) \otimes_A B \longrightarrow \Big(\coprod_p A\Big) \otimes_A B \longrightarrow M \otimes_A B \longrightarrow 0 \quad \text{is exact,}$$

i.e., the sequence

$$\coprod_q B \longrightarrow \coprod_p B \longrightarrow M \otimes_A B \longrightarrow 0 \quad \text{is exact,}$$

and since $\mathrm{Hom}_B(-, N \otimes_A B)$ is a left-exact cofunctor, we get

$$0 \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) \longrightarrow \prod_p \mathrm{Hom}_B(B, N \otimes_A B) \longrightarrow \prod_q \mathrm{Hom}_B(B, N \otimes_A B) \quad \text{is exact.}$$

Thus, we have the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_A(M, N) \otimes_A B & \longrightarrow & \prod_p \mathrm{Hom}_A(A, N) \otimes_A B & \longrightarrow & \prod_q \mathrm{Hom}_A(A, N) \otimes_A B \\
 & & \downarrow{\scriptstyle \Theta} & & \downarrow{\scriptstyle \Theta_p} & & \downarrow{\scriptstyle \Theta_q} \\
0 & \longrightarrow & \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) & \longrightarrow & \prod_p \mathrm{Hom}_B(B, N \otimes_A B) & \longrightarrow & \prod_q \mathrm{Hom}_B(B, N \otimes_A B).
\end{array}$$

But, clearly Θ_p and Θ_q are isomorphisms; so, the five lemma shows that Θ is an isomorphism. □

These results are wrong if M has no finiteness properties.

Take $A = \mathbb{Z}_{(p)} = \left\{ \frac{r}{s} \;\middle|\; (s,p) = 1 \right\}$ $(= \widehat{\mathbb{Z}_{(p)}} \cap \mathbb{Q})$; this is a local ring, in fact, a local P.I.D. Take $M = \mathbb{Q}$ as $\mathbb{Z}_{(p)}$-module. What is $\kappa(p) = \mathbb{Z}_{(p)}/\mathfrak{m}_p$, where $\mathfrak{m}_p = (p)^e = \left\{ \frac{r}{s} \;\middle|\; r \equiv 0 \,(\mathrm{mod}\, p),\ (s,p) = 1 \right\}$? We have $\mathbb{Z}_{(p)}/\mathfrak{m}_p$ is equal to the localization of $\mathbb{Z}/p\mathbb{Z}$, i.e., $\kappa(p) = \mathbb{Z}/p\mathbb{Z}$. How about $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p)$? We have a surjection $\mathbb{Q} \otimes_{\mathbb{Z}} \kappa(p) \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p)$. But, $\mathbb{Q} \otimes_{\mathbb{Z}} \kappa(p) = (0)$, so $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p) = (0)$. Therefore, $\kappa(p)$ is **not** faithful on $\mathbb{Q}$. Now, were $\mathbb{Q}$ free, then $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \kappa(p)$ would be a vector space of rank equal to $\mathrm{rk}(\mathbb{Q})$ over $\kappa(p)$. So, $\mathbb{Q}$ is not free over $\mathbb{Z}_{(p)}$. But $\mathbb{Q}$ is flat over $\mathbb{Z}_{(p)}$ as $\mathbb{Q}$ is $(\mathbb{Z}_{(p)})_{(0)}$ (the localization of $\mathbb{Z}_{(p)}$ at (0)). Note: $\mathbb{Q} = \varinjlim_n \mathbb{Z}_{(p)} \left[\frac{1}{p^n} \right]$.

Remarks on $M_\mathfrak{p}$, for any A module, M.

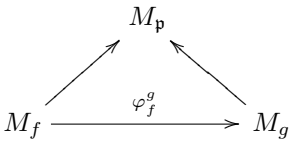
Let $S = A - \mathfrak{p}$, for a given $\mathfrak{p} \in \mathrm{Spec}\, A$. We can partially order S:

$$f \leq g \quad \text{iff} \quad f \mid g^n \quad \text{for some } n > 0,$$

i.e. iff there is some $\xi \in A$ with $f\xi = g^n$. (Note, $\xi \in S$, automatically). Check: This partial order has the Moore–Smith property. So, we can form $\varinjlim_{f \notin \mathfrak{p}} M_f$.

Claim: $\varinjlim_{f \notin \mathfrak{p}} M_f = M_\mathfrak{p}$.

We have maps $M_f \longrightarrow M_\mathfrak{p}$, for all f, and the commutative diagram



for all $f \leq g$. (Since $f \leq g$ iff $f\xi = g^n$ for some $\xi \in S$ and some $n > 0$, the map φ_f^g is given by $\varphi_f^g \left(\frac{m}{f^r} \right) = \frac{m\xi^r}{g^{nr}}$.) Check that φ_f^g is well-defined (DX). Hence, there exists a map $\varinjlim_{f \notin \mathfrak{p}} M_f \longrightarrow M_\mathfrak{p}$. To go backwards, pick $\xi \in M_\mathfrak{p}$. The element ξ is the class of some m/s, with $s \notin \mathfrak{p}$. Now, $m/s \in M_s$; hence, $\mathrm{can}_s(m/s) \in \varinjlim_{f \notin \mathfrak{p}} M_f$. Check that

(1) $\xi \mapsto \mathrm{can}_s(m/s)$ is well defined. It maps $M_\mathfrak{p} \longrightarrow \varinjlim_{f \notin \mathfrak{p}} M_f$.

(2) The map (1) and $\varinjlim_{f \notin \mathfrak{p}} M_f \longrightarrow M_\mathfrak{p}$ from above are mutually inverse.

Geometric Interpretation: We claim that $f \leq g$ iff $X_g \subseteq X_f$.

Indeed, $X_g \subseteq X_f$ iff $V((f)) \subseteq V((g))$ iff $\mathfrak{p} \supseteq (f)$ implies $\mathfrak{p} \supseteq (g)$ iff $\bigcap_{\mathfrak{p} \supseteq (f)} \mathfrak{p} \supseteq (g)$ iff $\sqrt{(f)} \supseteq (g)$ iff $\sqrt{(f)} \supseteq \sqrt{(g)}$. Now, $\sqrt{(f)} \supseteq \sqrt{(g)}$ iff $g \in \sqrt{(f)}$ iff $g^n \in (f)$ for some $n > 0$ iff $f \mid g^n$ iff $f \leq g$. This shows that $\varinjlim_{X_f \ni \mathfrak{p}} M_f = M_\mathfrak{p}$ and so, $M_\mathfrak{p}$ represents germs of some kind. We will come back and elucidate this point later. However, we want to note that for ideals, $\mathfrak{A}$ and $\mathfrak{B}$, the reasoning above shows that

$$V(\mathfrak{A}) \subseteq V(\mathfrak{B}) \quad \text{iff} \quad \sqrt{\mathfrak{A}} \supseteq \sqrt{\mathfrak{B}}.$$

Remark: The following proposition involving comaximal ideals will be needed in the next Chapter and is often handy.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring A are *comaximal* iff $\mathfrak{a}+\mathfrak{b}=A$. The following simple fact holds (DX): If $\mathfrak{a}, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$ are ideals so that $\mathfrak{a}$ and $\mathfrak{b}_i$ are comaximal for $i = 1, \ldots, n$, then $\mathfrak{a}$ and $\mathfrak{b}_1 \cdots \mathfrak{b}_n$ are comaximal.

Proposition 3.35 *(Chinese Remainder Theorem) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of a ring A. If for all $i \neq j$, the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are comaximal, then*

(1) The canonical map $\varphi\colon A \to \prod_{i=1}^n A/\mathfrak{a}_i$ is surjective.

(2) $\operatorname{Ker}\varphi = \bigcap_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{a}_i$.

Consequently, we have a canonical isomorphism

$$\psi\colon A\Big/\Big(\prod_{i=1}^n \mathfrak{a}_i\Big) \to \prod_{i=1}^n (A/\mathfrak{a}_i).$$

Moreover, the converse of (1) holds: If the canonical map $\varphi\colon A \to \prod_{i=1}^n A/\mathfrak{a}_i$ is surjective, then for all $i \neq j$, the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are comaximal.

Proof. We prove (1) and (2) together by induction on n. If $n = 2$, there exist $e_1 \in \mathfrak{a}_1$ and $e_2 \in \mathfrak{a}_2$ with $e_1 + e_2 = 1$. For any element $(\overline{a}_1, \overline{a}_2) \in A/\mathfrak{a}_1 \prod A/\mathfrak{a}_2$, let $a = e_2a_1 + e_1a_2$. Then,

$$\pi_i(a) = \pi_i(e_2a_1) + \pi_i(e_1a_2) = \overline{a}_i, \quad i = 1, 2$$

(where $\pi_i\colon A \to A/\mathfrak{a}_i$ is the canonical projection onto $A/\mathfrak{a}_i$). Thus, φ is surjective.

Since $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$, it is enough to prove that $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1\mathfrak{a}_2$. Now, as $1 = e_1 + e_2$, for every $a \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, we have $a = ae_1 + ae_2$; however, $ae_1 \in \mathfrak{a}_1\mathfrak{a}_2$ and $ae_2 \in \mathfrak{a}_1\mathfrak{a}_2$, so $a \in \mathfrak{a}_1\mathfrak{a}_2$. As $\operatorname{Ker}\varphi = \mathfrak{a}_1 \cap \mathfrak{a}_2$, we find $\operatorname{Ker}\varphi = \mathfrak{a}_1\mathfrak{a}_2$.

For the induction step, observe that (by the fact stated just before Proposition 3.35), $\mathfrak{b} = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}$ and $\mathfrak{a}_n$ are comaximal. Then, by the case $n = 2$, we have $\mathfrak{b} \cap \mathfrak{a}_n = \mathfrak{b}\mathfrak{a}_n$; moreover, by the induction hypothesis, $\mathfrak{b} = \bigcap_{i=1}^{n-1} \mathfrak{a}_i = \prod_{i=1}^{n-1} \mathfrak{a}_i$, so we have $\bigcap_{i=1}^{n} \mathfrak{a}_i = \prod_{i=1}^{n} \mathfrak{a}_i$.

By the case $n = 2$, we have an isomorphism

$$A/\mathfrak{b}\mathfrak{a}_n \cong (A/\mathfrak{b}) \prod (A/\mathfrak{a}_n)$$

and by the induction hypothesis, we have an isomorphism

$$A/\mathfrak{b} \cong \prod_{i=1}^{n-1} (A/\mathfrak{a}_i).$$

Therefore, we get an isomorphism

$$A\Big/\Big(\prod_{i=1}^n \mathfrak{a}_i\Big) \cong \prod_{i=1}^n A/\mathfrak{a}_i.$$

Finally, assume that the canonical map $\varphi\colon A \to \prod_{i=1}^n A/\mathfrak{a}_i$ is surjective. Pick i, j with $i \neq j$. By surjectivity, there is some $a \in A$ so that $\pi_i(a) = 0$ and $\pi_j(a) = 1$, i.e., $\pi_j(1 - a) = 0$. Therefore, $a \in \mathfrak{a}_i$ and $b = 1 - a \in \mathfrak{a}_j$ with $a + b = 1$, which proves $\mathfrak{a}_i + \mathfrak{a}_j = A$. □

The classical version of the Chinese Remainder Theorem is the case where $A = \mathbb{Z}$ and $\mathfrak{a}_i = m_i\mathbb{Z}$, where the $m_1, \ldots, m_n$ are pairwise relatively prime natural numbers. The theorem says that given any natural numbers $k_1, \ldots, k_n$, there is some natural number, q, so that

$$q \equiv k_i \pmod{m_i}, \quad i = 1, \ldots, n,$$

and the solution, q, is unique modulo $m_1m_2 \cdots m_n$.

Proposition 3.35 can be promoted to modules.

Proposition 3.36 *Let $M_1, \ldots, M_n$ be submodules of the A-module, M. Suppose the M_i are pairwise comaximal ($M_i + M_j = M$), then the natural map*

$$M \Big/ \Big(\bigcap_{i=1}^{n} M_i \Big) \longrightarrow \prod_{i=1}^{n} (M/M_i)$$

is an isomorphism. (Observe that, $M_i = \mathfrak{a}_i M$ with the $\mathfrak{a}_i$ comaximal ideals, is a special case.)

3.4 First Applications of Fraction Rings

A) **Rings with the DCC**

In this subsection, every ring is a commutative ring with unity.

Lemma 3.37 *If the ring A has the DCC, then* $\mathrm{Max}(A) = \mathrm{Spec}(A)$ *and* $\#(\mathrm{Max}(A))$ *is finite. Thus,* $\dim(A) = 0$.

Proof. Note, $\mathrm{Max}(A) = \mathrm{Spec}(A)$ iff $\dim(A) = 0$, in any commutative ring A. Pick $\mathfrak{p} \in \mathrm{Spec}(A)$ and look at $A/\mathfrak{p}$; the ring $A/\mathfrak{p}$ is a domain and it has the DCC. But, every integral domain with the DCC is a field and conversely. This is proved as follows: Say D is a domain with the DCC, and pick $x \neq 0$ in D. Look at the decreasing chain

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots \supseteq (x^n) \supseteq \cdots .$$

By the DCC, there is some n so that $(x^n) = (x^{n+1})$. Thus, $x^n \in (x^{n+1})$, and so, there is some $u \in D$ with $x^n = ux^{n+1}$. It follows that $x^n(1 - ux) = 0$; as $x \neq 0$ and D is a domain, we get $1 - ux = 0$, so, $x^{-1} = u$ and D is a field. Therefore, $\mathfrak{p}$ is maximal since $A/\mathfrak{p}$ is a field.

Let $\mathcal{S}$ be the set of finite intersections of distinct maximal ideals of A. Of course, $\mathcal{S} \neq \emptyset$, so, by the DCC, $\mathcal{S}$ has a minimal element, say $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n$. We claim that $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ are *all* the maximal ideals of A.

Take another maximal ideal, $\mathfrak{m}$, and look at $\mathfrak{m} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n$. This ideal is in $\mathcal{S}$ and

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n.$$

By minimality, we have

$$\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n \supseteq \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n.$$

As $\mathfrak{m}$ is prime, $\mathfrak{m} \supseteq \mathfrak{m}_j$, for some j; but both $\mathfrak{m}$ and $\mathfrak{m}_j$ are maximal, so $\mathfrak{m} = \mathfrak{m}_j$. □

Lemma 3.38 *If A is a noetherian ring, then every ideal, $\mathfrak{A}$, contains a product of prime ideals. In particular,* (0) *is a product of prime ideals.*

Proof. (Noetherian induction) Say the conclusion of the lemma is false and let $\mathcal{S}$ denote the collection of all ideals *not* containing a finite product of prime ideals. By assumption, $\mathcal{S} \neq \emptyset$. Since A is noetherian, $\mathcal{S}$ has a maximal element, $\mathfrak{A}$. The ideal $\mathfrak{A}$ can't be prime; so, there exist $a, b \notin \mathfrak{A}$ and yet, $ab \in \mathfrak{A}$. As $\mathfrak{A} + (a) > \mathfrak{A}$, we have $\mathfrak{A} + (a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, for some primes $\mathfrak{p}_i$. Similarly, $\mathfrak{A} + (b) \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$, for some primes $\mathfrak{q}_j$. Now, we have $\mathfrak{A} = \mathfrak{A} + (ab)$, since $ab \in \mathfrak{A}$; consequently, we get

$$\mathfrak{A} = \mathfrak{A} + (ab) \supseteq (\mathfrak{A} + (a))(\mathfrak{A} + (b)) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

a contradiction. Therefore, $\mathcal{S} = \emptyset$ and the lemma holds. □

Proposition 3.39 *(Akizuki, 1935) Say A is a local ring with the DCC. Then, the maximal ideal, $\mathfrak{m}$, of A is nilpotent (i.e., $\mathfrak{m}^n = (0)$ for some $n \geq 1$) and A is noetherian. The converse is also true.*

Proof. (Nagata) Consider the chain

$$\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots \supseteq \mathfrak{m}^n \supseteq \cdots ,$$

it must stop, by the DCC. Thus, there is some $n > 0$ so that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. Were $\mathfrak{m}^n \neq (0)$, the set $\mathcal{S} = \{\mathfrak{A} \mid \mathfrak{A}\mathfrak{m}^n \neq (0)\}$ would not be empty as $\mathfrak{m} \in \mathcal{S}$. By the DCC, the set $\mathcal{S}$ has a minimal element, call it $\mathfrak{A}$. Let $\mathfrak{p} = \mathrm{Ann}(\mathfrak{A}\mathfrak{m}^n)$. We claim that $\mathfrak{p}$ is a prime ideal. Pick $a, b \notin \mathfrak{p}$. Then, by definition of $\mathfrak{p}$, we have $a\mathfrak{A}\mathfrak{m}^n \neq (0)$ and $b\mathfrak{A}\mathfrak{m}^n \neq (0)$. Yet, $a\mathfrak{A} \subseteq \mathfrak{A}$ and $b\mathfrak{A} \subseteq \mathfrak{A}$ and $\mathfrak{A}$ is minimal in $\mathcal{S}$. Therefore,

$$a\mathfrak{A} = b\mathfrak{A} = \mathfrak{A}.$$

Now,

$$ab\mathfrak{A}\mathfrak{m}^n = a(b\mathfrak{A})\mathfrak{m}^n = (a\mathfrak{A})\mathfrak{m}^n = \mathfrak{A}\mathfrak{m}^n \neq (0),$$

and so, $ab \notin \mathfrak{p}$. Consequently, $\mathfrak{p}$ is indeed prime. By Lemma 3.37, the prime ideal, $\mathfrak{p}$, is maximal; as A is a local ring, we get $\mathfrak{m} = \mathfrak{p}$. As $\mathfrak{m} = \mathfrak{p} = \mathrm{Ann}(\mathfrak{A}\mathfrak{m}^n)$, we have $\mathfrak{m}\mathfrak{A}\mathfrak{m}^n = (0)$, so, $\mathfrak{A}\mathfrak{m}^{n+1} = (0)$, i.e., $\mathfrak{A}\mathfrak{m}^n = (0)$ (remember, $\mathfrak{m}^n = \mathfrak{m}^{n+1}$), a contradiction. Therefore, the maximal ideal, $\mathfrak{m}$, of A is nilpotent.

To prove A has the ACC, argue by induction on the least n so that $\mathfrak{m}^n = (0)$. When $n = 1$, we have $\mathfrak{m} = (0)$ and $A = \kappa(A)$ is a field. Since every field has the ACC, we are done. Assume that the induction hypothesis holds for all $r < n$. Consider the exact sequence

$$0 \longrightarrow \mathfrak{m}^{n-1}/\mathfrak{m}^n \,(= \mathfrak{m}^{n-1}) \longrightarrow A/\mathfrak{m}^n \,(= A) \longrightarrow A/\mathfrak{m}^{n-1} \longrightarrow 0.$$

The left hand term has the DCC and is a module over $A/\mathfrak{m} = \kappa(A)$; so, it is vector space over $\kappa(A)$ and it is finite dimensional. Consequently, it has the ACC, The righthand term has the ACC, by the induction hypothesis. It follows that the middle term, A, has the ACC.

Now, for the converse, assume that A is noetherian, local and that $\mathfrak{m}^n = (0)$ for some $n \geq 1$. We prove that A has the DCC by induction on the index of nilpotence of $\mathfrak{m}$. When $n = 1$, the ring $A = A/\mathfrak{m}$ is a field and so, it has the DCC. Assume that the induction hypothesis holds for all $r < n$. Say $\mathfrak{m}^n = (0)$. Then, we have the exact sequence

$$0 \longrightarrow \mathfrak{m}^{n-1}/\mathfrak{m}^n \,(= \mathfrak{m}^{n-1}) \longrightarrow A/\mathfrak{m}^n \,(= A) \longrightarrow A/\mathfrak{m}^{n-1} \longrightarrow 0,$$

where the righthand side has the DCC by the induction hypothesis. But, the left hand side is a module over $A/\mathfrak{m} = \kappa(A)$; so, it is vector space over $\kappa(A)$ and it has the ACC because A does. Thus, $\mathfrak{m}^{n-1}$ is a finite dimensional vector space, and so, it has the DCC. Therefore, A is caught between two DCC modules, and A is artinian. □

Theorem 3.40 *(Akizuki's structure theorem, 1935) If A is a commutative ring with unity, then A has the DCC iff A has the ACC and* $\mathrm{Max}(A) = \mathrm{Spec}(A)$ *(i.e.,* $\dim(A) = 0$*). When A has the DCC, the map*

$$\theta\colon A \to \prod_{\mathfrak{p}\in \mathrm{Spec}(A)} A_{\mathfrak{p}} \qquad (*)$$

is an isomorphism and each $A_{\mathfrak{p}}$ is an Artin local ring. Moreover, each map $h_{\mathfrak{p}}\colon A \to A_{\mathfrak{p}}$ is a surjection.

Proof. ($\Rightarrow$) By Lemma 3.37, we have $\mathrm{Max}(A) = \mathrm{Spec}(A)$ and $\mathrm{Max}(A)$ only has finitely many elements. Therefore, the product in $(*)$ is a finite product. Each $A_{\mathfrak{p}}$ is local with the DCC, so, it has the ACC (and its maximal ideal is nilpotent), by Proposition 3.39. If θ is an isomorphism, we are done with this part.

(1) The map θ is injective (this is true in general). Pick $a \in A$ and look at the principal ideal $(a) = Aa$. If $\theta(a) = 0$, then $(Aa)_{\mathfrak{p}} = (0)$ for every prime, $\mathfrak{p} \in \mathrm{Spec}(A)$. Therefore, $Aa = (0)$, so, $a = 0$.

(2) The map θ is surjective. The ideal $\mathfrak{p}^e$ in $A_{\mathfrak{p}}$ is nilpotent. So, $(\mathfrak{p}^e)^n = (0)$ in $A_{\mathfrak{p}}$, yet $(\mathfrak{p}^e)^n = (\mathfrak{p}^n)^e$, and thus,

$$A_{\mathfrak{p}} = A_{\mathfrak{p}}/(\mathfrak{p}^e)^n = A_{\mathfrak{p}}/(\mathfrak{p}^n)^e = (A/\mathfrak{p}^n)_{\overline{\mathfrak{p}}},$$

where $\overline{\mathfrak{p}}$ is the image of $\mathfrak{p}$ in $A/\mathfrak{p}^n$. Now, $\mathfrak{p}$ is the unique prime ideal of A which contains $\mathfrak{p}^n$ (since $\mathrm{Spec}(A) = \mathrm{Max}(A)$). Therefore, $A/\mathfrak{p}^n$ is a local ring and $\overline{\mathfrak{p}}$ is its maximal ideal. It follows that $(A/\mathfrak{p}^n)_{\overline{\mathfrak{p}}} = A/\mathfrak{p}^n$, and so $A_{\mathfrak{p}} \cong A/\mathfrak{p}^n$. Each $h_{\mathfrak{p}}$ is thereby a surjection. Since $\mathfrak{p}^{n_{\mathfrak{p}}}$ and $\mathfrak{q}^{n_{\mathfrak{q}}}$ are pairwise comaximal, which means that $(1) = \mathfrak{p}^{n_{\mathfrak{p}}} + \mathfrak{q}^{n_{\mathfrak{q}}}$ (because $\mathrm{Spec}(A) = \mathrm{Max}(A)$), the Chinese Remainder Theorem implies that θ is surjective.

($\Leftarrow$) This time, A has the ACC and $\mathrm{Max}(A) = \mathrm{Spec}(A)$. By Lemma 3.38, the ideal (0) is a product of maximal ideals, say $(0) = \prod_{j=1}^{t} \mathfrak{m}_j$. Let $\mathfrak{m}$ be any maximal ideal. Now $0 \in \mathfrak{m}$ implies that $\mathfrak{m} \supseteq \mathfrak{m}_j$, for some

j. Since both $\mathfrak{m}$ and $\mathfrak{m}_j$ are maximal, $\mathfrak{m} = \mathfrak{m}_j$. Thus, $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ are all the maximal ideals of A. Consider the descending chain

$$A \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_t = (0).$$

In this chain, we have $\mathfrak{m}_1 \cdots \mathfrak{m}_{s-1} \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_s$. The module $\mathfrak{m}_1 \cdots \mathfrak{m}_{s-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_s$ is an $A/\mathfrak{m}_s$-module, hence, a vector space, since $A/\mathfrak{m}_s$ is a field. By hypothesis, this vector space has the ACC. Thus, it is finite-dimensional and it has the DCC. But then, $\mathfrak{m}_1 \cdots \mathfrak{m}_{s-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_s$ has a composition series. If we do this for each s, we obtain a composition series for A. Consequently, A has finite length as A-module, so, it has the DCC. □

Remark: This is false for noncommutative rings. Take the ring R of $n \times n$ lower triangular matrices over $\mathbb{C}$. The "primes of R" are n in number and the localization at the j-th one, M_j, is the full ring of $j \times j$ matrices over $\mathbb{C}$. But, $\theta\colon R \to \prod_{j=1}^{n} M_j(\mathbb{C})$ is only injective, *not surjective*.

B) **Locally Free f.g. A-Modules**.

We begin by restating and reproving that $\mathrm{Supp}(M)$ is closed when M is f.g.

Lemma 3.41 *If M is a f.g. A-module and if $M_\mathfrak{p} = (0)$ for some $\mathfrak{p} \in \operatorname{Spec} A$, then there exists some $\sigma \notin \mathfrak{p}$ so that $\sigma M = (0)$ and $M_\sigma = (0)$.*

Proof. Write $m_1, \ldots . m_t$ for generators of M. Then, $m_j/1 = 0$ in $M_\mathfrak{p} = (0)$. So, there is some $s_j \notin \mathfrak{p}$ with $s_j m_j = 0$ for $j = 1, \ldots, t$. Let $\sigma = s_1 \cdots s_t$, then $\sigma m_j = 0$ for $j = 1, \ldots, t$. Consequently, $\sigma M = (0)$ and $m_j/1 = 0$ in M_σ for $j = 1, \ldots, t$, so, $M_\sigma = (0)$. □

Geometric Interpretation. If $\varphi\colon A \to B$ is a ring map we get a map, $\varphi^{\mathrm{a}}\colon \operatorname{Spec} B \to \operatorname{Spec} A$, namely, $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$. This is a continuous map (because $(\varphi^{\mathrm{a}})^{-1}(V(\mathfrak{A})) = V(B \cdot \varphi(\mathfrak{A}))$, for every ideal $\mathfrak{A} \subseteq A$). Since there is a map $A \longrightarrow A_s$, we get a map $\operatorname{Spec}(A_s) \longrightarrow \operatorname{Spec}(A)$. For this map we have

Proposition 3.42 *The map* $\operatorname{Spec}(A_s) \longrightarrow \operatorname{Spec}(A)$ *takes* $\operatorname{Spec}(A_s)$ *homeomorphically onto the open set, X_s, of* $\operatorname{Spec} A$.

Proof. We make a map $X_s \longrightarrow \operatorname{Spec}(A_s)$. For this, observe that $\mathfrak{p} \in X_s$ iff $s \notin \mathfrak{p}$ iff $\mathfrak{p}^e \in \operatorname{Spec}(A_s)$. Thus, the desired map is $\mathfrak{p} \mapsto \mathfrak{p}^e$. Now, $\mathfrak{q} = \mathfrak{p}^e$ iff $\mathfrak{p} = \mathfrak{q}^c$ = inverse image of $\mathfrak{q}$; therefore, our maps are inverse to one-another and the image of the contraction is X_s (an open set in $\operatorname{Spec} A$). We must now show that the map $X_s \longrightarrow \operatorname{Spec}(A_s)$ *via* $\mathfrak{p} \mapsto \mathfrak{p}^e$ is continuous. The open X_s has as basis of opens the $X_s \cap X_t = X_{st}$, where $t \in A$. The topology in $\operatorname{Spec}(A_s)$ has as basis the opens Y_τ, where $\tau \in A_s$ and $\mathfrak{q} \in Y_\tau$ iff $\tau \notin \mathfrak{q}$. We have $\tau = t/s^n$, for some t and some n. Moreover, $\mathfrak{q} = \mathfrak{p}^e$; so $\tau \notin \mathfrak{q}$ iff $t \notin \mathfrak{p}$ and it follows that $X_s \cap X_t$ corresponds to Y_τ. □

To continue with the 'geometric interpretation, let M be an A-module. We make a presheaf over $\operatorname{Spec} A$ from M, denote it by $\widetilde{M}$. For every open subset, U, in $X = \operatorname{Spec} A$,

$$\widetilde{M}(U) = \left\{ f\colon U \longrightarrow \bigcup_{\mathfrak{p} \in U} M_\mathfrak{p} \;\middle|\; \begin{array}{l} (1)\ f(\mathfrak{p}) \in M_\mathfrak{p} \\ (2)\ (\forall \mathfrak{p} \in U)(\exists m \in M, \exists s \in A)(s \notin \mathfrak{p}, \text{ i.e., } \mathfrak{p} \in X_s) \\ (3)\ (\forall \mathfrak{q} \in X_s \cap U)\left(f(\mathfrak{q}) = \text{image}\left(\tfrac{m}{s}\right) \text{ in } M_\mathfrak{q}\right). \end{array} \right\}$$

The intuition is that $\widetilde{M}(U)$ consists of kinds of functions ("sections") such that for every "point" $\mathfrak{p} \in U$, each function is locally defined in a consistent manner on a neighborhood $(X_s \cap U)$ of $\mathfrak{p}$ (in terms of some element $m \in M$).

The reader should prove that the presheaf, $\widetilde{M}$, is in fact a sheaf on $\operatorname{Spec} A$ (where $\operatorname{Spec} A$ has the Zariski topology) (DX).

Here are two important properties of the sheaf $\widetilde{M}$ (DX):

(1) $\widetilde{M}$ is an exact functor of M. This means, if

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence of A-modules, then

$$0 \longrightarrow \widetilde{M'} \longrightarrow \widetilde{M} \longrightarrow \widetilde{M''} \longrightarrow 0$$

is an exact sequence *of sheaves*. (Recall that if $\mathcal{F} \longrightarrow \mathcal{G}$ is a morphism of sheaves, it is surjective iff for every open, U, and every $\xi \in \mathcal{G}(U)$, there is a covering $\{U_\alpha \longrightarrow U\}_\alpha$ so that $\xi_\alpha = \rho_U^{U_\alpha}(\xi) \in \mathcal{G}(U_\alpha)$ comes from some $\eta_\alpha \in \mathcal{F}(U_\alpha)$ for all α.)

(2) The functor $M \rightsquigarrow \widetilde{M}$ commutes with arbitrary coproducts, i.e., if $M = \coprod_\alpha M_\alpha$, then $\widetilde{M} = \coprod_\alpha \widetilde{M}_\alpha$.

The easiest way to see (1) and (2) is *via* the following ideas: Say $\mathcal{F}$ is a presheaf on some space X. If $x \in X$ is a point, let $\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U)$. We call $\mathcal{F}_x$ the *stalk of the presheaf*, $\mathcal{F}$, at x.

Remark: The module, $M_\mathfrak{p}$, is the stalk of $\widetilde{M}$ at $\mathfrak{p}$. This is immediate from the definition (DX).

Proposition 3.43 *Say $\theta\colon \mathcal{F} \to \mathcal{G}$ is a map of sheaves (with values in a category based on sets, e.g., sets, groups, rings, ...) and suppose for all $x \in X$, the map $\theta_x\colon \mathcal{F}_x \to \mathcal{G}_x$ is injective (resp. surjective, bijective). Then θ is injective (resp. surjective, bijective). If $\mathcal{F}_x = (0)$ for all $x \in X$, then $\mathcal{F} = (0)$. (Here, $\mathcal{F}$ has values in groups or modules.)*

Proof. One checks that $\mathcal{F} \rightsquigarrow \mathcal{F}_x$ is an exact functor of $\mathcal{F}$ (for each $x \in X$). Then the last statement implies all the others. For example,

$$0 \longrightarrow \operatorname{Ker}\theta \longrightarrow \mathcal{F} \xrightarrow{\theta} \mathcal{G} \longrightarrow \operatorname{Coker}\theta \longrightarrow 0 \quad \text{is exact;}$$

so, take stalks at x. We get

$$0 \longrightarrow (\operatorname{Ker}\theta)_x \longrightarrow \mathcal{F}_x \xrightarrow{\theta_x} \mathcal{G}_x \longrightarrow (\operatorname{Coker}\theta)_x \longrightarrow 0 \quad \text{is exact.}$$

If θ_x is injective, then $(\operatorname{Ker}\theta)_x = (0)$. By the last statement of the proposition, $\operatorname{Ker}\theta = 0$, etc. So, we need to prove that $\mathcal{F}_x = (0)$ for all $x \in X$ implies that $\mathcal{F} = (0)$.

Pick an open, U, of X and pick any $x \in U$. We have $\mathcal{F}_x = \varinjlim_{V \ni x} \mathcal{F}(V)$ (with $V \subseteq U$). If $\xi \in \mathcal{F}(U)$, then ξ_x = image of ξ in $\mathcal{F}_x = 0$. This means that there is some open subset, $V = V_x$, with $\rho_U^V(\xi) = 0$ in $\mathcal{F}(V)$. Then, as x ranges over U, we have a cover, $\{V_x \longrightarrow U\}$, of U and $\rho_U^{V_x}(\xi) = 0$, for all V_x in the cover. By the uniqueness sheaf axiom, we must have $\xi = 0$. Since ξ is arbitrary in $\mathcal{F}(U)$, we get $\mathcal{F}(U) = (0)$. □

It is clear that the remark and this proposition imply (1) and (2) above.

As a special case of the tilde construction, if we view A has a module over itself, we can make the sheaf $\widetilde{A}$ on X, usually denoted $\mathcal{O}_X$. More explicitly, for every open subset, U, in $X = \operatorname{Spec} A$,

$$\mathcal{O}_X(U) = \left\{ f\colon U \longrightarrow \bigcup_{\mathfrak{p} \in U} A_\mathfrak{p} \;\middle|\; \begin{array}{l} (1)\ f(\mathfrak{p}) \in A_\mathfrak{p} \\ (2)\ (\forall \mathfrak{p} \in U)(\exists a, g \in A)(g \notin \mathfrak{p}, \text{ i.e., } \mathfrak{p} \in X_g) \\ (3)\ (\forall \mathfrak{q} \in X_g \cap U)\left(f(\mathfrak{q}) = \text{image}\left(\frac{a}{g}\right) \text{ in } A_\mathfrak{q}\right). \end{array} \right\}$$

Observe that $\mathcal{O}_X$ is a sheaf of local rings, which means that $\mathcal{O}_X(U)$ is a ring for all U and $\mathcal{O}_{X,\mathfrak{p}}$ $(= A_\mathfrak{p})$ is a local ring, for every $\mathfrak{p}$. The sheaf $\widetilde{M}$ is a sheaf of modules over $\mathcal{O}_X$.

Given a module M and an element $s \in A$, we have the sheaves $\widetilde{M} \restriction X_s$ and $\widetilde{M_s}$. Note that $\widetilde{M_s}$ is a sheaf on $\operatorname{Spec}(A_s)$ and $\widetilde{M} \restriction X_s$ is a sheaf on X_s, but the map $\operatorname{Spec}(A_s) \longrightarrow \operatorname{Spec} A$ gives a homeomorphism of $\operatorname{Spec}(A_s) \xrightarrow{\sim} X_s$.

Proposition 3.44 *Under the homeomorphism, $\varphi\colon \operatorname{Spec}(A_s) \widetilde{\longrightarrow} X_s$, the sheaves $\widetilde{M}_s$ and $\widetilde{M} \restriction X_s$ correspond.*

Proof. Say $\varphi\colon X \to Y$ is a continuous map of spaces and $\mathcal{F}$ is a sheaf on X. We can make $\varphi_*\mathcal{F}$, a new sheaf on Y, called the *direct image of* $\mathcal{F}$. For any open, V, in Y, set

$$\varphi_*\mathcal{F}(V) = \mathcal{F}(\varphi^{-1}(V)).$$

The sense of our proposition is that $\varphi_*(\widetilde{M}_s)$ and $\widetilde{M} \restriction X_s$ are isomorphic as sheaves on X_s. Now, $\varphi_*(\widetilde{M}_s)(U)$ is just $\widetilde{M}_s(\varphi^{-1}(U))$, where U is an open in $X_s \subseteq \operatorname{Spec} A$. The map $\varphi\colon Y = \operatorname{Spec} A_s \to X_s$ is just $\mathfrak{q} \in \operatorname{Spec}(A_s) \mapsto \mathfrak{q}^c \in \operatorname{Spec} A$. We have

$$\widetilde{M}_s(\varphi^{-1}(U)) = \left\{ f\colon \varphi^{-1}(U) \longrightarrow \bigcup_{\mathfrak{p}\in\varphi^{-1}(U)} (M_s)_{\mathfrak{p}} \;\middle|\; \begin{array}{l} (1)\ f(\mathfrak{p}) \in (M_s)_{\mathfrak{p}} \\ (2)\ (\forall \mathfrak{p} \in \varphi^{-1}(U))(\exists \mu \in M_s, \exists \tau \in A_s)(\mathfrak{p} \in Y_\tau) \\ (3)\ (\forall \mathfrak{q} \in Y_\tau \cap \varphi^{-1}(U))\left(f(\mathfrak{q}) = \text{image}\left(\tfrac{\mu}{\tau}\right) \text{ in } (M_s)_{\mathfrak{q}}\right). \end{array} \right\}$$

Now, $\mathfrak{q} \in \varphi^{-1}(U)$ iff $\mathfrak{q} = \mathfrak{p}^e$ and $\mathfrak{p} \in U \subseteq X_s$. We also have $\mu = m/s^n$, for some $m \in M$; $\tau = t/s^n$, for some $t \in A$, and so, $\mu/\tau = m/t$. It follows that there exists a natural map, $\widetilde{M} \restriction X_s(U) \longrightarrow \varphi_*(\widetilde{M}_s)(U)$, *via* f [given by m/t] $\mapsto f$ [given by $(m/s^n)/(t/s^n)$] $= \mu/\tau$.

This gives a map of sheaves, $\widetilde{M} \restriction X_s \longrightarrow \varphi_*(\widetilde{M}_s)$. We check that on stalks the map is an isomorphism: $(\widetilde{M} \restriction X_s)_{\mathfrak{p}} = M_{\mathfrak{p}}$ and $\varphi_*(\widetilde{M}_s)_{\mathfrak{q}} = (M_s)_{\mathfrak{q}} = (M_s)_{\mathfrak{p}^e} = M_{\mathfrak{p}}$. Therefore, our global map, being a stalkwise isomorphism, is an isomorphism. □

Recall that the stalk $(\widetilde{M})_{\mathfrak{p}}$ is just $M_{\mathfrak{p}}$. So,

$$M_{\mathfrak{p}} = \varinjlim_{f\notin\mathfrak{p}} M_f = \varinjlim_{\mathfrak{p}\in X_f} M_f = \varinjlim_{\mathfrak{p}\in X_f} \widetilde{M}(X_f).$$

Consequently, $M_{\mathfrak{p}}$ consists indeed of "germs"; these are the germs of "sections" of the sheaf $\widetilde{M}$. Thus, $A_{\mathfrak{p}} =$ germs of functions in $\mathcal{O}_X(U)$, for any $\mathfrak{p} \in U$.

Say X is an open ball in $\mathbb{R}^n$ or $\mathbb{C}^n$. Equip X with the sheaf of germs of C^k-functions on it, where $0 \le k \le \infty$ or $k = \omega$:

$$\mathcal{O}_X(U) = \left\{ f\colon U \longrightarrow \bigcup_{u\in U} \mathcal{O}_{X,u} \;\middle|\; \begin{array}{l} (1)\ f(u) \in \mathcal{O}_{X,u} \text{ (germs of } C^k\text{-functions at } u) \\ (2)\ (\forall u \in U)(\exists \text{ small open } X_\epsilon \subseteq U)(\exists\, C^k\text{-function, } g, \text{ on } X_\epsilon) \\ (3)\ (\forall u \in X_\epsilon)\,(f(u) = \text{image}(g) \text{ in } \mathcal{O}_{X,u}). \end{array} \right\}$$

For $\mathbb{C}^n$ and $k = \omega$, we can take g to be a power series converging on X_ϵ. Observe that $\mathcal{O}_X$ is a sheaf of local rings (i.e., $\mathcal{O}_{X,u}$(= germs at u) is a local ring).

The concept of a sheaf help us give a reasonable answer to the question, "what is geometry?"

A *local ringed space* (LRS) is a pair, $(X, \mathcal{O}_X)$, so that

(1) X is a topological space.

(2) $\mathcal{O}_X$ is a sheaf of local rings on X.

Examples.

(1) Open balls in $\mathbb{R}^n$ or $\mathbb{C}^n$, with the sheaf of germs of C^k functions, for a given k, are local ringed spaces.

(2) $(\operatorname{Spec} A, \widetilde{A})$ is an LRS.

The LRS's form a category, $\mathcal{LRS}$. A map $(X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ is a pair of maps, (φ, Φ), such that:

(a) $\varphi\colon X \to Y$ is a continuous map.

(b) $\Phi\colon \mathcal{O}_Y \to \varphi_*\mathcal{O}_X$ is a homomorphism of sheaves of rings.

Now, *geometry is the study of local ringed spaces that are locally standard*, i.e., each point $x \in X$ has a neighborhood, U, and the LRS $(U, \mathcal{O}_X \restriction U)$ is isomorphic to a standard model.

Some standard models:

(a) C^k, *real geometry (C^k-manifolds)*: The standards are open balls, U, in $\mathbb{R}^n$ and $\mathcal{O}_X(U)$ is the sheaf of germs of real C^k-functions on U. (Here, $1 \leq k \leq \infty$, and $k = \omega$ is also allowed).

(b) *Holomorphic geometry*: $k = \omega$. The standards are open balls, U, in $\mathbb{C}^n$ and $\mathcal{O}_X(U)$ is the sheaf of germs of complex C^ω-functions on U (complex holomorphic manifolds).

(c) *Algebraic geometry*: The standard model is $(\operatorname{Spec} A, \widetilde{A})$.

Notice that we can "glue together" standard models to make the geometric objects that are locally standard. Namely, given a family $\{(U_\alpha, \mathcal{O}_{U_\alpha})\}$, of standard models of fixed kind, suppose for all α, β, there exist some opens $U_\alpha^\beta \subseteq U_\alpha$ and $U_\beta^\alpha \subseteq U_\beta$ and isomorphisms $\varphi_\alpha^\beta\colon (U_\alpha^\beta, \mathcal{O}_{U_\alpha} \restriction U_\alpha^\beta) \to (U_\beta^\alpha, \mathcal{O}_{U_\beta} \restriction U_\beta^\alpha)$, and suppose we also have the gluing conditions: $\varphi_\alpha^\beta = (\varphi_\beta^\alpha)^{-1}$ and $\varphi_\alpha^\gamma = \varphi_\beta^\gamma \circ \varphi_\alpha^\beta$ on $U_\alpha \cap U_\beta$, then we can glue all the $(U_\alpha, \mathcal{O}_{U_\alpha})$ together. That is, there is an LRS, $(X, \mathcal{O}_X)$, and it is locally isomorphic to each $(U_\alpha, \mathcal{O}_{U_\alpha})$.

What about a geometric interpretation of some of our previous results?

Consider Lemma 3.41: Given a f.p. module, M, if $M_\mathfrak{p} = (0)$ for some $\mathfrak{p} \in \operatorname{Spec} A$, then there is some $s \notin \mathfrak{p}$ so that $M_s = (0)$ and $sM = (0)$.

Observe that $M_\mathfrak{p} = (0)$ iff $(\widetilde{M})_\mathfrak{p} = (0)$ iff the stalk of $\widetilde{M}$ at $\mathfrak{p}$ is (0). Moreover, $M_s = (0)$ iff $\widetilde{M}_s = (0)$ iff $\widetilde{M} \restriction X_s$ vanishes. So, Lemma 3.41 says that if the stalk of $\widetilde{M}$ vanishes punctually at $\mathfrak{p} \in \operatorname{Spec} A$, then $\widetilde{M}$ vanishes on some open subset, containing $\mathfrak{p}$, of $\operatorname{Spec} A$.

Proposition 3.45 *If A is a commutative ring and M is a f.g. A-module, assume one of*

(i) M is projective, or

(ii) A is noetherian and $M_\mathfrak{p}$ is free over $A_\mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} A$.

Then

(a) There exist $\sigma_1, \ldots, \sigma_t \in A$ so that M_{σ_j} is free over A_{σ_j} and $X = \operatorname{Spec} A = \bigcup_{j=1}^t X_{\sigma_j}$, or

(b) There is some $\sigma \in A$ with $\mathfrak{p} \in X_\sigma$ so that M_σ is free over A_σ.

Proof. We can write

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0,$$

for any f.g. module, M, with F f.g. and free. If M is projective, then the sequence splits. Therefore, K (being an image of F) is f.g., and so, M is f.p.

In (ii), the ring A is noetherian and M is f.g, which implies that M is f.p., here, too. Thus, we will assume that M is f.p. If we prove the (b) statement, then as a f.p. projective is locally free everywhere, the (b) conclusion holds everywhere on $\operatorname{Spec} A$. As $X = \operatorname{Spec} A$ is quasi-compact, we only need finitely many opens to cover X. Therefore, we only need prove (b).

There exists a free module and a map, $\theta\colon F \to M$, so that *at* $\mathfrak{p}$, we have $F_\mathfrak{p} \cong M_\mathfrak{p}$. The sequence

$$0 \longrightarrow \operatorname{Ker}\theta \longrightarrow F \longrightarrow M \longrightarrow \operatorname{Coker}\theta \longrightarrow 0 \quad \text{is exact.}$$

Now, Coker θ is f.g. and $(\text{Coker }\theta)_{\mathfrak{p}} = (0)$. So, there is some $s \in A$ with $(\text{Coker }\theta)_s = (0)$. If we restrict to $X_s \cong \text{Spec } A_s$, we get

$$0 \longrightarrow \text{Ker } \theta \longrightarrow F \longrightarrow M \longrightarrow \text{Coker } \theta \longrightarrow 0 \quad \text{is exact on } X_s.$$

By Proposition 2.41, as M is f.p. and F is f.g., we see that Ker θ is f.g. But, $(\text{Ker }\theta)_{\mathfrak{p}} = (0)$, and by the lemma, again, $(\text{Ker }\theta)_t = (0)$, for some $t \in A$. If we let $\sigma = st$, then $X_\sigma = X_s \cap X_t$, and on X_σ, we have an isomorphism $F_\sigma \xrightarrow{\sim} M_\sigma$. $\square$

Given an A-module, M, we can make the $\mathcal{O}_X$-module, $\widetilde{M}$. This is a sheaf of $\mathcal{O}_X$-modules. There exist index sets, I and J, so that

$$A^{(J)} \longrightarrow A^{(I)} \longrightarrow M \longrightarrow 0, \quad \text{is exact.}$$

(Here, $A^{(I)}$ is an abbreviation for the coproduct $\coprod_I A$.) So, we get

$$\mathcal{O}_X^{(J)} \longrightarrow \mathcal{O}_X^{(I)} \longrightarrow \widetilde{M} \longrightarrow 0,$$

an exact sequence of sheaves. Now, M is free iff $\widetilde{M} \cong \mathcal{O}_X^{(I)}$, for some I. We say that an $\mathcal{O}_X$-module, $\mathcal{F}$, is *locally-free* iff for every $\mathfrak{p} \in \text{Spec } A$, the module $\mathcal{F}_{\mathfrak{p}}$ is a free $\mathcal{O}_{X,\mathfrak{p}}$-module. Our proposition says: If $\mathcal{F} = \widetilde{M}$ and $\mathcal{F}$ is f.p. then $\mathcal{F}$ is projective[3] iff $\mathcal{F}$ is locally-free. One can characterize the $\mathcal{O}_X$-modules, $\mathcal{F}$, that are of the form $\widetilde{M}$ for some module, M; these are called *quasi-coherent $\mathcal{O}_X$-modules*.

We proved that if $\mathcal{F}_{\mathfrak{p}}$ is a free module of finite rank and if A is noetherian and $\mathcal{F}$ is quasi-coherent, then there is some open set, X_σ, with $\mathfrak{p} \in X_\sigma$, so that $\mathcal{F} \restriction X_\sigma = \mathcal{O}_X^n \restriction X_\sigma$. Actually, we only used f.p., so the statement also holds if $\mathcal{F}$ is projective (A not necessarily noetherian) and then it holds *everywhere* on *small* opens, U, so that

$$\mathcal{F} \restriction U = \mathcal{O}_X^{n(U)} \restriction U.$$

Let's assume that M is projective and f.g. over A. Define $\text{rk}(\widetilde{M}) = \text{rk}(\mathcal{F})$, a function from Spec A to $\mathbb{Z}$, by

$$(\text{rk}\,\mathcal{F})(\mathfrak{p}) = \text{rk}(\mathcal{F}_{\mathfrak{p}}).$$

We showed that this function is locally constant on Spec A, i.e., $\text{rk}\,\mathcal{F}$ is a continuous function from Spec A to $\mathbb{Z}$, where $\mathbb{Z}$ has the discrete topology. Hence, if Spec A is connected, then the rank is a constant.

Proposition 3.46 *Suppose M is a f.g. projective A-module (so, M is f.p.), and let $\mathcal{F} = \widetilde{M}$ on $X = \text{Spec } A$. Then, the function* rk$(\mathcal{F})$ *takes on only finitely many values, $n_1, \ldots, n_t$ (in $\mathbb{Z}$) and there exist ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ of A, each a commutative ring with unity, so that*

(a) $A = \prod_{j=1}^t \mathfrak{A}_j$; so $1 = e_1 + \cdots + e_t$, with the e_j's being orthogonal idempotents (which means that $e_i^2 = e_i$ and $e_i e_j = 0$ for $i \neq j$) and $\mathfrak{A}_j = Ae_j$.

(b) If X_{e_j} is the usual open corresponding to the element e_j, then $X = \bigcup_{j=1}^t X_{e_j}$.

(c) If $M_j = \mathfrak{A}_j M$, then $M = \coprod_{j=1}^t M_j$ and each M_j is A and $\mathfrak{A}_j$-projective.

(d) Supp $M_j = X_{e_j}$, *and* rk(M_j) *on X_{e_j} is the constant n_j.*

The following lemma is needed:

Lemma 3.47 *If $X = \text{Spec } A$ and $X = X_1 \bigcup X_2$ is a disconnection, then there exist $e_1, e_2 \in A$ so that $X_j = X_{e_j}$ and $1 = e_1 + e_2$; $e_1^2 = e_1$; $e_2^2 = e_2$; $e_1 e_2 = 0$.*

[3] In the full subcategory of the $\mathcal{O}_X$-modules consisting of those of the form $\widetilde{M}$.

Proof. (DX)

Proof of Proposition 3.46. Let $X_n = \mathrm{rk}(\mathcal{F})^{-1}(\{n\})$ for every $n \geq 0$. Each X_n is an open and closed subset of X, by continuity. The X_n cover X and by quasi-compactness only finitely many are necessary. Yet, they are mutually disjoint. It follows that $\mathrm{rk}(\mathcal{F}) = n_1, \ldots, n_t$ and $\mathrm{rk}(\mathcal{F}) \restriction X_j = n_j$. (Here, $X_j = X_{n_j}$.) By Lemma 3.47, there exist $e_1, \ldots, e_t$, orthogonal idempotents with sum 1 and $X_j = X_{e_j}$, for $j = 1, \ldots, t$. Let $\mathfrak{A}_j = Ae_j$, this is an ideal, a ring and $e_j \in \mathfrak{A}_j$ is its unit element. Thus, parts (a) and (b) are proved.

Write $M_j = \mathfrak{A}_j M$; then, $M = \coprod_{j=1}^{t} M_j$, each M_j is a cofactor of M and, as M is A-projective, each M_j is A-projective. The ring A acts on M *via* $\mathfrak{A}_j$; therefore, M_j is $\mathfrak{A}_j$-projective.

Pick any $\mathfrak{q} \in \operatorname{Spec} \mathfrak{A}_j$ and write $\mathfrak{p} = \mathfrak{q} \coprod_{i \neq j} \mathfrak{A}_i$. This ideal, $\mathfrak{p}$, is a prime ideal of A. Note, e_i with $i \neq j$ lies in $\mathfrak{p}$, but $e_j \notin \mathfrak{p}$, so $\mathfrak{p} \in X_j$. Since $e_i e_j = 0$, we also have $e_i e_j = 0$ in $A_\mathfrak{p}$. Yet, $e_j \notin \mathfrak{p}$, so e_j is a unit in $A_\mathfrak{p}$; it follows that $e_i = 0$ in $A_\mathfrak{p}$ for all $i \neq j$. Then, we have

$$M_\mathfrak{p} = \coprod_i (M_i)_\mathfrak{p} = \coprod_i (\mathfrak{A}_i M)_\mathfrak{p} = \coprod_i (Ae_i M)_\mathfrak{p} = (M_j)_\mathfrak{p}.$$

The reader should check that $(M_j)_\mathfrak{p} = (M_j)_\mathfrak{q}$. Since $\mathfrak{p} \in X_j$, we deduce that $(\mathrm{rk}\, M_j)(\mathfrak{q}) = (\mathrm{rk}\, M)(\mathfrak{p}) = n_j$, so, $(\mathrm{rk}\, M_j)(\mathfrak{q}) = n_j$. As $e_i = 0$ iff $i \neq j$ in $A_\mathfrak{p}$, we get $\mathrm{Supp}(M_j) = X_{e_j} = X_j$. □

The simplest case, therefore, is: the A-module M is f.g., projective and $\mathrm{rk}\, M \equiv 1$ on $X = \operatorname{Spec} A$. We say that M is an *invertible module* or a *line bundle* if we wish to view it geometrically.

Note: If M and M' are invertible, then $M \otimes_A M'$ is again a rank 1 projective A-module because $(M \otimes_A M')_\mathfrak{p} = M_\mathfrak{p} \otimes_{A_\mathfrak{p}} M'_\mathfrak{p}$. Thus, these modules form a semigroup under $\otimes_A$ and A (the free module) is the unit element. Do they form a group?

Proposition 3.48 *If A is a commutative ring and M is a f.g. A-module, then M is rank* 1 *projective iff there is another module, M', so that $M \otimes_A M' \cong A$. When the latter condition holds, we can take $M' = M^D = \mathrm{Hom}_A(M, A)$.*

Proof. ($\Longrightarrow$) The module M is rank 1 projective and as it is projective, it is f.p. Look at $M \otimes_A M^D$. There exists a module map,

$$M \otimes_A M^D \longrightarrow A,$$

namely, the linear map induced by the bilinear map $(m, f) \mapsto f(m)$. Localize at each $\mathfrak{p}$. We get

$$M_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}^D \longrightarrow A_\mathfrak{p},$$

and $M_\mathfrak{p}^D = \mathrm{Hom}_A(M, A)_\mathfrak{p} \xrightarrow{\sim} \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p})$, as M is f.p. and $A_\mathfrak{p}$ is flat over A. But, $M_\mathfrak{p} \cong A_\mathfrak{p}$, by hypothesis and the reader should check that $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}^D \longrightarrow A_\mathfrak{p}$ is an isomorphism. As this holds for every $\mathfrak{p} \in \operatorname{Spec} A$, the map $M \otimes_A M^D \longrightarrow A$ is an isomorphism.

($\Longleftarrow$) Now, we have some A-module, M', and $M \otimes_A M' \cong A$. We can write

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0,$$

for some f.g. free module, F. Look at the last three terms in this sequence, and write $F = \coprod_{\text{finite}} A$:

$$\coprod_{\text{finite}} A \longrightarrow M \longrightarrow 0.$$

If we tensor with M', we get

$$\coprod_{\text{finite}} M' \longrightarrow M \otimes_A M' \cong A \longrightarrow 0.$$

But A is free, so the sequence splits and there is a map $A \longrightarrow \coprod_{\text{finite}} M'$. Now, tensor with M. We get

$$\coprod_{\text{finite}} A \longrightarrow M \longrightarrow 0,$$

and there is a splitting map $M \longrightarrow \coprod_{\text{finite}} A$. Thus, M is a cofactor of a free and f.g. module, so, M is f.g. and projective, and hence, f.p. Now look at

$$M \otimes_A M' \cong A$$

and localize at $\mathfrak{p}$. We get

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M'_{\mathfrak{p}} \cong A_{\mathfrak{p}},$$

and if we reduce mod $\mathfrak{p}^e$, we get

$$M_{\mathfrak{p}}/\mathfrak{p}^e M_{\mathfrak{p}} \otimes_{\kappa(A_{\mathfrak{p}})} M'_{\mathfrak{p}}/\mathfrak{p}^e M'_{\mathfrak{p}} \cong \kappa(A_{\mathfrak{p}}). \tag{$\dagger$}$$

All the modules in ($\dagger$) are vector spaces and, by counting dimensions, we get

$$\dim_{\kappa(A_{\mathfrak{p}})} M_{\mathfrak{p}}/\mathfrak{p}^e M_{\mathfrak{p}} = 1.$$

Since $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module, by Nakayama, we get $\mathrm{rk}(M_{\mathfrak{p}}) = 1$. Lastly,

$$M' \cong A \otimes_A M' \cong (M^D \otimes_A M) \otimes_A M' \cong M^D \otimes_A (M \otimes_A M') \cong M^D \otimes_A A \cong M^D.$$

Therefore, $M' \cong M^D$. □

The group of (isomorphism classes) of the rank 1 projectives, M, is called the *Picard group* of A, denoted $\mathrm{Pic}(A)$.

Corollary 3.49 *If k is a field or a PID, then* $\mathrm{Pic}(A) = (0)$.

The group $\mathrm{Pic}(A)$ is a subtle invariant of a ring (generally hard to compute).

3.5 Integral Dependence

The notion of integral dependence first arose in number theory; later, thanks to Zariski, it found application in algebraic geometry. Throughout this section as throughout this chapter, all rings are commutative with unity.

Definition 3.5 Suppose $\varphi\colon A \to B$ is a ring homomorphism and $b \in B$. The element, b, is *integral over* A iff there is a non-trivial **monic** polynomial, $f(X) \in A[X]$, so that $f(b) = 0$. (Here, $f(b)$ is $b^n + \varphi(a_1)b^{n-1} + \cdots + \varphi(a_{n-1})b + \varphi(a_n)$ if $f(X)$ is $X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$.) The A-algebra B is *integral over* A iff all its elements are integral over A and, in this case, φ is an *integral morphism*.

Clearly, each ring surjection is an integral morphism, but this is not what is really intended. Each homomorphism, φ, as above factors into a surjection whose image, $\widetilde{A}$, is a subring of B followed by the inclusion $\widetilde{A} \hookrightarrow B$. It is for inclusions that integrality is a real question and is decisive for certain situations. As usual, there are a number of equivalent ways to say integrality and their equivalence is quite useful technically.

Proposition 3.50 *Suppose $\varphi\colon A \to B$ is a ring homomorphism and $b \in B$. Then the following are equivalent conditions:*

(1) b is integral over A

(2) The A-algebra $A[b]$ (a sub-A-algebra of B) is finitely generated as A-module.

(3) There exists a sub-A-algebra, $\widetilde{B}$, of B which is a finitely generated A-module and $b \in \widetilde{B}$.

(4) There exists a finitely generated sub-A-module, $\widetilde{B}$, of B so that α) $b\widetilde{B} \subseteq \widetilde{B}$ and β) $\widetilde{A}[b] \cap \mathrm{Ann}(\widetilde{B}) = (0)$.

Proof. (1) $\Longrightarrow$ (2). We have the equation of integral dependence

$$b^n + a_1b^{n-1} + \cdots + a_{n-1}b + a_n = 0$$

(here, we drop $\varphi(a_j)$ and just denote it by a_j). Hence, $b^n \in A$-module generated by $1, b, \ldots, b^{n-1}$. But then, b^{n+1} is also in this A-module, etc. Thus, $A[b]$ is the finitely generated A-module given by generators $1, b, \ldots, b^{n-1}$.

(2) $\Longrightarrow$ (3). We take $\widetilde{B} = A[b]$.

(3) $\Longrightarrow$ (4). We use our subalgebra, $\widetilde{B}$, of (3) for the module of (4). Of course, α) holds as $\widetilde{B}$ is a ring by (3) and β) is clear as $a \in \widetilde{B}$.

(4) $\Longrightarrow$ (1). Let $\xi_1, \ldots, \xi_t$ be generators for $\widetilde{B}$ as A-module. Since $b\widetilde{B} \subseteq \widetilde{B}$, we see that for each i, the element $b\xi_i$ is an A-linear combination of the ξ's:

$$b\xi_i = \sum_{j=1}^{t} z_{ij}\xi_j.$$

That is,

$$\sum_{j=1}^{t} (\delta_{ij}b - z_{ij})\xi_j = 0, \quad \text{for } i = 1, 2, \ldots, t. \tag{$*$}$$

Write Δ for $\det(\delta_{ij}b - z_{ij})$, then by linear algebra we get $\Delta\xi_j = 0$ for all j, i.e., $\Delta \in \mathrm{Ann}(\widetilde{B})$. Upon expanding Δ by minors, we find that $\Delta \in \widetilde{A}[b]$; so, β) implies $\Delta = 0$. But the expansion by minors shows Δ has the form $b^t +$ lower powers of b and this gives (1). $\square$

There are many corollaries, but first notice that *if A is noetherian, we may replace (3) by the weaker condition*

($3'$) There is a finitely generated sub-A-**module**, $\widetilde{B}$, of B and $A[b] \subseteq \widetilde{B}$.

Let's write

$$\mathrm{Int}_A(B) = \{b \in B \mid b \text{ is integral over } A\}$$

and refer to $\mathrm{Int}_A(B)$ as the *integral closure of A in B* (we assume φ is given *a priori*).

Corollary 3.51 *Say A and B are given as above and $b_1, \ldots, b_t$ are elements of B. Then, $b_1, \ldots b_t \in \mathrm{Int}_A(B)$ iff the A-algebra $A[b_1, \ldots, b_t]$ is a finitely generated A-module. In particular, $\mathrm{Int}_A(B)$ is a A-algebra.*

Proof. ($\Longleftarrow$). Here, $A[b_j] \subseteq A[b_1, \ldots, b_t]$ and we apply (3) of Proposition 3.50 to get $b_j \in \mathrm{Int}_A(B)$.

($\Longrightarrow$). We have the chain of A-algebras

$$A[b_1, \ldots, b_t] \supseteq \cdots \supseteq A[b_1] \supseteq \widetilde{A}$$

each a finite module over its predecessor by (2) of Proposition 3.50. Then, it is clear that $A[b_1, \ldots, b_t]$ is a finite A-module. Lastly, if $x, y \in \mathrm{Int}_A(B)$, we see that $x \pm y$ and xy lie in $A[x, y]$. By the above, the latter is a finite A-module and (3) of Proposition 3.50 completes the proof. □

Corollary 3.52 *(Transitivity of Integral Dependence) Suppose that B is an A-algebra and C is a B-algebra. Then,*

$$\mathrm{Int}_{\mathrm{Int}_A(B)}(C) = \mathrm{Int}_A(C).$$

In particular, if C is integral over B and B is integral over A, then C is integral over A.

Proof. If $\xi \in C$ and ξ is integral over A, then ξ is *a fortiori* integral over the "bigger' ring $\mathrm{Int}_A(B)$, and so

$$\mathrm{Int}_A(C) \subseteq \mathrm{Int}_{\mathrm{Int}_A(B)}(C).$$

Now, if ξ is integral over $\mathrm{Int}_A(B)$, then ξ is integral over $A[b_1, \ldots, b_t]$ where the b_i are coefficients in the polynomial of integral dependence for ξ. Each b_i is in $\mathrm{Int}_A(B)$, so Corollary 3.51 shows $A[b_1, \ldots, b_t]$ is a finite A-module. Yet $A[b_1, \ldots, b_t][\xi]$ is a finite $A[b_1, \ldots, b_t]$-module by integrality of ξ. Therefore ξ is in the finitely generated A-module $A[b_1, \ldots, b_t, \xi]$ which is an A-algebra and we apply (3) of Proposition 3.50. The element ξ is then in $\mathrm{Int}_A(C)$, as required.

When C is integral over B and B is integral over A, we get $C = \mathrm{Int}_B(C)$ and $B = \mathrm{Int}_A(B)$; so $C = \mathrm{Int}_A(C)$ by the above. □

When $\mathrm{Int}_A(B)$ is $\widetilde{A}$ (image of A in B) itself, we say A *is integrally closed in B*. (Usually, for this terminology, one assume φ is an inclusion $A \hookrightarrow B$.) If S is the set of non-zero divisors of A, then S is a multiplicative set and $S^{-1}A$ is the *total fraction ring of A*. We denote it by $\mathrm{Frac}(A)$. When A in integrally closed in $\mathrm{Frac}(A)$, we call A a *normal ring* or an *integrally closed ring*. For example

Proposition 3.53 *Every unique factorization domain is a normal ring.*

Proof. We suppose A is a UFD, write $K = \mathrm{Frac}(A)$ (in this case K is a field as A is a domain). Let $\xi = \alpha/\beta$ be integral over A, and put α/β in lowest terms. Then,

$$\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n = 0, \quad \text{the } a_j \in A.$$

Insert the value of ξ ($= \alpha/\beta$) and clear denominators. We get

$$\alpha^n + a_1\alpha^{n-1}\beta + \cdots + a_{n-1}\alpha\beta^{n-1} + a_n\beta^n = 0.$$

If p is a prime element of A and p divides β, our equation shows $p \mid \alpha^n$; i.e., $p \mid \alpha$. This is a contradiction on lowest terms and so no p divides β. This means β is a unit; so, $\xi \in A$. □

Proposition 3.54 *If A is a normal domain and S is any multiplicative subset of A, then $S^{-1}A$ is also a normal domain.*

Proof. We know $\mathrm{Frac}(A) = \mathrm{Frac}(S^{-1}A)$. So, choose $\xi \in \mathrm{Frac}(A)$ integral over $S^{-1}A$. Then,

$$\xi^n + \frac{a_1}{s_1}\xi^{n-1} + \cdots + \frac{a_{n-1}}{s_{n-1}}\xi + \frac{a_n}{s_n} = 0.$$

We can write this with common denominator $s = \prod s_j$, then

$$\xi^n + \frac{a_1}{s}\xi^{n-1} + \cdots + \frac{a_{n-1}}{s}\xi + \frac{a_n}{s} = 0.$$

Upon multiplication by s^n, we find $(s\xi)$ is integral over A. By hypothesis, $s\xi \in A$; so, $\xi \in S^{-1}A$. □

Two easy facts are useful to know. Their proof are easy and will be left to the reader (DX):

Fact A. If B is integral over A and $\mathfrak{I}$ is any ideal of B, then $B/\mathfrak{I}$ is integral over $A/\varphi^{-1}(\mathfrak{I})$.

Fact B. If B is integral over A and S is a multiplicative set in A with $S \cap \mathrm{Ker}\ \varphi = \emptyset$, then $S^{-1}B$ is integral over $S^{-1}A$.

However, observe that *if A is a normal ring and $\mathfrak{A}$ is one of its ideals, then $A/\mathfrak{A}$ need* **not** *be normal.* A standard example is a "singular curve".

Here, we take $\mathbb{C}[X,Y]$ which is a normal ring as it is a UFD. Let $\mathfrak{A} = (Y^2 - X^3)$, then $\mathbb{C}[X,Y]/\mathfrak{A}$ is **not** normal (though it is a domain (DX)). For, the element $\overline{Y}/\overline{X}$ (in Frac$A/\mathfrak{A}$) is integral over $A/\mathfrak{A}$ as its square is $\overline{X}$, yet it is not itself in $A/\mathfrak{A}$ (DX). The interpretation is this: $Y^2 - X^3 = 0$ describes a curve in the plane over $\mathbb{C}$ and Y/X defines by restriction a function holomorphic on the curve except at $(0,0)$. But, $\overline{Y}/\overline{X}$ is bounded near $(0,0)$ *on the curve*, so it ought to be extendable to a holomorphic (and algebraic) function. Yet, the set of such (near $(0,0)$) is just $(A\mathfrak{A})_{\mathfrak{p}}$, where $\mathfrak{p} = \{f \in A/\mathfrak{A} \mid f(0,0) = 0\}$. Of course, $\overline{Y}/\overline{X} \notin (A\mathfrak{A})_{\mathfrak{p}}$. The trouble is that $Y^2 = X^3$ has a "singular point" at $(0,0)$, it is **not** a complex manifold there (but it is everywhere else). This shows up in the fact that $(A\mathfrak{A})_{\mathfrak{p}}$ is not normal.

When A is a noetherian ring, we can be more precise, but we need some of the material (on primary decomposition from Sections 3.6 and 3.7. The two main things necessary are the statement

If V is a submodule of the A-module, M, then $V = (0)$ iff $V_{\mathfrak{p}} = (0)$ for all $\mathfrak{p} \in \mathrm{Ass}(M)$ (see Section 3.6, Corollary 3.102 of Theorem 3.99); and Krull's Principal Ideal Theorem (Section 3.7, Theorem 3.120).

You should skip the proof of Lemma 3.55, Theorem 3.56 and Corollary 3.57 until you read this later material; pick up the thread in Theorem 3.58, below.

Write, for a ring A,

$$\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(A/(a)), \text{ for some } \textit{non-zero divisor}, a, \text{ of } A\}.$$

Lemma 3.55 *If A is a reduced Noetherian ring, then an element $\xi \in \mathrm{Frac}(A)$ is actually in A if and only if for every, $\mathfrak{p} \in \mathrm{Pass}(A)$, the image of $\xi \in \mathrm{Frac}(A)_{\mathfrak{p}}$ is in $A_{\mathfrak{p}}$.*

Proof. If $\xi \in A$, then of course its image in $\mathrm{Frac}(A)_{\mathfrak{p}}$ lies in $A_{\mathfrak{p}}$ for all $\mathfrak{p}$. So, assume

$$\xi \in \bigcap \{A_{\mathfrak{p}} \mid \mathfrak{p} \in \mathrm{Pass}(A)\}$$

(here, of course, we mean the images of ξ in $\mathrm{Frac}(A)$ are in $A_{\mathfrak{p}}$). We write $\xi = \alpha/\beta$, where β is a non-zero divisor and suppose that $\xi \notin A$. Then, α is not in (β), so $V = A\overline{\alpha} \subseteq A/(\beta)$ is non-zero. By the statement italicized above, there is a $\mathfrak{p} \in \mathrm{Ass}(A/(\beta))$ with $(A\overline{\alpha})_{\mathfrak{p}} \neq (0)$. This means $\alpha/1 \notin (\beta)_{\mathfrak{p}}$; that is, $\xi = \alpha/\beta \notin A_{\mathfrak{p}}$. Yet, $\mathfrak{p} \in \mathrm{Pass}(A)$, a contradiction. □

Here is a characterization of normality for Noetherian domains:

Theorem 3.56 *Suppose that A is a noetherian domain, then the following conditions are equivalent:*

(1) A is normal

(2) For every $\mathfrak{p} \in \mathrm{Pass}(A)$, the ideal $\mathfrak{p}^e$ is a principal ideal of $A_\mathfrak{p}$

(3) (a) Every $\mathfrak{p} \in \mathrm{Pass}(A)$ has height 1 and

(b) For all height one primes, $\mathfrak{p}$, of A, the ring $A_\mathfrak{p}$ is a PID.

Proof. We first prove (2) $\iff$ (3). Suppose $\mathfrak{p}$ is any prime ideal of A. If $\mathfrak{p}$ is a principal ideal of $A_\mathfrak{p}$. it is an isolated prime of itself and Krull's Principal Ideal Theorem shows that $\mathrm{ht}(\mathfrak{p}) = 1$. So by (2),

$$\mathrm{Pass}(A) \subseteq \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}.$$

But, $\mathrm{ht}(\mathfrak{p}) = 1$ implies $\mathfrak{p}$ is an isolated prime ideal of any of its non-zero elements and, since A is a domain, this shows $\mathfrak{p} \in \mathrm{Pass}(A)$. We've proved that (2) implies that

$$\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}. \tag{$*$}$$

This shows that (2) implies (3a) and for all height one primes, $\mathfrak{p}$, the maximal ideal, $\mathfrak{p}$, of $A_\mathfrak{p}$ is principal. We'll now show that $A_\mathfrak{p}$ is a PID. Pick an ideal, $\mathfrak{A}$, of $A_\mathfrak{p}$ and write $\mathfrak{m} = \mathfrak{p}^e$. As $\mathfrak{m}$ is the maximal ideal of $A_\mathfrak{p}$, we have $\mathfrak{A} \subseteq \mathfrak{m}$, and as $\mathfrak{m}$ is principal we may assume $(0) < \mathfrak{A} < \mathfrak{m}$. Now $\mathfrak{m}^n$ is principal for all $n \geq 0$ with generator π^n, where π generates $\mathfrak{m}$; we'll show $\mathfrak{A} = \mathfrak{m}^n$ for some n. Now, were $\mathfrak{A} \subseteq \mathfrak{m}^n$ for all n, the Krull Intersection Theorem (Theorem 3.113) would show $\mathfrak{A} = (0)$, contrary to assumption. So, pick n minimal so that $\mathfrak{A} \subseteq \mathfrak{m}^n$. Then, every $\xi \in \mathfrak{A}$ has the form $a\pi^n$, and for at least one ξ, the element a is a unit (else $a \in \mathfrak{m}$ implies $a = b\pi$ and all ξ have shape $b\pi^{n+1}$). But then,

$$\mathfrak{A} \supseteq (\xi) = (\pi^n) = \mathfrak{m}^n \supseteq \mathfrak{A}$$

and $\mathfrak{A}$ is indeed principal. Therefore, (2) implies (3a) and (3b). It is clear that (3a) and (3b) imply (3).

We come then to the main point of our theorem, that (1) is equivalent to both parts of (3). Observe that the argument in the very early part of the proof shows that we always have

$$\{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\} \subseteq \mathrm{Pass}(A).$$

(3) $\Longrightarrow$ (1). By (3a), $\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}$; so

$$\bigcap\{A_\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\} = \bigcap\{A_\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Pass}(A)\} \tag{$**$}$$

By Lemma 3.55, the right hand side of ($**$) is A and by (3b) each $A_\mathfrak{p}$ is a normal domain (Proposition 3.53). Hence, A, as an intersection of noremal domains in $\mathrm{Frac}(A)$, is itself normal.

(1) $\Longrightarrow$ (3). Here, we will actually show (1) $\iff$ (2), then we will be done. Pick $\mathfrak{p} \in \mathrm{Pass}(A)$, say $\mathfrak{p} \in \mathrm{Ass}(A/(a))$. Then, there exists an element $\xi \in A$ so that $\mathfrak{p}$ is the annihilator of $\xi \pmod{(a)}$. We need to prove $\mathfrak{p}^e$ is principal, so we may replace A by $A_\mathfrak{p}$ and $\mathfrak{p}$ by $\mathfrak{p}^e$. Thus, our situation is that A is local and $\mathfrak{p}$ is its maximal ideal. Write

$$\mathfrak{A} = \{\eta \in \mathrm{Frac}(A) \mid \eta\mathfrak{p} \subseteq A\} = (\mathfrak{p} \longrightarrow A) \quad (\text{in } \mathrm{Frac}(A)).$$

Of course, $\mathfrak{A}\mathfrak{p}$ is an ideal of A and $A \subseteq \mathfrak{A}$ shows that $\mathfrak{p} = A\mathfrak{p} \subseteq \mathfrak{A}\mathfrak{p}$. Hence, there are only two possibilities: $\mathfrak{A}\mathfrak{p} = \mathfrak{p}$ or $\mathfrak{A}\mathfrak{p} = A$. I claim that the first cannot hold. If it did, condition (4) of Proposition 3.50 applied to each η of $\mathfrak{A}$ (with $\widetilde{B} = \mathfrak{p}$ and $B = \mathrm{Frac}(A)$) would show that all these η are integral over A. By (1), the η lies in A; so $\mathfrak{A} = A$. Now $\mathfrak{p}$ annihilates the element $\xi \pmod{(a)}$ and $\xi \notin (a)$; that is, $\xi\mathfrak{p} = \mathfrak{p}\xi \subseteq (a)$; so

$(\xi/a)\mathfrak{p} \subseteq A$. But then $\xi/a \in \mathfrak{A}$, i.e., $\xi/a \in A$. The last assertion is that $\xi \in (a)$, contrary to the choice of ξ. We deduce, therefore, that $\mathfrak{A}\mathfrak{p} = A$. Now, the map

$$\mathfrak{A} \otimes_A \mathfrak{p} \longrightarrow \mathfrak{A}\mathfrak{p}$$

is an isomorphism because if $\sum_i q_i \otimes p_i$ goes to zero in A, then using a common denominator, say d, for the q_i, we find $(1/d)\sum_i \alpha_i \otimes p_i$ is 0, too. Clearly, $\mathfrak{A} \otimes_A \mathfrak{p} \longrightarrow \mathfrak{A}\mathfrak{p}$ is surjective. Proposition 3.48 now shows $\mathfrak{p}$ is a free rank one A-module (remember A is local), i.e., a principal ideal. □

Corollary 3.57 *If A is a Noetherian normal domain, then*

$$A = \bigcap \{A_{\mathfrak{p}} \mid \mathrm{ht}(\mathfrak{p}) = 1\}.$$

Proof. Theorem 3.56, condition (3a) shows

$$\mathrm{Pass}(A) = \{\mathfrak{p} \mid \mathrm{ht}(\mathfrak{p}) = 1\}$$

and we then apply Lemma 3.55. □

There are relations between the prime ideals of A and B when B is integral over A. These are expressed in the three Cohen-Seidenberg Theorems. Here is the first of them:

Theorem 3.58 *(Lying over Theorem; Cohen-Seidenberg, I) If B is integral over A and $\mathfrak{p}$ is any prime ideal of A, then there is a prime ideal, $\mathfrak{Q}$, of B lying over $\mathfrak{p}$ (that is, $\varphi^{-1}(\mathfrak{Q}) = \mathfrak{p}$, where $\varphi\colon A \to B$).*

Proof. Of course, we may and do assume $A \subseteq B$. Let $\mathcal{S}$ be the collection of all ideals, $\mathfrak{B}$, of B with $\mathfrak{B} \cap A \subseteq \mathfrak{p}$; partially order $\mathcal{S}$ by inclusion. As $\mathcal{S} \neq \emptyset$ ($(0) \in \mathcal{S}$) and clealry inductive, Zorn's Lemma furnishes a maximal element, say $\mathfrak{Q}$, in $\mathcal{S}$. We must show both $\mathfrak{Q} \cap A = \mathfrak{p}$ and $\mathfrak{Q}$ is a prime ideal.

Were $\mathfrak{Q} \cap A < \mathfrak{p}$, we could find $\xi \in \mathfrak{p}$ with $\xi \notin \mathfrak{Q} \cap A$. Write $\widetilde{\mathfrak{Q}}$ for the ideal $\mathfrak{Q} + B\xi$; as $\xi \notin \mathfrak{Q}$, we get $\widetilde{\mathfrak{Q}} > \mathfrak{Q}$. So, $\widetilde{\mathfrak{Q}} \notin \mathcal{S}$ and thus $\widetilde{\mathfrak{Q}} \cap A \not\subseteq \mathfrak{p}$. Therefore, there is some $\eta \in \widetilde{\mathfrak{Q}} \cap A$ (thus $\eta \in A$) yet $\eta \notin \mathfrak{p}$. Now η is in $\widetilde{\mathfrak{Q}}$, so looks like $q + b\xi$, for some $b \in B$. Note that $\eta - b\xi = q \in \mathfrak{Q}$.

The element b is integral over A:

$$b^n + a_1 b^{n-1} + \cdots + a_{n-1}b + a_n = 0, \quad \text{all } a_j \in A.$$

If we multiply by ξ^n, we find

$$(b\xi)^n + a_1\xi(b\xi)^{n-1} + \cdots + a_{n-1}\xi^{n-1}(b\xi) + a_n\xi^n = 0. \tag{$*$}$$

View $(*)$ in $B/\mathfrak{Q}$; there $\overline{\eta} = \overline{b\xi}$, and so,

$$(\overline{\eta})^n + \overline{a_1\xi}(\overline{\eta})^{n-1} + \cdots + \overline{a_{n-1}\xi^{n-1}}\overline{\eta} + \overline{a_n\xi^n} = 0 \quad \text{in } A/\mathfrak{Q}. \tag{$**$}$$

But now, all elements on the left hand side of $(**)$ when read in B actually lie in A; so the left hand side of $(**)$ is in $\mathfrak{Q} \cap A$. We get

$$\eta^n + a_1\xi\eta^{n-1} + \cdots + a_{n-1}\xi^{n-1}\eta + a_n\xi^n \in \mathfrak{p}.$$

Remembering that $\xi \in \mathfrak{p}$, we find $\eta \in \mathfrak{p}$, a contradiction. This shows $\mathfrak{Q} \cap A = \mathfrak{p}$.

To show $\mathfrak{Q}$ is a prime ideal, write S for the multiplicatice set $A - \mathfrak{p}$; S is a multiplicative subset of B. Of course, $\mathfrak{Q} \cap S = \emptyset$. Suppose $\mathfrak{Q}$ were not maximal among ideals of B whose intersection with S is empty. We'd find $\widetilde{\mathfrak{Q}} > \mathfrak{Q}$ and $\mathfrak{Q} \cap S = \emptyset$. But then $\mathfrak{Q} \cap A = \mathfrak{p}$ and so $\widetilde{\mathfrak{Q}}$ lies in $\mathcal{S}$ where $\mathfrak{Q}$ is maximal contradicting $\widetilde{\mathfrak{Q}} > \mathfrak{Q}$. Therefore, $\mathfrak{Q}$ is maximal among ideals of B with $\mathfrak{Q} \cap S = \emptyset$. Now, Proposition 3.8 (the implication (6) $\Longrightarrow$ (1)) shows $\mathfrak{Q}$ is prime. □

Theorem 3.59 *(Going-up Theorem; Cohen-Seidenberg, II) Suppose B is integral over A and $\mathfrak{p} \subseteq \mathfrak{q}$ are two prime ideals of A. If $\mathfrak{P}$ is a prime ideal of B lying over $\mathfrak{p}$, there exists a prime ideal, $\mathfrak{Q}$, of B lying over $\mathfrak{q}$ with $\mathfrak{P} \subseteq \mathfrak{Q}$.*

Proof. This is just a corollary of the lying over theorem. For once again, we may assume $A \subseteq B$ and we consider $A/\mathfrak{p}$ and $B/\mathfrak{P}$. As $\mathfrak{P} \cap A = \mathfrak{p}$ and B is integral over A, we find $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$ and apply Cohen-Seidenberg I to $A/\mathfrak{p}$ and $B/\mathfrak{P}$, using $\overline{\mathfrak{q}}$ as our ideal of $A/\mathfrak{p}$. There *is* $\overline{\mathfrak{Q}}$, a prime of $B/\mathfrak{P}$, over $\overline{\mathfrak{q}}$ and the pull-back of $\overline{\mathfrak{Q}}$ in B is what we want. □

Corollary 3.60 *If A and B are integral domains and B is integral over A, then A is a field iff B is a field.*

Proof. Suppose A is a field and $\xi \neq 0$ is in B. The element ξ is integral over A; so

$$\xi^n + a_1\xi^{n-1} + \cdots + a_{n-1}\xi + a_n = 0$$

for some $a_1, \ldots, a_n \in A$. Of course, we may assume that $a_n \neq 0$. Then

$$\xi(\xi^{n-1} + a_1\xi^{n-2} + \cdots + a_{n-1}) = -a_n;$$

and, as A is field, the element

$$-\frac{1}{a_n}(\xi^{n-1} + a_1\xi^{n-2} + \cdots + a_{n-1})$$

lies in B and is the inverse of ξ.

If B is a field and A is not, there are prime ideals $(0) < \mathfrak{q}$ of A. The going-up theorem gives us prime ideals (0) and $\mathfrak{Q}$ of B lying over (0) and $\mathfrak{A}$—but, B is a field; contradiction.

(We may also argue directly as in the first implication of the proof: Given $\xi \in A$, the element ξ is in B and B is a field. So, $1/\xi \in$B; thus $1/\xi$ is integral over A. We have

$$\left(\frac{1}{\xi}\right)^n + a_1\left(\frac{1}{\xi}\right)^{n-1} + \cdots + a_{n-1}\left(\frac{1}{\xi}\right) + a_n = 0.$$

Multiply through by ξ^n; we find

$$1 = -\xi(a_1 + \cdots + a_{n-1}\xi^{n-2} + a_n\xi^{n-1});$$

so ξ has an inverse in A.) □

Corollary 3.61 *If B is integral over A and $\mathfrak{P} \in \operatorname{Spec} B$ lies over $\mathfrak{p} \in \operatorname{Spec} A$, then $\mathfrak{p}$ is maximal iff $\mathfrak{P}$ is maximal.*

This is merely a restatement of Corollary 3.60. A more important remark is the *incomparability* of two primes lying over a fixed prime:

Proposition 3.62 *Say B is integral over A and $\mathfrak{P}$, $\mathfrak{Q}$ are two primes of B lying over the same prime, $\mathfrak{p}$, of A. Then $\mathfrak{P}$ and $\mathfrak{Q}$ are incomparable; that is we cannot have either $\mathfrak{P} \subseteq \mathfrak{Q}$ or $\mathfrak{Q} \subseteq \mathfrak{P}$ without $\mathfrak{P} = \mathfrak{Q}$.*

Proof. Assume $\mathfrak{P} < \mathfrak{Q}$ and reduce A mod $\mathfrak{p}$ and B mod $\mathfrak{P}$. Then we may assume A and B are domains and we have to prove no non-zero prime contracts to the zero ideal of A. In fact, we prove: *If A, B are domains with B integral over A and if $\mathfrak{B}$ is a non-zero ideal of B, then $\mathfrak{B}$ contracts to a non-zero ideal of A .*

Choose $b \in \mathfrak{B}$ with $b \neq 0$. Then we find

$$b^n + a_1b^{n-1} + \cdots + a_{n-1}b + a_n = 0.$$

and we may assume $a_n \neq 0$ (else we could divide out b and lower the degree, n; etc.) But then $a_n \in \mathfrak{B} \cap A$; so $\mathfrak{B} \cap A \neq (0)$, as required. □

Now we come to the circle of ideas around the third (and deepest) of the Cohen-Seidenberg Theorems, the so-called "Going–Down Theorem". This is a study of prime ideals in integral extensions where the bottom ring is a *normal* ring. For the proof of the theorem, we need some simple ideas from Galois theory) most of which are already familiar) which are covered in full in Chapter 4, sections one through four. Readers are urged to skip the proofs of Propositions 3.63 and 3.64 and Theorem 3.65, and come back to these after having read Sections 4.2–4.5 of Chapter 4. Once again, one can pick up the thread of our discussion in Proposition 3.66. Nonetherless the statements of all results below are clear.

Recall that if k is a field and B is a k-algebra, and element ξ, of B is algebraic over B iff it satisfies a (non-zero) polynomial $f(X) \in k[X]$. Of course, the set of all polynomials, $g(X)$, with $g(\xi) = 0$ is a principal ideal of $k[X]$ and the monic polynomial generating this ideal is the *minimal polynomial of* ξ *over* k. If B has zero divisors, the minimal polynomial of ξ over k will not, in general, be irreducible in $k[X]$. Even if no non-zero element of k becomes a zero divisor in B, still the minimal polynomial might be reducible.[4] But when B is at least a domain the minimal polyomial will be irreducible. We also want to consider in k an integral domain, A, with $k = \mathrm{Frac}(A)$.

So, let $\xi \in B$ be integral over A, assume B is a domain. Then we can factor the minimal polynomial $f(X)$, for ξ over $k = \mathrm{Frac}(A)$ in some big field over B (Section 4.4 of Chapter 4) and it will have exactly n roots where $n = \deg(f)$. Write these as $\xi = \xi_1, \xi_2, \ldots, \xi_n$. By Section 4.3, Chapter 4, each n_i is repated p^e times where $p = \mathrm{char}(k)$ and $e \geq 0$; p^e is the degree of inseparability of ξ over k. Moreover, there is an automorphism fixing the elements of k taking each ξ to ξ; so each ξ_i satisfies the equation of integral dependence which ξ satisfies (Section 4.4, Chapter 4 again). Now when we write $f(X)$ as a product of the linear factors $(X - \xi_i)$ we get

$$f(X) = \prod_{i=1}^{n}(X - \xi_i) = \sum_{j=0}^{n} \sigma_j(\xi_1, \ldots, \xi_n)(-1)^j X^{n-j},$$

here the σ_j are the *elementary symmetric functions* of the ξ_i, given as

$$\begin{aligned}
\sigma_0(\xi_1, \ldots, \xi_n) &= 1 \\
\sigma_1(\xi_1, \ldots, \xi_n) &= \xi_1 + \cdots + \xi_n \\
\sigma_2(\xi_1, \ldots, \xi_n) &= \sum_{i<j} \xi_i \xi_j \\
&\vdots \\
\sigma_r(\xi_1, \ldots, \xi_n) &= \sum_{i_1 < i_2 < \cdots < i_r} \xi_{i_1} \xi_{i_2} \cdots \xi_{i_r} \\
&\vdots \\
\sigma_n(\xi_1, \ldots, \xi_n) &= \xi_1 \xi_2 \cdots \xi_n.
\end{aligned}$$

Thus, when ξ is integral over A, so are all the ξ_i and all the elements $\sigma_j(\xi_1, \ldots, \xi_n)$, for $j = 1, 2, \ldots, n$. But each $\sigma_j(\xi_1, \ldots, \xi_n)$ is in k, therefore each σ_j is in $\mathrm{Aut}_k(A)$. The symmetric functions σ_1 and σ_n have special designation—they are the *trace* and *norm of* ξ *over* k, respectively. This argument gives the first two statements of

Proposition 3.63 *If A is a domain and $k = \mathrm{Frac}(A)$, write B for an overing of A and K for $\mathrm{Frac}(B)$. Then,*

[4] A standard example is the "ring of dual numbers over k", namely, $k[X]/(X^2)$. The minimal polynomial of $\overline{X}$ is X^2.

(1) When K is a field and $\xi \in K$ is integral over A, all the coefficients of the minimal polynomial for ξ over k are integral over A (so the norm and trace of ξ are integral over A).

(2) If A is a normal domain and K is a field, the minimal k-polynomial for an element $\xi \in K$ which is integral over A already lies in $A[X]$ and is an equation of integral dependence for ξ.

(3) If A is a normal domain and $f(X), g(X)$ are two monic polynomials in $k[X]$ so that $f(X)g(X)$ is in $A[X]$, then each of $f(X)$ and $g(X)$ is already in $A[X]$.

(4) If A is a normal domain and B is an overring of $\mathrm{Frac}(A)$*, and if $\xi \in B$ is integral over A, then the minimal k-polynomial of ξ is already in $A[X]$ and is an integral dependence relation for ξ. That is, (2) holds even K is not a field (B is an integral domain),* **provided** *$K \subseteq k$.*

(5) If A is a normal domain and B is an overring of A, with $\xi \in B$ integral over A, and if **non non-zero element of A becomes a zero divisor in** *B, then again the minimal k-polynomial for ξ is already in $A[X]$ and is an integral dependence.*

Proof. (1) and (2) are already proved; consider (3). Write $f(X) = \prod_i (X - \xi)$ and $g(X) = \prod_j (X - \eta_j)$ in some big overfield. Now $f(X)g(X)$ is a monic polynomial in $A[X]$ all xi_i and η_j satisfy it. But such a monic polynomial is an integral dependence relation; so, all ξ_i are integral over A and all the η_j are integral over A. By the argument for (1) each of the $\sigma_i(\xi_1, \ldots, \xi_t)$ and $\sigma_j(\eta_1, \ldots, \eta_r)$ are integral over A; hence they are in A by the normality of A. But, these are (up to sign) the coefficients of $f(X)$ and $g(X)$ and (3) is proved.

(4) B is a k-algebra, so ξ has a minimal polynomial, $f(X) \in k[X]$. Now ξ is also integral over A, therefore there is a monic polynomial, $h(X) \in A[X]$, with $h(\xi) = 0$. As f generates the principal $k[X]$ ideal of polynomials vanishing at ξ, there is a $g(X) \in k[X]$ with $f(X)g(X) = h(X)$ and clearly $g(X)$ is monic. Then, (3) shows $f(X) \in A[X]$ and is an equation of integral dependence.

(5) Here, if S is the multiplicative set of nonzero elements of A, then each $s \in S$ is a non-zero divisor of B and so $k = \mathrm{Frac}(A) \subseteq S^{-1}B \subseteq \mathrm{Frac}(B)$. We can then apply (4) to $S^{-1}B$ and conclude (5). □

Remark: Notice that the statement of (3) contains the essential ideal of Gauss' classical proof that if A is a UFD so is $A[X]$.

The hypothesis of (5) follows from a perhaps more easily checked condition:

Proposition 3.64 *If B is an A-algebra and B is flat over A, then no non-zero divisor of A becomes a non-trivial zero divisor in B.*

Proof. To say ξ is a non-zero divisor is to say

$$0 \longrightarrow A \xrightarrow{\xi} A \longrightarrow A/A\xi \longrightarrow 0$$

is exact. Now, tensor this exact sequence with B over A and use flatness to get

$$0 \longrightarrow B \xrightarrow{\xi} B \longrightarrow B/B\xi \longrightarrow 0$$

is exact. □

Theorem 3.65 *(Going-down Theorem; Cohen-Seidenberg, III) Suppose A is a normal domain and B is an overring of A. Assume either*

(1) B is integral over A and

(2) No non-zero element of A becomes a zero divisor of B

or

(1′) B is integral over A and

(2′) B is flat over A.

Then, given prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ of A and a prime ideal $\mathfrak{Q}$ of B over $\mathfrak{q}$, there is a prime ideal, $\mathfrak{P}$, of B, over $\mathfrak{p}$ so that $\mathfrak{P} \subseteq \mathfrak{Q}$.

Proof. If $\widetilde{A}$ is the image of A in B and (2′) holds, then B is flat over $\widetilde{A}$ and so, by Proposition 3.64, (2) holds. Therefore, we will assume (1) and (2).

The key to the proof is to find an apt multiplicative set, S, of B and to consider $S^{-1}B$. Take S to be the collection of products, $a\alpha$, where $a \in A - \mathfrak{p}$ and $\alpha \in B - \mathfrak{Q}$. Of course, S is closed under multiplication and $1 \in S$; further $0 \notin S$ else a, an element of A, would be a zero divisor of B contrary to (2). Observe, by taking $a = 1$ or $\alpha = 1$, we find $A - \mathfrak{p} \subseteq S$ and $B - \mathfrak{Q} \subseteq S$.

I claim the extended ideal, $\mathfrak{p}^e$, of $\mathfrak{p}$ in $S^{-1}B$ is not the unit ideal. Suppose, for the momemt, the claim is proved; we finish the proof as follows: The ideal $\mathfrak{p}^e$ is contained in some maximal ideal, $\mathfrak{M}$, of $S^{-1}B$, and so $\mathfrak{M}^c$ is a prime ideal of B. (As each ideal of $S^{-1}B$ is extended, $\mathfrak{M}$ is $\mathfrak{A}^e$ and so $\mathfrak{M}^{ce} = \mathfrak{A}^{ece} = \mathfrak{A}^e = \mathfrak{M} \neq S^{-1}B$; therefore, $\mathfrak{M}^e \neq B$.) Since $\mathfrak{M} \neq S^{-1}B$, the ideal $\mathfrak{M}^c$ cannot intersect S and $B - \mathfrak{Q} \subseteq S$ shows that $\mathfrak{M}^c \subseteq \mathfrak{Q}$. Now consider $\mathfrak{M}^c \cap A$, it is a prime ideal of A and cannot intersect S. Again, $A - \mathfrak{p} \subseteq S$ implies $\mathfrak{M}^c \cap A \subseteq \mathfrak{p}$. Yet

$$\mathfrak{p} \subseteq \mathfrak{p}B \cap A \subseteq \mathfrak{p}^{ec} \cap A \subseteq \mathfrak{M}^c \cap A,$$

therefore $\mathfrak{M}^c \cap A = \mathfrak{p}$ and we can set $\mathfrak{P} = \mathfrak{M}^c$.

We are therefore down to proving our claim, that is that $\mathfrak{p}B \cap S = \emptyset$. Pick $\xi \in \mathfrak{p}B$, write $\xi = \sum b_i p_i$ with $p_i \in \mathfrak{p}$ and $b_i \in B$. Let $\widetilde{B} = A[b_1, \ldots, b_t]$; it is a f.g. A-module (as well as A-algebra) by the integrality of B over A. We have $\xi\widetilde{B} \subseteq \mathfrak{p}\widetilde{B}$ and if $\xi_1, \ldots, \xi_r$ form a set of A-module generators for $\widetilde{B}$, we find from $\xi\xi_j \in \mathfrak{p}\widetilde{B}$ the linear equations:

$$\xi\xi_j = \sum_{i=1}^{r} p_{ij}\xi_i, \qquad p_{ij} \in \mathfrak{p}.$$

Just as in the argument (4) $\iff$ (1) of Proposition 3.50, this leads to $\Delta\xi_i = 0$ for $i = 1, \ldots, r$, where $\Delta = \det(\delta_{ij}\xi - p_{ij})$. Thus, $\Delta\widetilde{B} = 0$, yet $1 \in \widetilde{B}$; so $\Delta = 0$. By the minor expansion of Δ, we deduce the integral dependence

$$h(\xi) = \xi^r + \pi_1\xi^{n-1} + \cdots + \pi_{r-1}\xi + \pi_r = 0$$

and *here all the $\pi_i \in \mathfrak{p}$*.

Say ξ is in S, then it has the form $a\alpha$, with $a \in A - \mathfrak{p}$ and $\alpha \in B - \mathfrak{Q}$. By part (5) of Proposition 3.63, the minimal polynomial, $f(X) \in k[X]$, for ξ is already in $A[X]$ and is an integral dependence for ξ. But, also $f(X)$ divides $h(X)$ in $k[X]$ as $h(\xi) = 0$; so

$$f(X)g(X) = h(X) \qquad \text{in } k[X]$$

and $g(X)$ is monic. Apply part (3) of Proposition 3.63 and get that $g(X) \in A[X]$, too. This means we can reduce the coefficients of f, g, h mod $\mathfrak{p}$. The polynomial $h(X)$ becomes $\overline{h}(X) = X^r$. But $A/\mathfrak{p}$ is a domain and $\overline{h} = \overline{f}\,\overline{g}$; so $\overline{f}(X) = X^p$, that is

$$f(X) = X^s + \delta_1 X^{s-1} + \cdots + \delta_{s-1}X + \delta_s,$$

and *all the δ_i lie in $\mathfrak{p}$*.

Now $\xi = a\alpha$ and by (5) of Proposition 3.63 once again, we see that the k-minimal polynomial for α is actually in $A[X]$ and is an integral dependence for α. Write this polynomial, $m(X)$, as

$$m(X) = X^v + u_1 X^{v-1} + \cdots + u_{v-1}X + u_v$$

with each $u_i \in A$. Now multiply $m(X)$ by a^v, we get

$$a^v m(X) = (aX)^v + au_1(aX)^{v-1} + \cdots + a^{v-1}u_{v-1}(aX) + a^v u_v.$$

So, for the polynomial

$$\widetilde{f}(X) = X^v + au_1X^{v-1} + \cdots + a^{v-1}u_{v-1}X + a^v u_v$$

we find $\widetilde{f}(\xi) = a^v m(\alpha) = 0$ and therefore $f(X)$ divides $\widetilde{f}(X)$ in $k[X]$: $\widetilde{f}(X) = z(X)f(X)$. By (3) of Proposition 3.63, we see $z(X)$ is monic and in $A[X]$, and $v = \deg(\widetilde{f}) \geq \deg(f) = s$. However, by the same token if we divide $f(X)$ by a^s, we get

$$\left(\frac{X}{a}\right)^s + \frac{\delta_1}{a}\left(\frac{X}{a}\right)^{s-1} + \cdots + \frac{\delta_{s-1}}{a^{s-1}}\left(\frac{X}{a}\right) + \frac{\delta_s}{a^s}$$

giving us the k-polynomial

$$F(X) = X^s + \frac{\delta_1}{a}X^{s-1} + \cdots + \frac{\delta_{s-1}}{a^{s-1}}X + \frac{\delta_s}{a^s}.$$

We have $F(\alpha) = (1/a^s)f(\xi) = 0$; so $m \mid F$ in $k[X]$. Therefore,

$$s = \deg(F) \geq \deg(m) = v;$$

coupled with the above this shows $s = v$ and $Z(X) = 1$. Therefore, $f(X) = \widetilde{f}(X)$ so that

$$\delta_j = a^j u_j, \qquad j = 1, 2, \ldots, s.$$

Now $\delta_j \in \mathfrak{p}$ and, by choice of S, $a \notin \mathfrak{p}$. Therefore, *all the* u_j *belong to* $\mathfrak{p}$.

Finally, $m(\alpha) = 0$; so,

$$\alpha^s + u_1\alpha^{s-1} + \cdots + u_{s-1}\alpha + u_s = 0.$$

This shows $\alpha^s \in \mathfrak{p}B \subseteq \mathfrak{q}B \subseteq \mathfrak{Q}$; whence $\alpha \in \mathfrak{Q}$—a contradiction. □

The Cohen-Seidenberg Theorems have geometric content. It turns out that for a commutative ring A (over the complex numbers), $\operatorname{Spec} A$ can be made into a (generalized) complex space (perhaps of infinite dimension); that is into a complex manifold with some singularities (perhaps). For us, the important point is that $\operatorname{Spec} A$ is a topological space (see Section 3.3) and we'll only draw topological content from the Cohen-Seidenberg Theorems.

So, first say B is integral over A. The ring map $\varphi\colon A \to B$ gives a continuous map $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$, namely: $\mathfrak{P} \mapsto \varphi^{-1}(\mathfrak{P})$. The lying over theorem can now be expressed as:

If B is integral over A, the continuous map $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *is surjective.*

Remark: *We've used a Cohen-Seidenberg Theorem; so, we've assumed $A \longrightarrow B$ is an* **injection** *in the above.*

The question of $A \longrightarrow B$ being an injection and the "real" content of integrality can be teased apart as follows:

Proposition 3.66 *Say $A \longrightarrow B$ is an injection. Then the continuous map* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *has dense image. If $A \longrightarrow B$ is surjective, then the continuous map* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *is a homeomorphism onto a closed subset of* $\operatorname{Spec} A$.

Proof. Write φ for the homomorphism $A \longrightarrow B$ and $|\varphi|$ for the continuous map $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$. Pick any $\mathfrak{p} \in \operatorname{Spec} A$ and any $f \notin \mathfrak{p}$ (so that $\mathfrak{p} \in X_f$ in $\operatorname{Spec} A$). We must find $\mathfrak{q} \in \operatorname{Spec} B$ so that $|\varphi|(\mathfrak{q}) \in X_f$. Now f is not nilpotent; so, as φ is injective, neither is $\varphi(f)$. But then there is a prime ideal, $\mathfrak{q}$, of B, and $\varphi(f) \notin \mathfrak{q}$ (cf. either Proposition 3.8 #(6) or remark #(4) after Proposition 3.11); that is $f \notin |\varphi|(\mathfrak{q})$, which is what we needed.

Recall, from the discussion on the Zariski topology following Proposition 3.11, that the closed sets in $\operatorname{Spec} A$ are all of the form $V(\mathfrak{A})$ for some ideal $\mathfrak{A}$, of A. Now there is the usual one-to-one correspondence of ideals, $\mathfrak{B}$, of A which contain $\mathfrak{A}$ and all ideals of $A/\mathfrak{A}$. If we take for $\mathfrak{A}$ the kernel of φ, then the first consequence is that $\mathfrak{p} \mapsto |\varphi|(\mathfrak{p})$ is a continuous bijection of $\operatorname{Spec} B$ ($= \operatorname{Spec} A/\mathfrak{A}$) and the closed set, $V(\mathfrak{A})$, of $\operatorname{Spec} A$. But, this is also a closed map, because for $\mathfrak{B}$, an ideal of B, the map $|\varphi|$ takes $V(\mathfrak{B})$ onto $V(\varphi^{-1}(\mathfrak{B})) \subseteq \operatorname{Spec} A$. □

Proposition 3.67 *If B is integral over A, where $\varphi\colon A \to B$ need not be injective, then the map $|\varphi|$ from $\operatorname{Spec} B$ to $\operatorname{Spec} A$ is a closed map. In fact, it is universally closed; that is, the map $|\varphi_C|\colon \operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec} C$ is a closed map for every A-algebra, C.*

Proof. Note that if B is integral over A, then $B \otimes_A C$ is integral over C. To see this, observe that a general element of $B \otimes_A C$ is a sum of terms $b \otimes c$ with $b \in B$ and $c \in C$. If $b \otimes c$ is integral over C so is any sum of such terms. But, $b \otimes c = (b \otimes 1)(1 \otimes c)$ and $1 \otimes c$ is in C ($= A \otimes_A C$) so all we need check is that $b \otimes 1$ is integral over C. Write the integral dependence for b over A, then tensor with 1 (as in $b \otimes 1$) and get the integral dependence of $b \otimes 1$ over C.

This remark reduces us to proving the first statement. Now the map $A \longrightarrow B$ factors as

$$A \longrightarrow \widetilde{A} = A/\mathfrak{A} \hookrightarrow B,$$

so for the spaces $\operatorname{Spec} A$, etc., we get

$$\operatorname{Spec} B \longrightarrow \operatorname{Spec} \widetilde{A} \longrightarrow \operatorname{Spec} A.$$

By Proposition 3.66, the second of thesex maps is closed, therefore we are reduced to the case where $A \longrightarrow B$ is injective. A closed set of $\operatorname{Spec} B$ is $V(\mathfrak{B})$ and we know by Fact A following Proposition 3.54 that $B/\mathfrak{B}$ is integral over $A/(\mathfrak{B} \cap A)$. The interpretation of Cohen–Seidenberg II shows that
$\operatorname{Spec}(B/\mathfrak{B}) \longrightarrow \operatorname{Spec}(A/(\mathfrak{B} \cap A))$ is surjective. Coupled with the homeomorphisms

$$\operatorname{Spec}(B/\mathfrak{B}) \cong V(\mathfrak{B}); \quad \operatorname{Spec}(A/(\mathfrak{B} \cap A)) \cong V(\mathfrak{B} \cap A),$$

this finishes the proof. □

Let's continue with these topological considerations a bit further. Take $\mathfrak{p} \in \operatorname{Spec} A$, one wants to consider $\{\mathfrak{p}\}$ as Spec(?) for some A-algebra "?". At first $A_{\mathfrak{p}}$ seems reasonable, but $\operatorname{Spec} A_{\mathfrak{p}}$ consist of *all* the primes contained in $\mathfrak{p}$. We can get rid of all these extraneous primes by factoring out by $\mathfrak{p}^e$ and forming

$$\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}^e.$$

The A-algebra, $\kappa(\mathfrak{p})$, is a field; so, $\operatorname{Spec} \kappa(\mathfrak{p})$ is one-point—it corresponds to $\mathfrak{p}$. Indeed, in the map $\kappa(\mathfrak{p}) \longrightarrow \operatorname{Spec} A$ coming from the ring map

$$A \longrightarrow A_{\mathfrak{p}} \longrightarrow A_{\mathfrak{p}}/\mathfrak{p}^e = \kappa(\mathfrak{p}),$$

the one point of $\operatorname{Spec} \kappa(\mathfrak{p})$ goes to $\mathfrak{p}$ in $\operatorname{Spec} A$. If B is an A-algebra, then $B \otimes_A \kappa(\mathfrak{p})$ is a $\kappa(\mathfrak{p})$-algebra isomorphic to $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$. The commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & B \otimes_A \kappa(\mathfrak{p}) \\ \uparrow & & \uparrow \\ A & \longrightarrow & \kappa(\mathfrak{p}) \end{array}$$

shows that the elements of $\mathrm{Spec}(B\otimes_A \kappa(\mathfrak{p}))$ all go to $\mathfrak{p}$ under the map $\mathrm{Spec}(B\otimes_A \kappa(\mathfrak{p}) \longrightarrow \mathrm{Spec}\, A$. *Therefore,* $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p})$ *is the fibre of the map* $\mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A$ *over* $\{\mathfrak{p}\}$.

Proposition 3.68 *Suppose B is a finitely generated A-algebra and is also integral over A. Then, each fibre of the map* $\mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A$ *is finite.*

Proof. The algebra B has the form $A[b_1, \ldots, b_t]$ and each b_j is integral over A. Thus, B is a finitely-generated A-*module*. So, each $B \otimes_A \kappa(\mathfrak{p})$ is a finitely generated $\kappa(\mathfrak{p})$-vector space and therefore has the D.C.C. By Lemma 3.37, $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ is a finite set. □

We have more than stated: B is not only a finitely generated A-algebra it is a f.g. A-*module*. This is stronger than the condition that all the fibres of $|\varphi|\colon \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ be finite. Indeed, consider the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The points of $\mathrm{Spec}\,\mathbb{Z}$ are $\{0\}$, $\{2\}$, $\{3\}, \ldots$, $\{p\}, \ldots$, and the fibres of $\mathrm{Spec}\,\mathbb{Q}$ over $\mathrm{Spec}\,\mathbb{Z}$ are respectively $\{0\}$, $\emptyset$, $\emptyset, \ldots, \emptyset, \ldots$. Of course, $\mathbb{Q}$ is not integral over $\mathbb{Z}$ nor is it finitely–generated as $\mathbb{Z}$-algebra.

A more germane example is $\mathbb{C}[X]$ as included in $\mathbb{C}[X,Y]/(XY-1)$. The primes of $\mathbb{C}[X]$ are $\{0\}$ and the principal ideals $(X-\lambda)$, where λ ranges over $\mathbb{C}$. The fibre over $\{0\}$ is $\{0\}$, that over $(X-\lambda)$ for $\lambda \neq 0$, is the principal ideal which is the kernel of $X \mapsto \lambda$; $Y \mapsto 1/\lambda$. But, over (X), the fibre is $\emptyset$. So, all fibres are finite, $B = \mathbb{C}[X,Y]/(XY-1)$ is a finitely generated $\mathbb{C}[X]$-algebra yet B is not a finitely generated $\mathbb{C}[X]$-module; hence B is not integral over $A = \mathbb{C}[X]$ under the standard inclusion. Observe also that $\mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A$ is not a closed map in this case—this turns out to be the key. For, we have the following fact due to Chevalley:

Fact. If B is a finitely-generated A-algebra under a map φ and if $|\varphi|$ is both universally closed and has finite fibres, then B is a finite A-module (in particular, B is integral over A).

The proof of this is very far from obvious and is not part of our purview. However, the discussion does suggest the following question: Say A is a domain and write k for $\mathrm{Frac}\, A$. if K/k is a finite degree field extension, is $\mathrm{Int}_A(K)$ a finitely generated A-algebra (hence, a f.g. A-module)? The answer is "no", which perhaps is to be expected. But, even if A is noetherian, the answer is still "no". This is somewhat surprising and suggests that the finite generation of $\mathrm{Int}_A(K)$ is a delicate and deep matter. If we are willing to assume a bit more about K/k we get a very satisfying answer. We'll need some material from Chapter 4, Section 4.2 and 4.3 for this.

Theorem 3.69 *Suppose A is a normal domain with fraction field k and say K/k is a finite* **separable** *extension. Then,* $\mathrm{Int}_A(K)$ *is contained in a f.g. A-module in K. In fact, a basis for K/k can be found which generates the latter A-module. If A is, in addition, noetherian, then* $\mathrm{Int}_A(K)$ *is itself a finite A-module; hence is noetherian.*

Proof. We use the trace from K to k (see Chapter 4, Section 4.7), this is a k-linear map, $\mathrm{tr}\colon K \to k$. We set for $x, y \in K$

$$\langle x, y\rangle = \mathrm{tr}_{K/k}(xy).$$

The fact we need is that the separability of K/k entails the non-degeneracy of the pairing $\langle x, y\rangle$. (Actually, this is not proved in Section 4.7 of Chapter 4 but is an easy consequence of Newton's Identities connecting sums of powers of elements $x_1, \ldots, x_t$ with elementary symmetric functions in $x_1, \ldots, x_t$.) This being said, we see that K is self-dual as vector space over k, via our pairing $\langle x, y\rangle$.

Let $B = \mathrm{Int}_A(K)$, then in fact $\mathrm{Frac}(B) = K$. To see this, choose $x \in K$, then x has a minimal k-polynomial $m(T) \in k[T]$, say

$$m(x) = x^r + \alpha_1 x^{r-1} + \cdots + \alpha_{r-1}x + \alpha_r = 0, \qquad \alpha_i \in k. \tag{$\dagger$}$$

As $k = \mathrm{Frac}(A)$, for each i, there is $s_i \in A$ with $s_i\alpha_i \in A$. We take $s = \prod s_i$, then $s\alpha_i \in A$ for all i; so multiply ($\dagger$) by s^r, we get

$$(sx)^r + s\alpha_1(sx)^{r-1} + \cdots + s^{r-1}\alpha_{r-1}(sx) + s^r\alpha_r = 0.$$

This shows that $xs \in \mathrm{Int}_A(K) = B$, so $x \in \mathrm{Frac}(B)$. (It shows more. Namely, $K = (A - \{0\})^{-1}B$.) It follows that we may choose a k-basis for K from B; say this is $b_1, \ldots, b_t$. By the non-degeneracy of $\langle x, y\rangle$, the dual basis consists of elements of K, say they are $c_1, \ldots, c_t$. Thus,

$$\langle b_i, c_j\rangle = \delta_{ij}.$$

Now, choose $x \in B$ and write x in terms of the basis $c_1, \ldots, c_t$. We have $x = \sum \gamma_i c_i$, with the $\gamma_i \in k$. As x and the b_i lie in B, we see that $xb_i \in B$ and statement (1) of Proposition 3.63 shows that $\langle x, b_i\rangle \in A$ because A was assumed normal. But

$$\langle x, b_i\rangle = \langle \sum_j \gamma_j c_j, b_i\rangle = \sum_j \gamma_j \delta_{ji} = \gamma_i$$

so all $\gamma_i \in A$. Therefore $B \subseteq Ac_1 + \cdots + Ac_t$, as required in the first two conclusions of our theorem. Of course, if A is noetherian, then B, as a sub-module of a f.g. A-module, is itself finitely generated. □

Remark: We cannot expect B to be generated by just t elements as its containing module $Ac_1 + \cdots + Ac_t$ is so generated. On the other hand, it can never be generated by fewer than t elements. For if it were, say $B = Ad_1 + \cdots + Ad_r$, with $r < t$, then

$$(A - \{0\})^{-1}B = k \otimes_A B = k\text{-span of } d_1, \ldots, d_r.$$

Yet the left hand side is just K and so

$$t = \dim K \leq r,$$

a contradiction. When B *is* generated by t elements, this shows they must be a basis for K/k. If A is a P.I.D., one knows from $B \leq Ac_1 \coprod \cdots \coprod Ac_t$ that B is generated by t or fewer elements, and so we've proved

Corollary 3.70 *If A is a P.I.D. and K is a finite separable extension of $k = \mathrm{Frac}\, A$, then there exist elements $\beta_1, \ldots, \beta_t$ of $B = \mathrm{Int}_A(K)$ so that*

(1) B is the free A-module on $\beta_1, \ldots, \beta_t$ and

(2) $\beta_1, \ldots, \beta_t$ are a k-basis for K.

A set of elements $\beta_1, \ldots, \beta_t$ having properties (1) and (2) above is called an *integral basis for K/k*. An integral basis might exist for a given normal, noetherian A and an extension K/k, but it is guaranteed if A is a P.I.D.

Theorem 3.69 shows that the difficulty of the finite generation of $\mathrm{Int}_A(K)$ resides in the possible inseparability of the layer K/k. It can happen that we must continue to add more and more elements without end in a tower

$$A \subseteq B_1 \subseteq B_2 \subseteq \cdots \subseteq B_n \subseteq \cdots \subseteq B = \mathrm{Int}_A(K)$$

and examples (due to Nagata) exist of just this phenomenon. Fortunately, for a big class of integral domains of interest in both number theory and algebraic geometry, this does not happen—they are well-behaved. These are the integral domains, A, that are finitely generated k-algebras, where k is a *field*. We'll refer to them as *finitely generated domains over k*. We will also need some material from Chapter 4 Section 4.11, namely the notion of transcendence basis. This is just a subset of our domain, algebraically independent over k (i.e. satisfying no non-trivial polynomial in finitely many variables over k) and maximal with respect to this property. Every set of generators contains a transcendence basis and all transcendence bases have the same cardinality—called the *transcendence degree of A over k*. You should skip the proofs of Theorem 3.71 and 3.72 and come back to read them after Chapter 4.

A main step in proving that the finitely generated domains over k are well-behaved is the following important theorem due to E. Noether:

Theorem 3.71 *(Noether Normalization Lemma.) If A is a finitely generated domain over the field k, say $A = k[t_1, \ldots, t_n]$, and if d is the transcendence degree of A over k, then there exists a change of coordinates*

$$y_j = f_j(t_1, \ldots, t_n),$$

in A so that

(1) $y_1, \ldots, y_d$ are a transcendence basis for A over k and

(2) the injection $k[y_1, \ldots, y_d] \hookrightarrow A = k[y_1, \ldots, y_n]$ makes A integral over $k[y_1, \ldots, y_d]$.

If k is infinite, then f_j may be taken to be linear. If Frac A *is separably generated over k, then the y_j may be chosen to be a separating transcendence basis for* Frac A *over k.*

Proof. (Nagata). We prove the theorem by induction on n; the cases $n = 0$ or $n = 1$ are trivial. So, assume the theorem holds up to $n - 1$. If $d = n$, the remarks about transcendence bases just before our proof show that A is already the polynomial ring in n variables; so, again, nothing need be proved. Therefore, we may assume $d < n$. We'll show there exists $y_2, \ldots, y_n$ so that $k[y_2, \ldots, y_n] \hookrightarrow k[t_1, \ldots, t_n] = A$ is an integral morphism (separable in the separating transcendence basis case). If so, then the induction hypothesis applies to $k[y_2, \ldots, y_n]$ and this, together with transitivity of integral dependence and separability, will complete the proof.

Now $d < n$, so relabel the $t_1, \ldots, t_n$ to make t_1 algebraically dependent on $t_2, \ldots, t_n$. We have a non-trivial polynomial relation

$$\sum_{(\alpha)} c_{(\alpha)} t^{(\alpha)} = 0,$$

where $(\alpha) = (\alpha_1, \ldots, \alpha_n)$ is a multi-index and $t^{(\alpha)} = t_1^{\alpha_1} \cdots t_n^{\alpha_n}$. Set

$$y_j = t_j - t_1^{m_j}, \qquad j = 2, \ldots, n,$$

where the m_j are as yet undetermined integers (≥ 0). Then $t_j = y_j + t_1^{m_j}$ and so

$$\sum_{(\alpha)} c_{(\alpha)} t_1^{\alpha_1} (y_2 + t_1^{m_2})^{\alpha_2} \cdots (y_n + t_1^{m_n})^{\alpha_n} = 0.$$

Expand the latter equation by the binomial theorem to obtain the relation

$$\sum_{(\alpha)} c_{(\alpha)} t_1^{(\alpha)\cdot(m)} + G(t_1, y_2, \ldots, y_n) = 0, \tag{$\dagger$}$$

where $(m) = (1, m_2, \ldots, m_n)$ and $(\alpha) \cdot (m)$ stands for the dot product $\alpha_1 + \alpha_2 m_2 + \cdots + \alpha_n m_n$. The polynomial G has degree in t_1 less than the maximum of the exponents $(\alpha) \cdot (m)$. If we can choose the integers $m_2, \ldots, m_n$ so that the products $(\alpha) \cdot (m)$ are all distinct, then ($\dagger$) is an integral dependence of t_1 over $k[y_2, \ldots, y_n]$ as k is a field. But each t_j is expressed as $y_j + t_1^{m_j}$ for $j = 2, \ldots, n$; so each t_j is integral over $k[y_2, \ldots, y_n]$ and therefore $k[t_1, \ldots, t_n]$ is integral over $k[y_2, \ldots, y_n]$. When $k[t_1, \ldots, t_n]$ is separably generated over k, Mac Lane's Theorem (Theorem 4.90) shows we may choose t_1 separable algebraic over $k[t_2, \ldots, t_n]$. Then the relation $\sum_{(\alpha)} c_{(\alpha)} t^{(\alpha)} = 0$ may be chosen to be a separable polynomial in t_1 and the way we will choose the m's (below) will show t_1 is separable over $k[y_2, \ldots, y_n]$. As $t_j = y_j + t_1^{m_j}$, we get the separability of $k[t_1, \ldots, t_n]$ over $k[y_2, \ldots, y_n]$.

Now we must choose the integers $m_2, \ldots, m_n$. For this, consider the differences

$$(\delta)_{\alpha\alpha'} = (\delta_1, \ldots, \delta_n)_{\alpha\alpha'} = (\alpha) - (\alpha')$$

for all possible choices of our distinct multi-indices (α), except that we do not include $(\alpha') - (\alpha)$ if we have included $(\alpha) - (\alpha')$. Say there are N such differences, label them $\delta_1, \ldots, \delta_N$. Form the polynomial

$$H(T_2, \ldots, T_n) = \prod_{j=1}^{N} (\delta_{1j} + \delta_{2j} T_2 + \cdots + \delta_{nj} T_n)$$

here, $\delta_j = (\delta_{1j}, \ldots, \delta_{nj})$ and $T_2, \ldots, T_n$ are indeterminates. None of the δ_j are zero, so H is a non-zero polynomial and it has integer coefficients. It is well-known that there are non-negative integers $m_2, \ldots, m_n$ so that $H(m_2, \ldots, m_n) \neq 0$. Indeed, if b is a non-negative integer larger than any component of any of our (α)'s, then $b, b^2, \ldots, b^{m-1}$ is such a choice. It is also a choice which gives separability. The fact that $H(m_2, \ldots, m_n) \neq 0$ means that the $(\alpha) \cdot (m)$ are distinct.

Finally, assume k is infinite. Just as before, arrange matters so that t_1 depends algebraically (and separably in the separably generated case) on $t_2, \ldots, t_n$. Write the minimal polynomial for t_1 over $k(t_2, \ldots, t_n)$ as

$$P(U, t_2, \ldots, t_n) = 0.$$

We may asume the coefficients of $P(U, t_2, \ldots, t_n)$ are in $k[t_2, \ldots, t_n]$ so that the polynomial $P(U, t_2, \ldots, t_n)$ is the result of substituting $U, t_2, \ldots, t_n$ for $T_1, \ldots, T_n$ in some non-zero polynomial, $P(T_1, \ldots, T_n)$, having coefficients in k. Now perform the linear change of variables

$$y_j = t_j - a_j t_1, \qquad j = 2, \ldots, n,$$

where $a_2, \ldots, a_n$ are elements of k to be determined later. As before, each t_j is $y_j + a_j t_1$; so it suffices to prove that t_1 is integral (and separable in the separably generated case) over $k[y_2, \ldots, y_n]$.

We have

$$P(t_1, y_2 + a_2 t_1, \ldots, y_n + a_n t_1) = 0$$

which gives us

$$t_1^q f(1, a_2, \ldots, a_n) + Q(t_1, y_2, \ldots, y_n) = 0, \tag{$*$}$$

where $f(T_1, \ldots, T_n)$ is the highest degree form of $P(T_1, \ldots, T_n)$ and q is its degree The polynomial, Q, contains just terms of degree lower than q in t_1. If we produce elements a_j in k $(j = 2, 3, \ldots, n)$ so that $f(1, a_2, \ldots, a_n) \neq 0$, then $(*)$ is the required integral dependence of t_1 on the y's. In the separable case, we also need t_1 to be a simple root of its minimal polynomial, i.e.,

$$\frac{dP}{dt_1}(t_1, y_2, \ldots, y_n) \neq 0$$

(c.f. Theorem 4.5 of Chapter 4). By the chain rule, the latter condition is

$$\frac{dP}{dt_1}(t_1, y) = \frac{\partial P}{\partial t_1} + a_2 \frac{\partial P}{\partial t_2} + \cdots + a_n \frac{\partial P}{\partial t_n} \neq 0. \tag{$**$}$$

Now the middle term of $(**)$ is a linear form in $a_2, \ldots, a_n$ and it is not identically zero since on $a_2 = a_3 = \cdots = a_n = 0$ it takes the value $\partial P / \partial t_1$ and the latter is not zero because t_1 is separable over $k(t_2, \ldots, t_n)$ (Theorem 4.5, again). Thus, the vanishing of the middle term of $(**)$ defines a translate of a (linear) hyperplane in $n-1$ space over k, and on the complement of this hyperplane translate we have $dP/dt_1(t_1, y) \neq 0$. The latter complement is an infinite set because k is an infinite field. But from an infinite set we can always choose $a_2, \ldots, a_n$ so that $f(1, a_2, \ldots, a_n) \neq 0$; therefore both our conditions $dP/dt_1(t_1, y) \neq 0$ and $f(1, a_2, \ldots, a_n) \neq 0$ will hold, and the proof is finished. $\square$

The example discussed previously of $\mathbb{C}[X]$ embedded (in the standard way) in $\mathbb{C}[X,Y]/(XY-1)$ is an extremely simple instance of the normalization lemma. Namely, rotate the coordinates

$$X \mapsto X+Y; \quad Y \mapsto X-Y$$

and let $T = 1/2(X+Y)$; $W = 1/2(X-Y)$. Then our situation becomes $\mathbb{C}T$ embedded in $\mathbb{C}[T,W]/(T^2-W^2-1)$, an integral extension. See Figures 3.1 and 3.2 below:

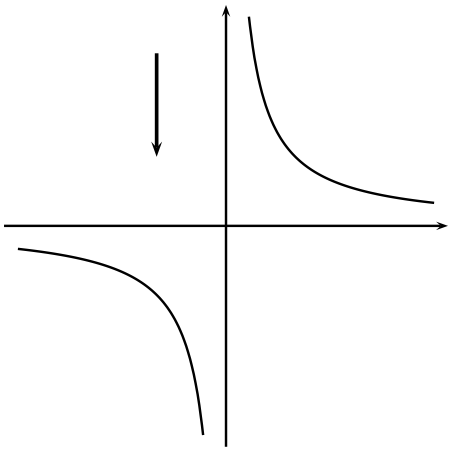


Figure 3.1: Before Normalization: A non-integral morphism

becomes after $\pi/4$ rotation

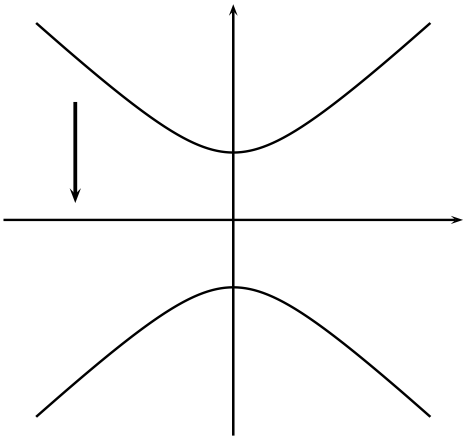


Figure 3.2: After Normalization: An integral morphism

Theorem 3.71 is not the sharpest form of the normalization lemma. Here's an improvement due to Eisenbud based on a previous improvement of Nagata's. We offer no proof as we won't use this sharper version.

Theorem 3.72 *If $A = k[t_1, \dots, t_n]$ is a finitely generated integral domain over a field k with $\mathrm{tr.d}_k\, A = d$ and if we are given a maximal length descending chain of prime ideals of A*

$$\mathfrak{p}_0 > \mathfrak{p}_1 > \cdots > \mathfrak{p}_{d-1} > (0),$$

then there exists a change of coordinates

$$y_j = f_j(t_1, \dots, t_n)$$

so that

(1) $y_1, \dots, y_d$ are a transcendence basis for A over k,

(2) the injection $k[y_1, \dots, y_d] \hookrightarrow A$ makes A integral over $k[y_1, \dots, y_d]$, and

(3) $\mathfrak{p}_j \cap k[y_1, \dots, y_d] = (y_1, \dots, y_{d-j})$.

Here is the promised application of Theorem 3.71 to the well behavedness of finitely generated integral domains over fields.

Theorem 3.73 *When A is a finitely generated integral domain over k and K is a finite extension field over $\mathrm{Frac}(A)$, then $\mathrm{Int}_A(K)$ is both a finitely generated integral domain over k and a finite A-module.*

Proof. We first make two reductions and then treat the main case:

(1) We may assume $K = \mathrm{Frac}\, A$. For if it is known that the integral closure of A in its own fraction field satisfies the conclusions of the theorem, then choose a basis $y_1, \dots, y_s$ for$K$ over $\mathrm{Frac}\, A$ which basis consists of elements from $\mathrm{Int}_A(K)$. This can be done by the argument in the middle of the proof of Theorem 3.69, which argument made no use of any separability hypothesis. Of course, $A[y_1, \dots, y_s]$is both a finite A-module and a finitely generated integral domain over k and its fraction field is K. So by our assumption $\mathrm{Int}_{A[y_1,\dots,y_s]}(K)$ satisfies the conclusions of the theorem. But, clearly, $\mathrm{Int}_A(K) = \mathrm{Int}_{A[y_1,\dots,y_s]}(K)$, which achieves our first reduction.

(2) We may assume both that k is infinite and that $\mathrm{Frac}\, A$ is separably generated over k. (Here, we are already using reduction (1) having replaced K by $\mathrm{Frac}\, A$.) To see this, write Ω for the algebraic closure of $\mathrm{Frac}\, A$ (see Theorem 4.77) and note that Ω contains $\overline{k}$, the algebraic closure of k. Now $\overline{k}$ is both infinite and perfect, so by Corollary 4.91, the field $\overline{k}(t_1, \dots, t_n)$ is separably generated over $\overline{k}$; here, $A = k[t_1, \dots, t_n]$. By our assumption, $\mathrm{Int}_{\overline{k}[t_1,\dots,t_n]}(\overline{k}(t_1, \dots, t_n))$ is a finite $\overline{k}[t_1, \dots, t_n]$-module and a finitely generated $\overline{k}$-algebra, say $\overline{k}[w_1, \dots, w_q]$.

Now by the normalization lemma (in the infinite, separable case) there are $z_1, \dots, z_d$, algebraically independent, which are linear combinations

$$z_j = \sum_{i=1}^{n} \alpha_{ij} t_i$$

of the $t_1, \dots, t_n$ so that $\overline{k}[t_1, \dots, t_n]$ is integral and separable over $\overline{k}[z_1, \dots, z_d]$. Each w_j satisfies a separable, integral dependence

$$g_j(w_j, z_1, \dots, z_d) = 0, \qquad j = 1, 2, \dots, q,$$

over the polynomial ring $\overline{k}[z_1, \dots, z_d]$. Also,

$$\mathrm{Int}_{\overline{k}[z_1,\dots,z_d]}(\overline{k}(t_1, \dots, t_n)) = \overline{k}[w_1, \dots, w_q].$$

Adjoin to k all the coefficients of these q polynomials and all the α_{ij} to get a field, $\widetilde{k}$, of finite degree over k. The entire situation involving $\overline{k}[z$'s] and $\overline{k}[w$'s] comes from the same situation involving $\widetilde{k}[z$'s] and $\widetilde{k}[w$'s]; so, *by the algebraic independence of the z's*, we find

$$\mathrm{Int}_{\widetilde{k}[z_1,\dots,z_d]}(\widetilde{k}(t_1, \dots, t_n)) = \widetilde{k}[w_1, \dots, w_q]$$

and we know

$$\mathrm{Int}_{\widetilde{k}[z_1,\ldots,z_d]}(\widetilde{k}(t_1,\ldots,t_n)) = \mathrm{Int}_{k[t_1,\ldots,t_n]}(\widetilde{k}(t_1,\ldots,t_n)).$$

Of course, $\widetilde{k}[w_1,\ldots,w_q]$ is a finite $\widetilde{k}[t_1,\ldots,t_n]$-module and $\widetilde{k}[t_1,\ldots,t_n]$ is a finite $k[t_1,\ldots,t_n] = A$-module as $\widetilde{k}$ has finite degree over k. Thus, $\widetilde{k}[w_1,\ldots,w_q]$ is a finite A-module as are all of its submodules, A being noetherian. But $\mathrm{Int}_A(\mathrm{Frac}\,A))$ is the submodule $\mathrm{Frac}(A) \cap \widetilde{k}[w_1,\ldots,w_q]$ and as A is a finitely generated k-algebra so is any A-algebra which is a finite A-module. This achieves reduction (2).

Finally we have the case $K = \mathrm{Frac}\,A$, k is infinite and $\mathrm{Frac}\,A$ is separably generated over k. By the normalization lemma, there are linear combinations

$$z_j = \sum_{i=1}^{n} \beta_{ij} t_i, \qquad j = 1,\ldots,d$$

so that $z_1,\ldots,z_d$ are algebraically independent and A is integral and separable over $k[z_1,\ldots,z_d]$. By Theorem 3.69, $\mathrm{Int}_{k[z_1,\ldots,z_d]}(\mathrm{Frac}\,A)$ is a finite $k[z_1,\ldots,z_d]$-module; hence, a finite A-module. Yet, by transitivity of integral dependence,

$$\mathrm{Int}_{k[z_1,\ldots,z_d]}(\mathrm{Frac}\,A) = \mathrm{Int}_A(\mathrm{Frac}\,A).$$

So, $\mathrm{Int}_A(\mathrm{Frac}\,A)$ is a finite A-module; thereby a finitely generated k-algebra, as required. □

The somewhat involved nature of the two finiteness Theorems (Theorems 3.69 and 3.73) indicates the delicate nature of the finiteness of $\mathrm{Int}_A(K)$ as A-module. If the Krull dimension of A is 3 or larger, it can even happen that $\mathrm{Int}_A(K)$ is not noetherian (even if A is so). The Japanese school around Nagata studied these questions and Grothendieck in his algebraic geometry treatise (EGA, IV, part 1, [21]) called attention to the class of domains having the finiteness property together with all their finitely generated algebra extensions. He used the terminology *universally Japanese rings*, but it seems that *Nagata rings* is the one used most often now. The formal definition is this

Definition 3.6 An integral domain, A, is a *Nagata ring* if and only if for every finitely generated A-algebra, B, which is a domain and any finite extension, K, of $\mathrm{Frac}\,B$, the ring $\mathrm{Int}_B(K)$ is a finite B-module.

As a corollary of Theorem 3.69, we see immediately the following

Proposition 3.74 *If A is the ring of integers in a number field (i.e., $A = \mathrm{In}_{\mathbb{Z}}(K)$, where K is a finite extension of $\mathbb{Q}$), then A is a Nagata ring as is $A[t_1,\ldots,t_n]$.*

A main theorem, proved by Nagata, concerning these matters is the following:

Theorem 3.75 *(Nagata) Say A is a complete, noetherian local domain, and K is a finite degree extension field of* $\mathrm{Frac}(A)$*, then* $\mathrm{Int}_A(K)$ *is a finitely generated A-algebra and a finite A-module.*

This theorem is not part of our purview, nor will we use it; so, its proof is omitted.

There is another finiteness result involving integrality which has many uses.

Proposition 3.76 *(E. Noether) If B is a finitely generated A-algebra, A being noetherian, and if C is a sub A-algebra of B so that B is integral over C, then C is a finitely generated A-algebra.*

Proof. Write $B = A[t_1,\ldots,t_n]$; each t_j satisfies an integral dependence over C

$$g_j(t_j) = 0, \qquad j = 1,\ldots,n.$$

If $\alpha_1, \ldots, \alpha_q$ are the coefficients ($\in C$) of all these equations, form $A[\alpha_1, \ldots, \alpha_q] \subseteq C$. The t_i are integral over $A[\alpha_1, \ldots, \alpha_q]$ and they generate B; so, B is a finite $A[\alpha_1, \ldots, \alpha_q]$-module. But C is a sub $A[\alpha_1, \ldots, \alpha_q]$-module of B and $A[\alpha_1, \ldots, \alpha_q]$ is noetherian. Therefore, C is a finitely generated $A[\alpha_1, \ldots, \alpha_q]$-module, say $C = A[\alpha_1, \ldots, \alpha_q][z_1, \ldots, z_s]$; we are done. □

What happens if $A \subseteq \mathrm{Frac}(A)$ is not a normal domain? Of course we'll form $\mathrm{Int}_A(\mathrm{Frac}(A)) = \widetilde{A}$, then we want to study the relations between A and $\widetilde{A}$. For example look at

$$A = \mathbb{Z}[ni], \quad n \in \mathbb{Z} \quad \text{and} \quad n > 0$$

and

$$\widetilde{A} = \mathrm{Int}_A(\mathbb{Q}(i)) = \mathbb{Z}[i].$$

The main invariant controlling the relations between A and $\widetilde{A}$ is the transporter $(\widetilde{A} \longrightarrow A)$ in A. That is, we examine

$$f = (\widetilde{A} \longrightarrow A) = \{\xi \in A \mid \xi\widetilde{A} \subseteq A\}.$$

The set f is, of course, an ideal of A; it is called the *conductor* of A in $\widetilde{A}$ or just the *conductor of the integral closure of* A. The symbol f comes from the German word for conductor: Führer. But, clearly, f is also an ideal of $\widetilde{A}$. In the example above,

$$f = \{\xi \in \mathbb{Z}[ni] \mid n | \Re(\xi)\}.$$

Remark: The domain, A, is normal if and only if f is the unit ideal. An ideal, $\mathfrak{A}$, of A which is also an ideal of $\widetilde{A}$ must necessarily be contained in the conductor, f. That is, f is the unique largest ideal of A which is simultaneously an ideal of $\widetilde{A}$.

The first of these statetements is obvious; for the second, we have $\mathfrak{A}\widetilde{A} \subseteq \mathfrak{A}$ as $\mathfrak{A}$ is an $\widetilde{A}$-ideal and $\mathfrak{A} \subseteq A$ as $\mathfrak{A}$ is an A-ideal. Thus,

$$\mathfrak{A}\widetilde{A} \subseteq \mathfrak{A} \subseteq A$$

and this says $\mathfrak{A} \subseteq (\widetilde{A} \longrightarrow A) = f$.

The connection between A and $\widetilde{A}$ *vis a vis* localization and prime ideals is this:

Proposition 3.77 *For a domain, A, its integral closure $\widetilde{A}$ and the conductor, f, of A in $\widetilde{A}$ we have*

(1) If S is a multiplicative set in A, then $S^{-1}\widetilde{A} = \mathrm{Int}_{S^{-1}A}(\mathrm{Frac}(A))$

(2) If $f \cap S \neq \emptyset$, then $S^{-1}A = S^{-1}\widetilde{A}$, that is $S^{-1}A$ is normal.

(3) If $\widetilde{A}$ is a finite A-module then the conductor of $S^{-1}A$ in $S^{-1}\widetilde{A}$ is $f \cdot S^{-1}A = f^e$.

(4) If $\widetilde{A}$ is a finite A-module, them $S^{-1}A$ is normal if and only if $f \cap S \neq \emptyset$.

(5) If $\widetilde{A}$ is a finite A-module, then

$$\{\mathfrak{p} \in \mathrm{Spec}\, A \mid A_\mathfrak{p} \quad \textit{is} \textbf{ not } \textit{normal}\}$$

is closed in Spec A*; indeed it is $V(f)$. Hence, in this case, $A_\mathfrak{p}$ is a normal ring on an open dense set of* Spec A.

Proof. (1) This is clear from Proposition 3.54 and Fact B following it.

(2) Write $s \in f \cap S$ and choose $\alpha \in \widetilde{A}$. We know $s\alpha = a \in A$; so, $\alpha = a/s \in S^{-1}A$. We find $\widetilde{A} \subseteq S^{-1}A$, hence $S^{-1}\widetilde{A} \subseteq S^{-1}A$. The other inclusion is clear.

(3) Write $\alpha_1, \ldots, \alpha_t$ for a finite set of A-module generators for $\widetilde{A}$ in this part and in part (4). To check that an element $x \in S^{-1}A$ lies in $(S^{-1}\widetilde{A} \longrightarrow S^{-1}A)$, it suffices to see that it is in $(\widetilde{A} \longrightarrow S^{-1}A)$. For the latter, all we need is $x\alpha_j \in S^{-1}A$ for $j = 1, \ldots, t$. Conversely, if $x \in (S^{-1}\widetilde{A} \longrightarrow S^{-1}A)$, then certainly $x\alpha_j \in S^{-1}A$, all j.

Now $x\alpha_j \in S^{-1}A$ implies there is some $s_j \in S$ with $s_j x\alpha_j \in A$. If $s = s_1 \cdots s_t$, then $sx\alpha_j \in A$ therefore $sx \in f$, i.e., $x \in f^e$. The converse is clear.

(4) The "if" part of our conclusion is (2), so say $S^{-1}A$ is normal. Then the conductor $(S^{-1}\widetilde{A} \longrightarrow S^{-1}A)$ is the unit ideal; so, (3) shows $f^e =$ unit ideal. This implies $f \cap S \neq \emptyset$.

(5) Write $S(\mathfrak{p})$ for $A - \mathfrak{p}$, then $A_{\mathfrak{p}}$ is not normal iff $f \cap S(\mathfrak{p}) = \emptyset$ which holds iff $f \subseteq \mathfrak{p}$; that is iff $\mathfrak{p} \in V(f)$. To finish the proof we need only show that any non-empty open set of Spec A is dense when A is a domain. But, this will hold if we show $X_f \cap X_g \neq \emptyset$ (provided neither X_f nor X_g is empty) (DX). However, $X_f \cap X_g = X_{fg}$, and, as neither f nor g is zero, their product is non-zero (and not nilpotent). Now apply Proposition 3.12 part (3). □

Corollary 3.78 *For a domain A and its integral closure, $\widetilde{A}$, assume $\widetilde{A}$ is a finite A-module. Then, for a prime $\mathfrak{p}$ of* Spec A *not in $V(f)$, there exists one and only one prime ideal, $\widetilde{\mathfrak{p}}$, of $\widetilde{A}$ lying over A. This prime ideal is $\mathfrak{p}A_{\mathfrak{p}} \cap \widetilde{A}$.*

Proof. Existence is clear either by the Lying Over Theorem or by the fact that $\mathfrak{p}A_{\mathfrak{p}}$ is prime and $A_{\mathfrak{p}} \supseteq \widetilde{A}$. (The latter holds as $A_{\mathfrak{p}}$ is normal since $\mathfrak{p} \notin V(f)$.) To see uniqueness, observe as $\mathfrak{p} \not\supseteq f$ there is $\delta \in f$ with $\delta \notin \mathfrak{p}$. Then for any ideal, $\mathfrak{A}$, of $\widetilde{A}$

$$\delta\mathfrak{A} \subseteq \delta\widetilde{A} \subseteq A$$

and $\delta\mathfrak{A} \subseteq \mathfrak{A}$, too. Therefore $\delta\mathfrak{A} \subseteq \mathfrak{A} \cap A$; so if $\mathfrak{A}$ is an ideal contracting to $\mathfrak{p}$ we get $\delta\mathfrak{A} \subseteq \mathfrak{p}$. Now, $\delta \notin \mathfrak{p}$, therefore $\mathfrak{A} \subseteq \mathfrak{p}A_{\mathfrak{p}}$, so $\mathfrak{A} \subseteq \mathfrak{p}A_{\mathfrak{p}} \cap \widetilde{A} = \widetilde{\mathfrak{p}}$. Suppose, in fact, $\mathfrak{A}$ is prime yet $\mathfrak{A} < \widetilde{\mathfrak{p}}$, then we'd have a contradiction to non-comparability (Proposition 3.62). □

Note: Generally, $\mathfrak{p}\widetilde{A}$ is not a prime ideal of $\widetilde{A}$; but, of course, $\mathfrak{p}\widetilde{A}$ is always contained in $\widetilde{\mathfrak{p}}$.

3.6 Primary Decomposition

In $\mathbb{Z}$, we have unique factorization and we know this is not valid in an arbitrary (even Noetherian) commutative ring. Can one generalize so as to obtain a "decomposition" of ideals (or submodules) into special ideals (resp. modules) which resemble prime powers? Surprisingly, the answer is connected with a generalization of Fitting's lemma from linear algebra.

Lemma 3.79 *(Fitting's lemma) If V is a finite dimensional vector space over a field, k, and $\theta\colon V \to V$ is an endomorphism, then there exist subspaces W and Z of V so that*

(1) $V = W \coprod Z$.

(2) $\theta \restriction W$ *is an isomorphism.*

(3) $\theta \restriction Z$ *is nilpotent.*

Proof. See any introductory algebra text. □

Look at $\mathbb{Z}$. Pick n, then we have the ideal $\mathfrak{A} = n\mathbb{Z}$. Factor n as $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where $p_1, \ldots, p_t$ are distinct prime numbers. We get $\mathfrak{A} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_t^{e_t}$, where $\mathfrak{P}_j$ is the prime ideal $p_j\mathbb{Z}$. Now, we also have $\mathfrak{A} = \bigcap_{j=1}^{t} \mathfrak{P}_j^{e_j}$, since the $\mathfrak{P}_j$ are pairwise comaximal.

This last equality is still wrong, say in $\mathbb{C}[X, Y]$, and the fault is the $\mathfrak{P}_i^{e_i}$. They are not general enough.

Let A be a commutative ring, M an A-module and $N \subseteq M$ a submodule. Set

$$\mathrm{Rad}_M(N) = \sqrt{(M \longrightarrow N)} = \sqrt{\{x \in A \mid xM \subseteq N\}} = \{x \in A \mid (\exists k > 0)(x^k M \subseteq N)\}.$$

This is the *relative radical of N in M*. The following properties are easily checked:

(1) $\mathrm{Rad}_{M/N}((0)) = \mathrm{Rad}_M(N)$.

(2) $\mathrm{Rad}_M((0)) = \sqrt{\mathrm{Ann}(M)}$.

(3) $\mathrm{Rad}_A(\mathfrak{q}) = \sqrt{\mathfrak{q}}$.

(3a) $\mathrm{Rad}_{A/\mathfrak{q}}((0)) = \sqrt{\mathfrak{q}}$.

(4) $\mathrm{Rad}_M(N \cap P) = \mathrm{Rad}_M(N) \cap \mathrm{Rad}_M(P)$.

(5) $\mathrm{Rad}_M(\mathfrak{A}N) \supseteq \sqrt{\mathfrak{A}} \cap \mathrm{Rad}_M(N)$.
Here, $\mathfrak{A}$ is an ideal of A; M is an A-module; N is a submodule of M.

Definition 3.7 A module, M, is *coprimary* iff for every $a \in A$, the map $\sigma_a\colon M \to M$ *via* $\sigma_a(m) = am$ is either injective or nilpotent. (The map σ_a is called a *homothety*.) An ideal, $\mathfrak{q}$, of A is a *primary ideal* iff the module, $A/\mathfrak{q}$, is coprimary.

Notice the clear connection of this idea with Fitting's lemma.

Proposition 3.80 *For any commutative ring, A, and any ideal, $\mathfrak{q}$, the following are equivalent:*

(α) For all $x, y \in A$ if $xy \in \mathfrak{q}$ but $y \notin \mathfrak{q}$, then $x^k \in \mathfrak{q}$, for some $k \geq 1$.

(β) For all $y \notin \mathfrak{q}$, we have $(y \longrightarrow \mathfrak{q}) \subseteq \sqrt{\mathfrak{q}}$.

(γ) $\bigcup_{y \notin \mathfrak{q}} (y \longrightarrow \mathfrak{q}) = \sqrt{\mathfrak{q}}$.

(δ) Every zero divisor of the ring $A/\mathfrak{q}$ is nilpotent.

(ϵ) The ideal $\mathfrak{q}$ is primary.

Proof. The equivalence $(\alpha) \Longleftrightarrow (\beta)$ is clear and the implication $(\gamma) \Longrightarrow (\beta)$ is a tautology. If (β), then pick $\xi \in \sqrt{\mathfrak{q}}$. If $\xi \in \mathfrak{q}$, then $\xi \in (y \longrightarrow \mathfrak{q})$ for all y. Thus, we may assume that $\xi \notin \mathfrak{q}$ and so, there is a minimum $k \geq 2$ so that $\xi^k \in \mathfrak{q}$. Let $y = \xi^{k-1} \notin \mathfrak{q}$. We have $\xi y = \xi^k \in \mathfrak{q}$, so, $\xi \in (\xi^{k-1} \longrightarrow \mathfrak{q})$ and (γ) holds.

$(\alpha) \Longrightarrow (\delta)$. Pick $\overline{x} \in A/\mathfrak{q}$, a zero divisor, which means that there is some $\overline{y} \neq 0$ with $\overline{x}\,\overline{y} = 0$. It follows that $y \notin \mathfrak{q}$ and $xy \in \mathfrak{q}$; by (α), we get $x^k \in \mathfrak{q}$, for some k, and so, $\overline{x}^k = 0$.

$(\delta) \Longrightarrow (\epsilon)$. Pick $a \in A$. We need to show that σ_a is injective or nilpotent in $A/\mathfrak{q}$. Say σ_a is not injective. Then, there is some $\overline{y} \neq 0$ in $A/\mathfrak{q}$ and $a\overline{y} = 0$ in $A/\mathfrak{q}$, i.e. $\overline{a}\,\overline{y} = 0$. But, $\overline{y} \neq 0$, so, by (δ), $\overline{a}$ is nilpotent. Consequently, $\overline{a}^k = 0$, and so, $(\sigma_a)^k = 0$ in $A/\mathfrak{q}$.

$(\epsilon) \Longrightarrow (\alpha)$. Pick x, y with $xy \in \mathfrak{q}$ and $y \notin \mathfrak{q}$. Look at σ_x on $A/\mathfrak{q}$. We have

$$\sigma_x(\overline{y}) = \overline{x}\,\overline{y} = \overline{xy} = 0, \quad \text{as } xy \in \mathfrak{q}.$$

As $\overline{y} \neq 0$, the map σ_x is not injective on $A/\mathfrak{q}$. By (ϵ), the map σ_x is nilpotent. This means that $(\sigma_x)^k = \sigma_{x^k} = 0$ in $A/\mathfrak{q}$. In particular, $\sigma_{x^k}(1) = \overline{x}^k 1 = 0$, i.e., $\overline{x^k} = 0$. Therefore, $x^k \in \mathfrak{q}$. □

Corollary 3.81 *If $\sqrt{\mathfrak{q}}$ is maximal, then $\mathfrak{q}$ is primary. In particular, if $\mathfrak{m}$ is a maximal ideal, then $\mathfrak{m}^n$ is primary for all $n > 0$.*

Proof. The image of $\sqrt{\mathfrak{q}}$ in $A/\mathfrak{q}$ is the nilradical of $A/\mathfrak{q}$. Since $\sqrt{\mathfrak{q}}$ is maximal in A, the ring $A/\mathfrak{q}$ has a unique maximal ideal. It follows that every element of $A/\mathfrak{q}$ is either a unit or nilpotent, so Proposition 3.80 (3) applies. The second part of the statement follows from the first since $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for every prime ideal, $\mathfrak{p}$. □

There exist prime ideals, $\mathfrak{p}$, such that $\mathfrak{p}^n$ is not primary. There exist primary ideals, $\mathfrak{q}$, **not** of the form $\mathfrak{p}^n$, where $\mathfrak{p} \in \operatorname{Spec} A$.

Corollary 3.82 *Say $\mathfrak{q}$ is a primary ideal of A, then $\sqrt{\mathfrak{q}}$ is a prime ideal.*

Proof. Pick $x, y \in A$ with $xy \in \sqrt{\mathfrak{q}}$ and $y \notin \sqrt{\mathfrak{q}}$. Then, $x^k y^k = (xy)^k \in \mathfrak{q}$, for some $k > 0$. So, $\sigma_{x^k}(\overline{y}^k) = 0$ in $A/\mathfrak{q}$ and $\overline{y}^k \neq 0$ in $A/\mathfrak{q}$. Therefore, our homothety, σ_{x^k}, is nilpotent, so, σ_x is nilpotent, i.e., $(\sigma_x)^l \equiv 0$ on $A/\mathfrak{q}$. Then, $(\sigma_x)^l(1) = x^l \cdot 1 = x^l = 0$ in $A/\mathfrak{q}$, and so, $x^l \in \mathfrak{q}$, i.e., $x \in \sqrt{\mathfrak{q}}$. □

There exist *non-primary ideals*, $\mathfrak{A}$, yet $\sqrt{\mathfrak{A}}$ *is* prime.

Definition 3.8 A submodule, N, of a module, M, is *primary in M* iff M/N is co-primary. Then, $\operatorname{Rad}_M(N)$ is prime (same argument), say $\mathfrak{p}$. In this case, we say N is $\mathfrak{p}$-primary when M/N is $\mathfrak{p}$-coprimary, *i.e.*, M/N is coprimary and $\operatorname{Rad}_M(N) = \mathfrak{p}$.

Say M is an A-module, N is a submodule of M and S is a multiplicative set in A. Look at

$$N^{ec} = \{m \in M \mid (\exists s \in S)(sm \in N)\} = S(N),$$

and call it the *S-component* of N or *S-saturation* of N.

Further Properties:

(6) $S((0)) = \operatorname{Ker}(M \longrightarrow S^{-1}M)$.

(7) $S(\bigcap_{i=1}^t N_i) = \bigcap_{i=1}^t S(N_i)$.

(8) $S(V \longrightarrow N) = (V \longrightarrow S(N))$.

Proposition 3.83 *If A is a commutative ring, M is a f.g. A-module and N a submodule of M, then the following are equivalent:*

(1) N is primary in M.

(2) For all multiplicative sets, $S \subseteq A$, we have

$$S(N) = \begin{cases} N \\ \qquad \text{or} \\ M. \end{cases}$$

(3) For all multiplicative sets, $S \subseteq A$, the map $M/N \longrightarrow S^{-1}(M/N)$ is either injective or zero.

Proof. Note that $S_{M/N}(0) = \overline{S(N)} = \text{Ker}\,(M/N \longrightarrow S^{-1}(M/N))$. Therefore, (2) and (3) are equivalent.

(1) $\Longrightarrow$ (2). Take any S and examine $\sqrt{(M \longrightarrow N)} = \text{Rad}_{M/N}((0))$. There are two cases:
(1) $S \cap \text{Rad}_{M/N}((0)) = \emptyset$ or (2) $S \cap \text{Rad}_{M/N}((0)) \neq \emptyset$.

Case 2. There is some $s \in S$ with $s \in \text{Rad}_{M/N}((0))$. So, $s^k \in (M \longrightarrow N)$ and then $s^k \in S$ implies that $M \subseteq S(N)$; thus, $M = S(N)$.

Case 1. Pick $s \in S$ and look at σ_s. If σ_s is nilpotent on M/N, then $(\sigma_s)^k = \sigma_{s^k} \equiv 0$ on M/N, which implies that $s^k M \subseteq N$. So, $s \in \sqrt{(M \longrightarrow N)} \cap S$, a contradiction. Therefore, σ_s must be injective on M/N, by (1). This means given any $m \in M$, we have $\sigma_s(\overline{m}) = s\overline{m} = 0$ in M/N iff $m \in N$, already, i.e., $sm \in N$ iff $m \in N$. As this holds for all $s \in S$, we have $S(N) = N$.

(2) $\Longrightarrow$ (1). Pick $s \in A$ and look at $S = \{s^k \mid k \geq 0\}$. If $s \in \mathcal{N}(A)$, then $(\sigma_s)^k = \sigma_{s^k} \equiv 0$ on *any* module. So, we may assume $s \notin \mathcal{N}(A)$ and then, S is a multiplicative set. Thus, (2) holds for S. We have to show that M/N is coprimary, i.e., σ_s is either nilpotent or injective. Say, σ_s is not injective on M/N, i.e., $S(N) \neq N$. By (2), we have $S(N) = M$. Pick generators, $m_1, \ldots, m_t$ for M. As $S(N) = M$, each $m_j \in S(N)$; so, there is some k_j with $s^{k_j} m_j \in N$, for $j = 1, \ldots, t$. Let $k = \max\{k_1, \ldots, k_t\}$, then $s^k m_j \in N$, for $j = 1, \ldots, t$. It follows that $s^k M \subseteq N$ and so, s^k kills M/N, i.e. σ_s is nilpotent on M/N. □

Proposition 3.84 *(E. Noether, 1921) If M is a noetherian module, then any non-primary submodule, N, of M is reducible, i.e., N is the intersection, $N = Q_1 \cap Q_2$, of proper submodules of M properly containing N.*

Proof. (Adapted from Fitting's lemma.) Since N is non-primary, M/N is not coprimary. So, there is some $a \in A$ so that σ_a is not injective and not nilpotent on M/N. Write $\overline{M_j} = \text{Ker}\,(\sigma_a)^j = \text{Ker}\,(\sigma_{a^j})$ on M/N. We have an ascending chain

$$\overline{M_1} \subseteq \overline{M_2} \subseteq \overline{M_3} \subseteq \cdots .$$

By the ACC, the chain stops, say at r. We have $\overline{M_r} = \overline{M_{r+1}} = \cdots = \overline{M_{2r}}$. Let $\varphi = \sigma_{a^r} \in \text{End}_A(M/N)$. We have $\text{Ker}\,\varphi \neq M/N$, else $(\sigma_a)^r \equiv 0$, contradicting the non-nilpotence of σ_a. So, $\text{Im}\,\varphi \neq (0)$. Also, $\text{Ker}\,\varphi \supseteq \text{Ker}\,\sigma_a \neq (0)$, as σ_a is not injective. I claim that $\text{Ker}\,\varphi \cap \text{Im}\,\varphi = (0)$.

Pick $\xi \in \text{Ker}\,\varphi \cap \text{Im}\,\varphi$. So, $\xi = \varphi(\eta) = a^r\eta$. As $\varphi(\xi) = 0$, we have $\varphi(a^r\eta) = 0$; thus $a^r\varphi(\eta) = 0$, and so, $a^{2r}\eta = 0$, i.e., $\eta \in \overline{M_{2r}} = \overline{M_r}$. Consequently, $a^r\eta = 0$, i.e., $\xi = 0$, as desired. But, now, $\text{Ker}\,\varphi \cap \text{Im}\,\varphi = (0)$ implies that

$$N = \pi^{-1}(\text{Ker}\,\varphi) \cap \pi^{-1}(\text{Im}\,\varphi),$$

where $\pi\colon M \to M/N$ is the natural projection. □

We need a restatement of a Proposition 3.83 for the reduction process:

Proposition 3.85 *Say N is a submodule of M, and $\mathfrak{p}$ is a given prime ideal.*

(a) N is $\mathfrak{p}$-primary in M iff for all multiplicative sets, S, of A, we have

$$S(N) = \begin{cases} N & \text{iff } \mathfrak{p} \cap N = \emptyset \\ M & \text{iff } \mathfrak{p} \cap N \neq \emptyset. \end{cases}$$

(b) If $N_1, \ldots, N_t$ are all $\mathfrak{p}$-primary, then $N_1 \cap \cdots \cap N_t$ is again $\mathfrak{p}$-primary.

(c) If V is any submodule of M, then when N is $\mathfrak{p}$-primary, we have

$$S(V \longrightarrow N) = \begin{cases} A & \text{iff } V \subseteq N \\ \mathfrak{p}\text{-primary ideal} & \text{iff } V \not\subseteq N. \end{cases}$$

Proof. (a) The module N is primary iff M/N is coprimary iff $S((0)) = (0)$ or $S((0)) = M/N$, for any multiplicative subset, S (where $(0) \subseteq M/N$) iff $S(N) = N$ or $S(N) = M$, for any such S. (Recall, $S((0)) = \overline{S(N)}$.) But, the dichotomy: $S(N) = N$ or M, depends on $S \cap \mathrm{Rad}_M(N) = S \cap \mathrm{Rad}_{M/N}((0)) = S \cap \sqrt{(M \longrightarrow N)}$. Namely, $S(N) = N$ iff $S \cap \mathrm{Rad}_M(N) = \emptyset$ and $S(N) = M$ iff $S \cap \mathrm{Rad}_M(N) \neq \emptyset$. But here, $\mathfrak{p} = \mathrm{Rad}_M(N)$, so (a) is proved.

(b) Now, $S(\bigcap_{i=1}^t N_i) = \bigcap_{i=1}^t S(N_i)$, so (a) implies (b).

(c) If $V \subseteq N$, then $(V \longrightarrow N) = A$, so, $S(V \longrightarrow N) = A$. So, we may assume $V \not\subseteq N$. Recall that $S(V \longrightarrow N) = (V \longrightarrow S(N))$. We will test $S(V \longrightarrow N)$ by part (a) (here, $M = A$). But,

$$S(N) = \begin{cases} M & \text{iff } S \cap \mathfrak{p} \neq \emptyset \\ N & \text{iff } S \cap \mathfrak{p} = \emptyset. \end{cases}$$

In the case $S \cap \mathfrak{p} \neq \emptyset$, we have $S(V \longrightarrow N) = (V \longrightarrow M) = A$. If $S \cap \mathfrak{p} = \emptyset$, then $S(V \longrightarrow N) = (V \longrightarrow N)$, and the test of (a) shows (c). □

Reduction Process for Primary Decomposition

Say $N = Q_1 \cap Q_2 \cap \cdots \cap Q_t$ is a decomposition of N as a finite intersection of $\mathfrak{p}_i$-primary modules, Q_i.

No assertion $\mathfrak{p}_i \neq \mathfrak{p}_j$ is made.

(1) Remove all Q_j from the intersection $\bigcap_{i=1}^t Q_i$, whose removal does not affect the intersection.

(2) Lump together as an intersection all the Q_i's for which the $\mathfrak{p}_i$'s agree. By (b), the "new" intersection satisfies:

(α) No $\widetilde{Q}_j$, still primary, can be removed without changing the intersection.

(β) All the $\mathfrak{p}_j$ $\left(= \sqrt{(M \longrightarrow \widetilde{Q}_j)}\right)$ are distinct.

Such a primary decomposition is called *reduced*.

Theorem 3.86 *(Lasker-Noether Decomposition Theorem, 1921) Every submodule, N, of a noetherian module, M, can be represented as a reduced primary decomposition:*

$$N = Q_1 \cap Q_2 \cap \cdots \cap Q_t.$$

Proof. (Noetherian induction—invented for this theorem.) Let

$$\mathcal{S} = \{N \subseteq M \mid N \text{ is not a finite intersection of primary submodules}\}.$$

If $\mathcal{S} \neq \emptyset$, by the ACC, the set $\mathcal{S}$ has maximal element. Call it N. Of course, N is not primary. By Noether's proposition (Proposition 3.84), there exist $Q_1, Q_2 > N$, so that $N = Q_1 \cap Q_2$. But N is maximal in $\mathcal{S}$, so

$Q_j \notin \mathcal{S}$ for $j = 1, 2$. Thus, we can write $Q_1 = \bigcap_{j=1}^{t_1} Q_j^{(1)}$ and $Q_2 = \bigcap_{k=1}^{t_2} Q_j^{(2)}$, where the $Q_j^{(i)}$ are primary ($i = 1, 2$, finitely many j's). Consequently, we get

$$N = Q_1^{(1)} \cap \cdots \cap Q_{t_1}^{(1)} \cap Q_1^{(2)} \cap \cdots \cap Q_{t_2}^{(2)},$$

contradicting $N \in \mathcal{S}$. Therefore, $\mathcal{S} = \emptyset$. Now apply the reduction process to a primary decomposition of N and we get the conclusion. □

Corollary 3.87 *(Lasker's Decomposition Theorem, original form, 1905) If $A = \mathbb{C}[X_1, \ldots, X_n]$, then every ideal, $\mathfrak{A}$, admits a reduced primary decomposition: $\mathfrak{A} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$.*

Corollary 3.88 *(Noether's statement) If A is any noetherian ring and $\mathfrak{A}$ is any ideal of A, then $\mathfrak{A}$ admits a reduced primary decomposition: $\mathfrak{A} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$.*

Now, what about uniqueness?

Proposition 3.89 *Say that N is an A-submodule of M, and $N = Q_1 \cap \cdots \cap Q_t$ is a reduced primary decomposition for N. Let $I = \{1, \ldots, t\}$ and given any multiplicative subset, S, of A, write*

$$S(I) = \{i \in I \mid S \cap \mathfrak{p}_i = \emptyset\}.$$

Here, $\mathfrak{p}_i = \mathrm{Rad}_M(Q_i)$ is the prime associated to Q_i. Then,

(a) $$S(N) = \bigcap_{j \in S(I)} Q_j.$$

(b) $$S^{-1}Q_i = \begin{cases} S^{-1}M & \text{if } i \notin S(I) \\ \mathfrak{p}_i^e\text{-primary submodule of } S^{-1}M & \text{if } i \in S(I). \end{cases}$$

(c) $$S^{-1}N = \bigcap_{j \in S(I)} S^{-1}Q_j,$$

and this is a reduced primary decomposition for $S^{-1}N$ as submodule of $S^{-1}M$.

Proof. (a) We know that $S(N) = \bigcap_{j=1}^{t} S(Q_j)$ and $S(Q_j) = M$ when $j \notin S(I)$ and $S(Q_j) = Q_j$ for $j \in S(I)$ (previous proposition). Thus, it is clear that (a) holds.

(b) Now, Q_i is $\mathfrak{p}_i$-primary, so $S(Q_i) = M$ if $\mathfrak{p}_i \cap S \neq \emptyset$ else $S(Q_i) = Q_i$ or equivalently, $S((0)) = M/Q_i$ if $i \notin S(I)$ else $S((0)) = (0)$ (where (0) is the zero ideal in M/Q_i). Say, $i \notin S(I)$, then $S(Q_i) = M$, and so, for every $m \in M$, there is some $s = s(m) \in S$ with $sm \in Q_i$. Hence, $m/1 \in S^{-1}Q_i$ and it follows that $S^{-1}M \subseteq S^{-1}Q_i$; yet, of course, $S^{-1}Q_i \subseteq S^{-1}M$, so $S^{-1}Q_i = S^{-1}M$, as required. Now, say $i \in S(I)$, so $\mathfrak{p}_i \cap S = \emptyset$. Observe, every multiplicative set, say T, of $S^{-1}A$, has the form $S^{-1}T_0$, for some multiplicative set, T_0, of A. But, M/Q_i is coprimary which means that $M/Q_i \longrightarrow T_0^{-1}(M/Q_i)$ is either injective (case: $T_0((0)) = (0)$) or zero (case: $T_0((0)) = M/Q_i$)). Therefore, as $S^{-1}A$ is flat over A, we get

$$S^{-1}(M/Q_i) \longrightarrow S^{-1}T_0^{-1}(M/Q_i) \quad \text{is injective or zero,} \tag{$*$}$$

the first if $T_0 \cap \mathfrak{p}_i = \emptyset$, i.e., $T(= S^{-1}T_0) \cap \mathfrak{p}_i^e = \emptyset$, the second if $T_0 \cap \mathfrak{p}_i \neq \emptyset$, i.e., $T(= S^{-1}T_0) \cap \mathfrak{p}_i^e \neq \emptyset$. But, $S^{-1}T_0^{-1}(M/Q_i) = T^{-1}(S^{-1}M/S^{-1}Q_i)$ and $S^{-1}M/S^{-1}Q_i = S^{-1}(M/Q_i)$, so

$$S^{-1}M/S^{-1}Q_i \longrightarrow T^{-1}(S^{-1}M/S^{-1}Q_i) \quad \text{is injective or zero}$$

depending on $T \cap \mathfrak{p}_i^e$ being empty or not. Therefore, $S^{-1}Q_i$ satisfies our test for $\mathfrak{p}_i^e$-primariness.

(c) We know from (b) that $S^{-1}Q_j$ is $\mathfrak{p}_j^e$-primary and $\mathfrak{p}_i^e \neq \mathfrak{p}_j^e$ if $i \neq j$, as $i, j \in S(I)$ and there is a one-to-one correspondence between the $\mathfrak{p}$'s so that $\mathfrak{p} \cap S = \emptyset$ and the $\mathfrak{p}^e$ of $S^{-1}A$. The rest should be obvious (DX). □

Theorem 3.90 *(First Uniqueness Theorem) If N, an A-submodule of M, has a reduced primary decomposition $N = Q_1 \cap \cdots \cap Q_t$, then the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ ($\mathfrak{p}_i = \sqrt{(M \longrightarrow Q_i)}$) are uniquely determined by N and M, up to the order of their listing.*

Proof. Assume that $N = Q_1 \cap \cdots \cap Q_s = Q'_1 \cap \cdots \cap Q'_t$ are two reduced decompositions for N in M. We use induction on $s+t$. When $s+t=2$, we have $s=t=1$ and $Q_1 = Q'_1$ and uniqueness is obvious. Assume that uniqueness holds for all submodules, N, for which $s+t \leq r-1$. Consider N and two decompositions with $s+t=r$ and let

$$S = A - \bigcup_{i=1}^{s-1} \mathfrak{p}_i - \bigcup_{\mathfrak{p}'_j \neq \mathfrak{p}_s} \mathfrak{p}'_j.$$

Now, $S \cap \mathfrak{p}_i = \emptyset$ for $i = 1, \ldots, s-1$ and $S \cap \mathfrak{p}'_j = \emptyset$ for all j with $\mathfrak{p}'_j \neq \mathfrak{p}_s$. So,

$$S(N) = \bigcap_{i=1}^{s} S(Q_i) = \bigcap_{i=1}^{s-1} Q_i$$

as $S(Q_i) = Q_i$ whenever $S \cap \mathfrak{p}_i = \emptyset$. Also,

$$S(N) = \bigcap_{\mathfrak{p}'_j \neq \mathfrak{p}_s} S(Q'_j) = \bigcap_{\mathfrak{p}'_j \neq \mathfrak{p}_s} Q'_j.$$

For $S(N)$, the sum of the number of components is at most $s-1+t < r$; so, the induction hypothesis implies $S(N)$ has the uniqueness property. However, can it be that $\mathfrak{p}'_j \neq \mathfrak{p}_s$ for $j = 1, \ldots, t$? Were that true, the second intersection would give $S(N) = \bigcap_{j=1}^{t} Q'_j = N$. Thus, we would have

$$\bigcap_{i=1}^{s} Q_i = N = S(N) = \bigcap_{j=1}^{s-1} Q_j,$$

contradicting the fact that the first decomposition is reduced. Therefore, there is some j with $\mathfrak{p}'_j = \mathfrak{p}_s$, and now the induction hypothesis implies

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}\} = \{\mathfrak{p}'_j \mid \mathfrak{p}'_j \neq \mathfrak{p}_s\},$$

and the proof is complete. □

Definition 3.9 If N is a submodule of M and N has a primary decomposition, then the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ corresponding to the Q_j's which appear in the decomposition are called the *essential primes of N in M*. The set of such is denoted $\mathrm{Ess}_M(N)$. When $N = (0)$, the primes appearing are called *associated primes of M* and this set is denoted $\mathrm{Ass}(M)$. Of course, $\mathrm{Ass}(M/N) = \mathrm{Ess}_M(N)$. The minimal elements of $\mathrm{Ess}_M(N)$ or $\mathrm{Ass}(M)$ are called *isolated essential primes* of N in M (resp. *isolated associated primes* of M). The Q_i corresponding to isolated primes of either type are called *isolated primary components* of N in M or *isolated primary components* of M.

Theorem 3.91 *(Second Uniqueness Theorem) The isolated primary components of N in M are uniquely determined by M and N.*

Proof. Let Q be such an isolated component of N in M and let $\mathfrak{p}$ be the corresponding minimal prime. Look at $S = A - \mathfrak{p}$. If $\mathfrak{P} \in \mathrm{Ess}_M(N)$, then $\mathfrak{P} > \mathfrak{p}$ implies that $\mathfrak{P} \cap S \neq \emptyset$ and as $\mathfrak{p}$ is minimal, all other $\mathfrak{P}$ touch S. It follows from Proposition 3.89 that $S(N) = Q$. □

The Lasker-Noether theorem has an immediate application to number theory. This concerns factorization and it shows clearly how Lasker-Noether provides a generalization to Noetherian rings of unique factorization in UFD's.

Definition 3.10 A *Dedekind domain* is a noetherian, normal domain of Krull dimension 1.

Examples of Dedekind domains.

(1) Every P.I.D. is a Dedekind domain.

(2) If K is a finite extension of $\mathbb{Q}$ (that is, K is a *number field*) and $O_K = \mathrm{Int}_{\mathbb{Z}}(K)$ (the integral closure of $\mathbb{Z}$ in K), then O_K is a Dedekind domain. The ring O_K is called the *ring of integers in* K.

(3) Let X be a compact Riemann surface and $x \in X$, any point in X. Let

$$\mathcal{A} = \{f \in \mathcal{M}\mathrm{er}(X) \mid \text{ poles of } f \text{ are only at } x\}.$$

Then, $\mathcal{A}$ is a Dedekind domain.

(3a) Let X be an open Riemann surface of finite character, which means that $\overline{X} = X \cup$ finite set of points is a compact Riemann surface. Then, $\mathrm{Hol}(X)$(= the ring of all holomorphic functions on X) is a Dedekind domain.

Say A is a Dedekind domain. If $\mathfrak{p} \in \mathrm{Spec}\, A$ but $\mathfrak{p} \neq (0)$, then dimension 1 implies that $\mathfrak{p} \in \mathrm{Max}(A)$. From Theorem 3.56, $A_{\mathfrak{p}}$ is a PID. Take any non-zero ideal, $\mathfrak{A}$, then by Lasker-Noether, we can write $\mathfrak{A} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, a reduced primary decomposition. Now,

$$\mathfrak{p}_j = \sqrt{\mathfrak{q}_j} \supseteq \mathfrak{A} > (0),$$

so each of the $\mathfrak{p}_j$'s is a maximal ideal. It follows that each $\mathfrak{p}_j$ is isolated and, by the second uniqueness theorem, the $\mathfrak{q}_j$'s are unique. Moreover, whenever $i \neq j$,

$$\sqrt{\mathfrak{q}_i + \mathfrak{q}_j} = \sqrt{\mathfrak{p}_i + \mathfrak{p}_j} = A,$$

so that $1 \in \mathfrak{q}_i + \mathfrak{q}_j$. We deduce that the $\mathfrak{q}_j$ are pairwise comaximal and the Chinese Remainder Theorem says

$$\mathfrak{A} = \bigcap_{i=1}^{t} \mathfrak{q}_i = \prod_{i=1}^{t} \mathfrak{q}_i.$$

The ring $A/\mathfrak{q}_i$ is noetherian and any $\mathfrak{p} \in \mathrm{Spec}(A/\mathfrak{q}_i)$ corresponds to a prime of A containing $\mathfrak{p}_i$; that is, $\mathfrak{p}$ must be $\mathfrak{p}_i$. Consequently, $A/\mathfrak{q}_i$ is a local ring with the DCC and by Nagata's Theorem $\overline{\mathfrak{p}_i}$ (= image $\mathfrak{p}_i$ in $A/\mathfrak{q}_i$) is nilpotent. Let e_i be its index of nilpotence so that

$$\mathfrak{p}_i^{e_i} \subseteq \mathfrak{q}_i < \mathfrak{p}_i^{e_i - 1}.$$

But, $A_{\mathfrak{p}_i}$ is a PID, and Proposition 3.5 shows that $\mathfrak{q}_i = \mathfrak{p}_i^{e_i}$. In summary, we get the following theorem of Dedekind:

Theorem 3.92 *(Dedekind, 1878) In a Dedekind domain, every nonzero ideal, $\mathfrak{A}$, is a unique product of powers of prime ideals: $\mathfrak{A} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}$.*

Corollary 3.93 *(Kummer, 1833) In the ring of integers of a number field, every nonzero ideal is a unique product of powers of prime ideals.*

After this little excursion into number theory and the connection of primary decomposition to questions of factorization, we resume our study of primary decomposition for modules—especially its applications to the structure of modules.

Lemma 3.94 *Say M is a $\mathfrak{p}$-coprimary module and N ($\neq (0)$) is a submodule of M. Then, N is also $\mathfrak{p}$-coprimary.*

Proof. Pick $a \in A$ with σ_a not injective on N. Then, σ_a is not injective on M, so, σ_a is nilpotent on M (as M is coprimary). Therefore, $\sigma_a \restriction N$ is also nilpotent; so, N is coprimary. Let $\widetilde{\mathfrak{p}}$ be the prime associated with N while $\mathfrak{p}$ is the prime for M. We know that $\mathfrak{p} = \sqrt{\mathrm{Ann}(M)}$, while $\widetilde{\mathfrak{p}} = \sqrt{\mathrm{Ann}(N)}$. If $x \in \mathfrak{p}$, then $x^k \in \mathrm{Ann}(M)$; so, $x^k \in \mathrm{Ann}(N)$, i.e, $x \in \widetilde{\mathfrak{p}}$. Thus, $\mathfrak{p} \subseteq \widetilde{\mathfrak{p}}$.

Now, pick x with σ_x not injective on N. This implies that $(\sigma_x)^k \equiv 0$ on N, that is, $x^k \in \mathrm{Ann}(N)$, *i.e.*, $x \in \widetilde{\mathfrak{p}}$. Thus, $x \in \widetilde{\mathfrak{p}}$ implies σ_x is not injective on N, hence σ_x is not injective on M, and so $(\sigma_x)^k \equiv 0$ on M as M is coprimary which implies that $x \in \mathfrak{p}$. Therefore, we also have $\widetilde{\mathfrak{p}} \subseteq \mathfrak{p}$, and $\widetilde{\mathfrak{p}} = \mathfrak{p}$. □

Proposition 3.95 *A necessary and sufficient condition that M be $\mathfrak{p}$-coprimary is that* $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. *Let $N \subseteq M$, for arbitrary M and N, then* $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M)$.

Proof. Assume M is $\mathfrak{p}$-coprimary. Then (0) is $\mathfrak{p}$-primary in M. By the first uniqueness theorem, $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. Conversely, if $\mathrm{Ass}(M) = \{\mathfrak{p}\}$, then (0) has just one primary component, whose prime is $\mathfrak{p}$. So, (0) is $\mathfrak{p}$-primary and it follows that M is $\mathfrak{p}$-coprimary.

Assume $N \subseteq M$. Write $(0) = Q_1 \cap \cdots \cap Q_t$, a reduced primary decomposition of (0) in M. Then, $\mathrm{Ass}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. By intersecting $(0) = Q_1 \cap \cdots \cap Q_t$ with N, we get

$$(0) = (Q_1 \cap N) \cap \cdots \cap (Q_t \cap N).$$

Observe that we have the composite map

$$N \hookrightarrow M \longrightarrow M/Q_i$$

and its kernel is $N \cap Q_i$. Hence, $N/(N \cap Q_i) \hookrightarrow M/Q_i$. But, M/Q_i is $\mathfrak{p}_i$-coprimary; so, from the argument above, $N/(N \cap Q_i)$ is also $\mathfrak{p}_i$-coprimary, provided that $N/(N \cap Q_i) \neq (0)$. Now, we have $N/(N \cap Q_i) = (0)$ iff $Q_i \supseteq N$. Consequently, we have

$$(0) = (Q_{i_1} \cap N) \cap \cdots \cap (Q_{i_s} \cap N) \quad \text{in } N,$$

where $Q_{i_l} \not\supseteq N$, for each i_l, and $Q_{i_l} \cap N$ is $\mathfrak{p}_{i_l}$-primary in N. By the first uniqueness theorem, we deduce that

$$\mathrm{Ass}(N) = \{\mathfrak{p} \in \mathrm{Ass}(M) \mid Q \not\supseteq N, \text{ where } Q \text{ corresponds to } \mathfrak{p}\}.$$

□

Corollary 3.96 *(of the proof) If $N \subseteq M$, then*

$$\mathrm{Ass}(N) = \{\mathfrak{p} \in \mathrm{Ass}(M) \mid Q \not\supseteq N, \text{ where } Q \text{ corresponds to } \mathfrak{p}\}.$$

Proposition 3.97 *Say $(0) = \bigcap_{i=1}^{t} Q_i$ is a reduced primary decomposition of (0) in M and let N be a submodule of M. Then, N is $\mathfrak{p}_i$-coprimary if and only if $N \cap Q_i = (0)$. In particular, there exist $\mathfrak{p}_i$-coprimary submodules of M, namely, $\bigcap_{j \neq i} Q_j$. In fact, $\mathfrak{p} \in \mathrm{Ass}(M)$ iff M contains a submodule which is $\mathfrak{p}$-coprimary. Lastly, if $N \cap (Q_i + Q_j) = (0)$, then $N = (0)$. Therefore, M is an essential extension of $Q_i + Q_j$.*

Proof. Say $N \cap Q_i = (0)$, then

$$N = N/(N \cap Q_i) \hookrightarrow M/Q_i.$$

Therefore, N is a submodule of the $\mathfrak{p}_i$-coprimary module M/Q_i. But then, N is $\mathfrak{p}_i$-coprimary (as a submodule of a $\mathfrak{p}_i$-coprimary is $\mathfrak{p}_i$-coprimary). Conversely, since $(0) = \bigcap_i Q_i$, we get

$$(0) = \bigcap_i (Q_i \cap N), \tag{$*$}$$

and we know that $Q_i \cap N$ is $\mathfrak{p}_i$-primary if $Q_i \cap N \neq N$, and that $(*)$ is a reduced decomposition. Since N is $\mathfrak{p}_i$-coprimary, by the first uniqueness theorem, there can be only one term in $(*)$, i.e., $Q_j \supseteq N$ for all $j \neq i$; then $(0) = Q_i \cap N$. The second statement is now obvious. If $N \cap (Q_i + Q_j) = (0)$, then, of course, $N \cap Q_i = N \cap Q_j = (0)$. Then, $\mathfrak{p}_i$ and $\mathfrak{p}_j$ would be primes of N, yet, N is coprimary by the first statement. Consequently, $\mathfrak{p}_i = \mathfrak{p}_j$, a contradiction. So, $N = (0)$. □

To finish this chain of ideas, we need the "power lemma":

Lemma 3.98 *(Power lemma) Say A is a commutative ring with unity and M, F are A-module with $F \subseteq M$. Write $\mathfrak{A} = \sqrt{(M \longrightarrow F)}$ and assume $\mathfrak{A}$ is f.g. as ideal. Then, there is some $\rho >> 0$ so that $\mathfrak{A}^\rho M \subseteq F$.*

Proof. Let $\alpha_1, \ldots, \alpha_t$ be generators for $\mathfrak{A}$. For $l = 1, \ldots, t$, there is some $k_l > 0$ so that $\alpha_l^{k_l} M \subseteq F$. Let $\rho = k_1 + \cdots + k_t$. Every element of $\mathfrak{A}$ has the form $r_1\alpha_1 + \cdots + r_t\alpha_t$, where $r_i \in A$. Every element of $\mathfrak{A}^\rho$ is a sum of terms $s(a_1a_2 \cdots a_\rho)$; $s \in A$; $a_1, \ldots, a_\rho \in \mathfrak{A}$. Then, $a_1 \cdots a_\rho$ is a sum of monomials of the form $c\alpha_1^{i_1} \cdots \alpha_t^{i_t}$, where $c \in A$ and $i_1 + \cdots + i_t = \rho$. Now, at least one $i_l \geq k_l$ in the last sum, and then, $\alpha_1^{i_1} \cdots \alpha_t^{i_t} M \subseteq F$. Therefore, $\mathfrak{A}^\rho M \subseteq F$. □

Theorem 3.99 *If A is a noetherian ring and M is a f.g. A-module, then for all submodules, N, of M, all the prime ideals of $\mathrm{Ann}(N)$ are in $\mathrm{Ass}(M)$. A prime ideal, $\mathfrak{p}$, is in $\mathrm{Ass}(M)$ iff there is some $x \in M$ so that $\mathfrak{p} = \mathrm{Ann}(x)$ iff $A/\mathfrak{p}$ is isomorphic to a submodule of M.*

Proof. In M, we have $(0) = \bigcap_i Q_i$, a reduced primary decomposition, and we let $\mathfrak{p}_i$ correspond to Q_i. The first uniqueness theorem implies $\mathrm{Ass}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. Also,

$$\mathrm{Ann}(N) = (N \longrightarrow (0)) = \bigcap_i (N \longrightarrow Q_i).$$

But, we know that

$$(N \longrightarrow Q_i) = \begin{cases} A & \text{if } N \subseteq Q_i \\ \mathfrak{p}_i\text{-primary ideal} & \text{otherwise.} \end{cases}$$

We get a reduced primary decomposition of $\mathrm{Ann}(N)$:

$$\mathrm{Ann}(N) = \bigcap_{j | Q_j \not\supseteq N} (N \longrightarrow Q_j).$$

By the first uniqueness theorem, the primes of $\mathrm{Ann}(N)$ are the $\mathfrak{p}_j$'s for which $Q_j \not\supseteq N$, so, they are contained in $\mathrm{Ass}(M)$.

We have $\mathfrak{p} = \mathrm{Ann}(A/\mathfrak{p})$ and $A/\mathfrak{p} = A\xi$, for some ξ (where ξ is the image of 1 modulo $\mathfrak{p}$). Given x with $\mathrm{Ann}(x) = \mathfrak{p}$, the map $\xi \mapsto x$ gives $A/\mathfrak{p} \cong Ax \subseteq M$ and conversely. Say $\mathfrak{p}$ kills some x exactly, then, as $A/\mathfrak{p}$ is $\mathfrak{p}$-coprimary, $\mathrm{Ass}(Ax) = \{\mathfrak{p}\}$. Yet $Ax \subseteq M$, so, $\mathfrak{p} \in \mathrm{Ass}(M)$.

Conversely, say $\mathfrak{p} \in \mathrm{Ass}(M)$. We must find $x \in M$ with $\mathrm{Ann}(x) = \mathfrak{p}$.

By Proposition 3.97, if $\mathfrak{p} \in \mathrm{Ass}(M)$, then there is a submodule, P, so that P is $\mathfrak{p}$-coprimary. Thus, $\mathfrak{p} = \sqrt{\mathrm{Ann}(P)}$, i.e., $\mathfrak{p} = \sqrt{(P \longrightarrow (0))}$. In the power lemma, set $\mathfrak{p} = \mathfrak{A}$, $P = M$, $(0) = F$. As A is noetherian, $\mathfrak{p}$ is f.g. and by the power lemma, there is some $\rho >> 0$ with $\mathfrak{p}^\rho P = (0)$. If we choose ρ minimal with the above property, we have $\mathfrak{p}^\rho P = (0)$ and $\mathfrak{p}^{\rho-1} P \neq (0)$. Pick any $x \neq 0$ in $\mathfrak{p}^{\rho-1}P$. Then,

$$\mathfrak{p}x \subseteq \mathfrak{p}\mathfrak{p}^{\rho-1}P = \mathfrak{p}^\rho P = (0),$$

so, $\mathfrak{p} \subseteq \mathrm{Ann}(x)$. But $x \in P$ implies $Ax \subseteq P$ and P is $\mathfrak{p}$-coprimary; consequently, Ax is also $\mathfrak{p}$-coprimary. It follows that

$$\sqrt{\mathrm{Ann}(Ax)} = \sqrt{\mathrm{Ann}(x)} = \mathfrak{p}.$$

So, we get $\mathfrak{p} \subseteq \mathrm{Ann}(x) \subseteq \sqrt{\mathrm{Ann}(x)} = \mathfrak{p}$. □

In all of the following corollaries, A is a noetherian ring and M is a f.g. A-module. By taking $N = M$ in Theorem 3.99, we get:

Corollary 3.100 *The primes of* $\mathrm{Ann}(M)$ *are in* $\mathrm{Ass}(M)$.

Corollary 3.101 *Say* $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ *is exact. Then,*

$$\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N).$$

Proof. Pick $\mathfrak{p} \in \mathrm{Ass}(M)$ and say $\mathfrak{p} \notin \mathrm{Ass}(N)$. By Theorem 3.99, there is some $x \in M$ so that $\mathfrak{p} = \mathrm{Ann}(x)$. Look at $(Ax) \cap N$. We claim that $(Ax) \cap N = (0)$. If not, $(Ax) \cap N \subseteq Ax$ and Ax is $\mathfrak{p}$-coprimary. Thus, $(Ax) \cap N$ is also $\mathfrak{p}$-coprimary and $\mathrm{Ass}((Ax) \cap N) = \{\mathfrak{p}\}$, But, $(Ax) \cap N \subseteq N$; so, $\mathrm{Ass}((Ax) \cap N) \subseteq \mathrm{Ass}(N)$. It follows that $\mathfrak{p} \in \mathrm{Ass}(N)$, a contradiction.

Therefore, $(Ax) \cap N = (0)$. Thus, we have

$$Ax \xrightarrow{\sim} Ax/((Ax) \cap N) \hookrightarrow M/N,$$

which means that Ax is a submodule of M/N. By Theorem 3.99, we have $\mathfrak{p} \in \mathrm{Ass}(M/N)$. □

Corollary 3.102 *We have* $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$.

Proof. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then $\mathfrak{p} = \mathrm{Ass}(Ax)$, for some $x \in M$, i.e., we have the inclusion $A/\mathfrak{p} \longrightarrow M$. By localizing, we get $(A/\mathfrak{p})_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}$, yet

$$(A/\mathfrak{p})_{\mathfrak{p}} = \mathrm{Frac}(A/\mathfrak{p}) \neq (0).$$

Thus, $M_{\mathfrak{p}} \neq (0)$, i.e., $\mathfrak{p} \in \mathrm{Supp}(M)$. □

Corollary 3.103 *Each of our* M*'s possesses a chain (of submodules)*

$$(0) = M_0 < M_1 < M_2 < \cdots < M_n = M \tag{$\dagger$}$$

for which $M_j/M_{j-1} \cong A/\mathfrak{p}_j$*, for some* $\mathfrak{p}_j \in \mathrm{Spec}\, A$*. Every* $\mathfrak{p} \in \mathrm{Ass}(M)$ *appears as at least one of these* $\mathfrak{p}_j$ *in each such chain.*

Proof. If $\mathfrak{p} \in \mathrm{Ass}(M)$, there is some $x \in M$ so that $A/\mathfrak{p} \cong Ax \subseteq M$. If we let $M_1 = Ax$, it follows that $M_1/M_0 \cong A/\mathfrak{p}$. Look at M/M_1. If $\widetilde{\mathfrak{p}} \in \mathrm{Ass}(M/M_1)$, repeat the argument to get $\overline{M_2} \subseteq M/M_1$ with $\overline{M_2} = A\overline{y}$, for some $\overline{y} \in M/M_1$, and $A/\widetilde{\mathfrak{p}} \cong A\overline{y}$. By the second homomorphism theorem, $\overline{M_2} = M_2/M_1$. Then, we have $(0) < M_1 < M_2$; $M_2/M_1 \cong A/\widetilde{\mathfrak{p}}$; $M_1/M_0 \cong A/\mathfrak{p}$. If we continue this process, we obtain an ascending chain of the desired type

$$(0) = M_0 < M_1 < M_2 < \cdots < M_n < \cdots .$$

As M is noetherian, this chain stops. This proves the first statement.

We prove the last statement by induction on the length of a given chain.

Hypothesis: If M has a chain, ($\dagger$), of length n, each $\mathfrak{p} \in \mathrm{Ass}(M)$ appears among the primes from ($\dagger$).

If $n = 1$, then $M \cong A/\widetilde{\mathfrak{p}}$. As $A/\widetilde{\mathfrak{p}}$ is $\widetilde{\mathfrak{p}}$-coprimary, we have $\mathrm{Ass}(M) = \{\widetilde{\mathfrak{p}}\}$; yet $\mathfrak{p} \in \mathrm{Ass}(M)$, so, $\mathfrak{p} = \widetilde{\mathfrak{p}}$.

Assume the induction hypothesis holds up to $n-1$. Given a chain, ($\dagger$), of length n and $\mathfrak{p} \in \mathrm{Ass}(M)$, we know there exists some $x \in M$ with $\mathfrak{p} = \mathrm{Ann}(x)$, i.e., we have an inclusion $A/\mathfrak{p} \hookrightarrow M$. There is some j such that $x \in M_j$ and $x \notin M_{j-1}$, where the M_j's are in ($\dagger$). If $j < n$, then apply the induction hypothesis to M_{n-1} to conclude that $\mathfrak{p}$ is among $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$.

So, we may assume $x \in M_n$ and $x \notin M_{n-1}$. Look at $(Ax) \cap M_{n-1}$. There are two cases.

(a) $(Ax) \cap M_{n-1} \neq (0)$. Then, $(Ax) \cap M_{n-1} \subseteq Ax$, where the latter is $\mathfrak{p}$-coprimary; it follows that $(Ax) \cap M_{n-1}$ is $\mathfrak{p}$-coprimary and $\mathrm{Ass}((Ax) \cap M_{n-1}) = \{\mathfrak{p}\}$. Yet, $(Ax) \cap M_{n-1} \subseteq M_{n-1}$, so,

$$\mathrm{Ass}((Ax) \cap M_{n-1}) \subseteq \mathrm{Ass}(M_{n-1}).$$

Therefore, $\mathfrak{p}$ is among $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$, by the induction hypothesis.

(b) $(Ax) \cap M_{n-1} = (0)$. In this case, $Ax \cong Ax/((Ax) \cap M_{n-1}) \hookrightarrow M/M_{n-1} \cong A/\mathfrak{p}_n$, so, $\mathrm{Ass}(Ax) = \{\mathfrak{p}\} \subseteq \mathrm{Ass}(A/\mathfrak{p}_n) = \{\mathfrak{p}_n\}$. Therefore, $\mathfrak{p} = \mathfrak{p}_n$. □

The chain, (†), shows that M is a multiple extension of the "easy" modules $A/\mathfrak{a}_j$. That is, we have exact sequences

$$\begin{aligned}
&0 \longrightarrow M_1 = A/\mathfrak{p}_1 \longrightarrow M_2 \longrightarrow M_2/M_1 = A/\mathfrak{p}_2 \longrightarrow 0\\
&0 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow A/\mathfrak{p}_3 \longrightarrow 0\\
&\qquad\qquad\qquad\vdots\\
&0 \longrightarrow M_{n-1} \longrightarrow M \longrightarrow A/\mathfrak{p}_n \longrightarrow 0
\end{aligned}$$

We define $\mathrm{Ext}(M/N, N)$ as the set

$$\{M \mid 0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0\}/\sim,$$

where the equivalence relation $\sim$ is defined as in the case of group extensions. It turns out that not only is $\mathrm{Ext}(M/N, N)$ an abelian group, it is an A-module. If the A-modules $\mathrm{Ext}(A/\mathfrak{p}_j, M_{j-1})$ can be successively computed, we can classify all f.g. A-modules, M.

To attempt such a task, one should note the following:

Remarks:

(1) Say $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ is exact, then

$$\mathrm{Supp}(M) = \mathrm{Supp}(N) \cup \mathrm{Supp}(M/N).$$

Proof. Localize at any prime $\mathfrak{p}$. We get

$$0 \longrightarrow N_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow (M/N)_{\mathfrak{p}} \longrightarrow 0 \quad \text{is exact.}$$

From this, (1) is clear. □

(2) If M and N are two f.g. modules, then

$$\mathrm{Supp}(M \otimes_A N) = \mathrm{Supp}(M) \cap \mathrm{Supp}(N).$$

Proof. We always have

$$(M \otimes_A N)_{\mathfrak{p}} \cong M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}.$$

So, if $\mathfrak{p} \in \mathrm{Supp}(M \otimes_A N)$, the left hand side is nonzero which implies that $M_{\mathfrak{p}} \neq (0)$ and $N_{\mathfrak{p}} \neq (0)$. Consequently,

$$\mathrm{Supp}(M \otimes_A N) \subseteq \mathrm{Supp}(M) \cap \mathrm{Supp}(N).$$

Now, assume $\mathfrak{p} \in \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$, then $M_{\mathfrak{p}} \neq (0)$ and $N_{\mathfrak{p}} \neq (0)$. As $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are f.g. $A_{\mathfrak{p}}$-modules (since M and N are f.g. A-modules), Nakayama's lemma implies

$$M_{\mathfrak{p}}/\mathfrak{m}M_{\mathfrak{p}} \neq (0) \quad \text{and} \quad N_{\mathfrak{p}}/\mathfrak{m}N_{\mathfrak{p}} \neq (0).$$

As these are vector spaces over $\kappa(A_{\mathfrak{p}})$, we deduce that

$$M_{\mathfrak{p}}/\mathfrak{m}M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}/\mathfrak{m}N_{\mathfrak{p}} \neq (0).$$

But, this is just $(M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}})/\mathfrak{m}(M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}})$; so, $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \neq (0)$. □

(3) If M is a f.g. A-module, then $\mathfrak{p} \in \mathrm{Supp}(M)$ iff there exists a chain

$$(0) = M_0 < M_1 < M_2 \cdots < M_n = M \qquad (\dagger)$$

with $M_j/M_{j-1} \cong A/\mathfrak{p}_j$ and $\mathfrak{p}$ is one of these $\mathfrak{p}_j$.

Proof. If we have a chain (†) and $\mathfrak{p} = \mathfrak{p}_j$ for some j, then $A/\mathfrak{p}_j = A/\mathfrak{p}$ and $(A/\mathfrak{p})_{\mathfrak{p}} = \mathrm{Frac}(A/\mathfrak{p})$. Therefore, $(M_j/M_{j-1})_{\mathfrak{p}} \neq (0)$. By exactness, $(M_j)_{\mathfrak{p}} \neq (0)$. As $M_j \hookrightarrow M$ and localization is exact, $M_{\mathfrak{p}} \neq (0)$ and $\mathfrak{p} \in \mathrm{Supp}(M)$.

Conversely, if $\mathfrak{p} \in \mathrm{Supp}(M)$, then there is some $\mathfrak{q} \in \mathrm{Ass}(M)$ and $\mathfrak{p} \supseteq \mathfrak{q}$. So, $A/\mathfrak{q}$ is in a chain and $A/\mathfrak{p} = (A/\mathfrak{q})/(\mathfrak{p}/\mathfrak{q})$ implies (DX) $\mathfrak{p}$ is in a chain. □

Corollary 3.104 *The following are equivalent conditions:*

(1) $\mathfrak{p} \in \mathrm{Ass}(M/N)$*, for some submodule,* N*, of* M*.*

(2) $\mathfrak{p} \in \mathrm{Supp}(M)$*.*

(3) $\mathfrak{p} \supseteq \mathrm{Ann}(M)$ *(*$\mathfrak{p} \in V(\mathrm{Ann}(M))$*).*

(4) $\mathfrak{p}$ *contains some associated prime of* M*.*

Proof. (1) ⇒ (2). We have $\mathfrak{p} \in \mathrm{Ass}(M/N) \subseteq \mathrm{Supp}(M/N)$ and remark (1) shows that $\mathfrak{p} \in \mathrm{Supp}(M)$.

(2) ⇒ (3). This has already been proved in Section 3.3, Proposition 3.21.

(3) ⇒ (4). If $\mathfrak{p} \supseteq \mathrm{Ann}(M)$, then $\mathfrak{p} \supseteq \sqrt{\mathrm{Ann}(M)}$. However, $\sqrt{\mathrm{Ann}(M)} = \bigcap_{j=1}^{t} \mathfrak{p}_j$, where the $\mathfrak{p}_j$'s are the primes associated with $\mathrm{Ann}(M)$. So,

$$\mathfrak{p} \supseteq \bigcap_{j=1}^{t} \mathfrak{p}_j \supseteq \prod_{j=1}^{t} \mathfrak{p}_j,$$

and it follows that $\mathfrak{p} \supseteq \mathfrak{p}_j$, for some j. By Corollary 3.100, we have $\mathfrak{p}_j \in \mathrm{Ass}(M)$ and $\mathfrak{p} \supseteq \mathfrak{p}_j$, proving (4).

(4) ⇒ (1). Say $\mathfrak{p} \supseteq \mathfrak{q}$ and $\mathfrak{q} \in \mathrm{Ass}(M)$. By our theorem, we know that there is some $x \in M$ so that $\mathfrak{q} = \mathrm{Ann}(x)$, i.e., $A/\mathfrak{q} \hookrightarrow M$. But, $\mathfrak{p}/\mathfrak{q} \hookrightarrow A/\mathfrak{q} \hookrightarrow M$. Let $N = \mathfrak{p}/\mathfrak{q}$, then,

$$A/\mathfrak{p} \cong (A/\mathfrak{q})/(\mathfrak{p}/\mathfrak{q}) \hookrightarrow M/N,$$

so $\{\mathfrak{p}\} = \mathrm{Ass}(A/\mathfrak{p}) \subseteq \mathrm{Ass}(M/N)$. □

Corollary 3.105 *The minimal elements of* $\mathrm{Supp}(M)$ *and the minimal elements of* $\mathrm{Ass}(M)$ *are the same set.*

Proof. Let $\mathfrak{p} \in \mathrm{Supp}(M)$ be minimal. By Corollary 3.104 (4), we have $\mathfrak{p} \supseteq \mathfrak{q}$, for some $\mathfrak{q} \in \mathrm{Ass}(M)$. But $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$, so, $\mathfrak{q} \in \mathrm{Supp}(M)$. Since $\mathfrak{p}$ is minimal, we get $\mathfrak{p} = \mathfrak{q} \in \mathrm{Ass}(M)$. Now, $\mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$, so it is also minimal in $\mathrm{Ass}(M)$.

Now, let $\mathfrak{p} \in \mathrm{Ass}(M)$ be minimal. As $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$, we have $\mathfrak{p} \in \mathrm{Supp}(M)$. If $\mathfrak{p} \supseteq \mathfrak{q}$ for some $\mathfrak{q} \in \mathrm{Supp}(M)$, then, by Corollary 3.104 (4), we have $\mathfrak{q} \supseteq \widetilde{\mathfrak{q}}$, for some $\widetilde{\mathfrak{q}} \in \mathrm{Ass}(M)$. So, $\mathfrak{p} \supseteq \widetilde{\mathfrak{q}}$; since $\mathfrak{p}$ is minimal, we get $\mathfrak{p} = \widetilde{\mathfrak{q}}$. □

Remark: We saw in Section 3.3 that $\mathrm{Supp}(M)$ is closed in $\mathrm{Spec}\, A$. In fact, $\mathrm{Supp}(M)$ is a finite (irredundant) union of irreducible subsets (recall, a set is irreducible iff it is not the union of two proper closed subsets). In this decomposition, the irreducible components are $V(\mathfrak{p})$, for $\mathfrak{p}$ an isolated prime in $\mathrm{Ass}(M)$ (= a minimal element of $\mathrm{Supp}(M)$). Thus, the minimal elements of $\mathrm{Ass}(M)$ are exactly the generic points of $\mathrm{Supp}(M)$.

Corollary 3.106 *If A is a noetherian ring, then*

$$\{x \in A \mid x \text{ is a zero divisor in } A\} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(A)} \mathfrak{p}.$$

Proof. Say $\xi \in \bigcup_{\mathfrak{p}\in \mathrm{Ass}(A)} \mathfrak{p}$, so $\xi \in \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(A)$. By Theorem 3.99, we have $\mathfrak{p} = \mathrm{Ann}(y)$, for some $y \in A$. Clearly $y \neq 0$ and $y\xi \in y\mathfrak{p} = (0)$, so ξ is a zero divisor.

Conversely, pick $x \notin \bigcup_{\mathfrak{p}\in \mathrm{Ass}(A)} \mathfrak{p}$ and let $S = A - \bigcup_{\mathfrak{p}\in \mathrm{Ass}(A)} \mathfrak{p}$. We know from previous work that S is a multiplicative set. Now, we have a primary decomposition $(0) = \bigcap \mathfrak{q}$, where $\sqrt{\mathfrak{q}} = \mathfrak{p} \in \mathrm{Ass}(A)$. We get $S((0)) = \bigcap_{\mathfrak{q}} S(\mathfrak{q})$ and we know that $S(\mathfrak{q}) = \mathfrak{q}$ iff $S \cap \mathfrak{p} = \emptyset$. By definition of S, we conclude that $S((0)) = (0)$. If $xy = 0$, as $x \in S$, we get $y \in S((0)) = (0)$. Therefore, $y = 0$ and x is not a zero divisor. □

Corollary 3.107 *Say $M = \bigcup_\alpha M_\alpha$, for some submodules, M_α, of M. Then,*

$$\mathrm{Ass}(M) = \bigcup_\alpha \mathrm{Ass}(M_\alpha).$$

Proof. Since $M_\alpha \subseteq M$, we get $\mathrm{Ass}(M_\alpha) \subseteq \mathrm{Ass}(M)$, so, $\bigcup_\alpha \mathrm{Ass}(M_\alpha) \subseteq \mathrm{Ass}(M)$. If $\mathfrak{p} \in \mathrm{Ass}(M)$, then there is some $m \in M$ so that $\mathfrak{p} = \mathrm{Ann}(m)$. But, $m \in M_\alpha$ for some α; Theorem 3.99 implies that $\mathfrak{p} \in \mathrm{Ass}(M_\alpha)$. □

Corollary 3.108 *Given an A-module, M, and any nonempty subset, $\Phi \subseteq \mathrm{Ass}(M)$, then there is some submodule, N, of M so that $\mathrm{Ass}(N) = \Phi$.*

Proof. Let $\Phi = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. By proposition 3.97, there are some submodules, P_j, of M so that $\mathrm{Ass}(P_j) = \{\mathfrak{p}_j\}$. I claim, the map $\coprod_{j=1}^t P_j \longrightarrow M$ is injective and $\mathrm{Ass}(\coprod_{j=1}^t P_j) = \Phi$. First, consider the case $t = 2$. Look at the map $P_1 \coprod P_2 \longrightarrow P_1 + P_2 \subseteq M$. This is an isomorphism iff $P_1 \cap P_2 = (0)$. But, $P_1 \cap P_2 \subseteq P_j$ for $j = 1, 2$, so, $\mathrm{Ass}(P_1 \cap P_2) \subseteq \{\mathfrak{p}_1\}$ and $\mathrm{Ass}(P_1 \cap P_2) \subseteq \{\mathfrak{p}_2\}$; as $\mathfrak{p}_1 \neq \mathfrak{p}_2$, we conclude that $P_1 \cap P_2 = (0)$. Then, the sequence

$$0 \longrightarrow P_1 \longrightarrow P_1 \coprod P_2 \longrightarrow P_2 \longrightarrow 0$$

is exact and split. Consequently, $\mathrm{Ass}(P_1 \coprod P_2) = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. For $t > 2$, we proceed by induction (DX). □

Proposition 3.109 *If $N \subseteq M$ and N possesses a primary decomposition in M, then*

$$\mathrm{Rad}_M(N) = \bigcap_{\substack{\mathfrak{p}\in \mathrm{Ess}_N(M) \\ \mathfrak{p} \text{ isolated}}} \mathfrak{p}.$$

In fact, the isolated primes of $\mathrm{Rad}_M(N)$ are just the isolated essential primes of N in M (The hypothesis holds if A is noetherian and M is f.g.).

Proof. As $\mathrm{Rad}_M(N) = \mathrm{Rad}_{M/N}((0)) = \sqrt{\mathrm{Ann}(M/N)}$ and $\mathrm{Ess}_M(N) = \mathrm{Ass}(M/N)$, we may assume that $N = (0)$. We must show that

$$\sqrt{\mathrm{Ann}(M)} = \bigcap_{\substack{\mathfrak{p}\in \mathrm{Ass}(M) \\ \mathfrak{p} \text{ isolated}}} \mathfrak{p}.$$

Now, we have a reduced primary decomposition $(0) = \bigcap_{j=1}^t Q_j$, so

$$\mathrm{Ann}(M) = (M \longrightarrow (0) = \bigcap_{j=1}^t (M \longrightarrow Q_j).$$

But, $(M \longrightarrow Q_j)$ is $\mathfrak{p}_j$-primary, by previous work, so,

$$\sqrt{\mathrm{Ann}(M)} = \sqrt{(M \longrightarrow (0)} = \bigcap_{j=1}^t \sqrt{(M \longrightarrow Q_j)} = \bigcap_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p} = \bigcap_{\substack{\mathfrak{p}\in \mathrm{Ass}(M) \\ \mathfrak{p} \text{ isolated}}} \mathfrak{p}.$$

The rest should be clear. □

3.7 Theorems of Krull and Artin–Rees

We begin with a generalization of the power lemma.

Lemma 3.110 *(Herstein's Lemma) If A is a noetherian ring, $\mathfrak{A}$ is some ideal, M is a f.g. A-module and N is a submodule of M, then there is some $n >> 0$ (depending on A, $\mathfrak{A}$, M, N) so that*

$$\mathfrak{A}^n M \cap N \subseteq \mathfrak{A}N.$$

Proof. By reducing modulo $\mathfrak{A}N$, we may assume $\mathfrak{A}N = (0)$ and we must prove $\mathfrak{A}^n M \cap N = (0)$. Let $\mathcal{S} = \{F \subseteq M \mid F \cap N = (0)\}$. Clearly, $\mathcal{S}$ is nonempty and since M is f.g. and A is noetherian, $\mathcal{S}$ has a maximal element, call it F, again. Let $m_1, \ldots, m_t$ be generators of M and pick $a \in \mathfrak{A}$. Given m_j, for any $n \geq 0$, consider

$$F_n^{(j)}(a) = (a^n m_j \longrightarrow F) = \{x \in A \mid xa^n m_j \in F\}.$$

The $F_n^{(j)}(a)$'s are ideals of A and we have

$$F_1^{(j)}(a) \subseteq F_2^{(j)}(a) \subseteq F_3^{(j)}(a) \subseteq \cdots.$$

By the ACC in A, there is some $N_j(a)$ so that

$$F_{N_j(a)}^{(j)}(a) = F_{N_j(a)+1}^{(j)}(a), \quad \text{for } j = 1, \ldots, t.$$

Let $N(a) = \max_{1 \leq j \leq t}\{N_j(a)\}$. I claim that $a^{N(a)} M \subseteq F$.

Of course, if we show that $a^{N(a)} m_j \in F$ for $j = 1, \ldots, t$, we will have proved the claim.

If the claim is false, there is some j so that $a^{N(a)} m_j \notin F$. Then, $F + Aa^{N(a)} m_j > F$, and by maximality of F, we must have $(F + Aa^{N(a)} m_j) \cap N \neq (0)$. So, there is some $f \in F$ and some $\alpha \in A$ so that

$$0 \neq f + \alpha a^{N(a)} m_j \in N. \tag{$\dagger$}$$

If we multiply ($\dagger$) by a, we get

$$af + \alpha a^{N(a)+1} m_j \in aN = (0),$$

since $\mathfrak{A}N = (0)$ and $a \in \mathfrak{A}$. Thus, $\alpha a^{N(a)+1} m_j = -af \in F$, and so,

$$\alpha \in (a^{N(a)+1} m_j \longrightarrow F) = F_{N(a)+1}^{(j)}(a) = F_{N(a)}^{(j)}(a).$$

It follows that $\alpha a^{N(a)} m_j \in F$; so, $f + \alpha a^{N(a)} m_j \in F$, which means that $F \cap N \neq (0)$, a contradiction. Therefore, $a \in \sqrt{(M \longrightarrow F)}$; as $\mathfrak{A}$ is f.g., by the power lemma, we get $\mathfrak{A}^\rho M \subseteq F$. Thus, finally, $\mathfrak{A}^\rho M \cap N \subseteq F \cap N = (0)$. $\square$

Theorem 3.111 *(Krull Intersection Theorem) Say A is a noetherian ring, M is a f.g. A-module and $\mathfrak{A}$ is an ideal of A. Write $S = 1 - \mathfrak{A}$ $(= \{1 - \alpha \mid \alpha \in \mathfrak{A}\})$. Then,*

$$\bigcap_{n \geq 0} \mathfrak{A}^n M = S(0) = \operatorname{Ker}(M \longrightarrow S^{-1}M).$$

Proof. Write $N = \bigcap \mathfrak{A}^n M$. By Herstein's lemma there exists $\rho > 0$ so that $\mathfrak{A}^\rho M \cap N \subseteq \mathfrak{A}N$. But, $N \subseteq \mathfrak{A}^\rho M$, so $\mathfrak{A}^\rho M \cap N = N$ and it follows that $N \subseteq \mathfrak{A}N$. Of course, we get $\mathfrak{A}N = N$. Now, N is f.g., say $n_1, \ldots, n_t$ are some generators. As $\mathfrak{A}N = N$, there exist some $\alpha_{ij} \in A$ so that

$$n_j = \sum_{i=1}^{t} \alpha_{ij} n_i, \quad \text{for } j = 1, \ldots, t.$$

Therefore, $0 = \sum_{i=1}^{t}(\alpha_{ij} - \delta_{ij})n_i$, for $j = 1, \ldots, t$; so, the matrix $(\delta_{ij} - \alpha_{ij})$ kills the vector $(n_1, \ldots, n_t)$. By linear algebra, if $\Delta = \det(\delta_{ij} - \alpha_{ij}) \in A$, then

$$\Delta n_j = 0, \quad \text{for } j = 1, \ldots, t.$$

(This can be seen as follows: If T is the linear map given by the matrix $(\delta_{ij} - \alpha_{ij})$, then by the Cayley–Hamilton theorem, $\chi(T) = T^t + \beta_1 T^{t-1} + \cdots + \beta_{t-1}T + \beta_t I = 0$. But, $\beta_t = \pm\Delta$ and if we apply $\chi(T)$ to $(n_1, \ldots, n_t)$, then $\chi(T)$ and all the nonnegative powers of T kill it. Consequently, $\beta_t I(n_1, \ldots, n_t) = 0$.) Now, $\Delta = 1 - d$, for some $d \in \mathfrak{A}$. Thus, $\Delta \in S$. For all j, we have $n_j \in S(0)$, so $N \subseteq S(0)$. On the other hand, if $\xi \in S(0)$, then there is some $s \in S$ with $s\xi = 0$. Yet, $s = 1 - \alpha$, for some $\alpha \in \mathfrak{A}$. Thus, $(1 - \alpha)\xi = 0$, i.e., $\xi = \alpha\xi$. An immediate induction yields $\xi = \alpha^n\xi$, for all $n \geq 0$. However, $\alpha^n\xi \in \mathfrak{A}^n M$, for every $n \geq 0$, so $\xi \in \bigcap \mathfrak{A}^n M$; this proves that $S(0) \subseteq N$. □

Corollary 3.112 *Under the hypotheses of Theorem 3.111, if $\mathfrak{A} \subseteq \mathcal{J}(A)$, then $\bigcap \mathfrak{A}^n M = (0)$.*

Proof. Since $S = 1 - \mathfrak{A} \subseteq 1 - \mathcal{J}(A) \subseteq$ units of A, we get $S(0) = (0)$. □

Corollary 3.113 *(Original Krull theorem) If A is local noetherian and $\mathfrak{m}$ is its maximal ideal, then $\bigcap \mathfrak{m}^n = (0)$.*

Proof. As A is local, $\mathfrak{m} = \mathcal{J}(A)$; the result follows from Corollary 3.112 applied to $M = A$. □

Corollary 3.114 *Say X is a real or complex manifold and $x \in X$. Write $\mathcal{O}_{X,x}$ for the local ring of germs of C^∞-functions at x. Then, $\mathcal{O}_{X,x}$ is never noetherian.*

Proof. As the question is local on X, we may assume X is an open ball in $\mathbb{R}^n$ and $x = 0$ in this ball (with n even in case of a complex manifold). Let

$$f(x) = \begin{cases} e^{-1/(x,x)} & \text{for } x \in \mathbb{R}^n,\ x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

(Here, (x, y) is the usual euclidean inner product on $\mathbb{R}^n$.) We have $f(x) \in C^\infty(\text{ball})$. Moreover $f^{(n)}(0) = 0$, for all $n \geq 0$. But, in $\mathcal{O}_{X,x}$, observe that $\mathfrak{m}^n$ consists of the classes of functions defined near zero so that the n-th derivative and all previous derivatives are 0 at the origin. So, $\text{germ}(f) \in \bigcap \mathfrak{m}^n$; by the Krull intersection theorem, our ring $\mathcal{O}_{X,x}$ is *not* noetherian. □

$\mathfrak{A}$-adic Topologies.

Let A be a ring, $\mathfrak{A}$ be an ideal in A and M be an A-module. At the origin in M, take as basis of opens (= fundamental system of neighborhoods at 0) the subsets $\mathfrak{A}^n M$, for $n = 0, 1, 2, \ldots$. Topologise M by translating these so that $\{m + \mathfrak{A}^n M\}_{n \geq 0}$ is a neighborhood basis around m. When $M = A$, the ring A receives a topology and A is a topological ring in this topology which is called the $\mathfrak{A}$-*adic topology*. Similarly, the module M is a topological module in this topology also called the $\mathfrak{A}$-*adic topology*. The $\mathfrak{A}$-adic topology is *pseudo-metric*, i.e., set

$$\text{ord}_{\mathfrak{A}}(m) = \begin{cases} n & \text{if } m \in \mathfrak{A}^n M, \text{ yet } m \notin \mathfrak{A}^{n+1} M \\ \infty & \text{if } m \in \bigcap_{n \geq 0} \mathfrak{A}^n M, \end{cases}$$

and define

$$d(m_1, m_2) = e^{-\text{ord}_{\mathfrak{A}}(m_1 - m_2)}.$$

Then, we have

(1) $d(m_1, m_2) \geq 0$.

(2) $d(m_1, m_2) = d(m_2, m_1)$.

(3) $d(m_1, m_3) \leq \max(d(m_1, m_2), d(m_2, m_3))$ (ultrametric property).

Yet, it can happen that $d(m_1, m_2) = 0$ and $m_1 \neq m_2$. The $\mathfrak{A}$-adic topology is Hausdorff iff d *is* a metric (i.e., $d(m_1, m_2) = 0$ iff $m_1 = m_2$)) iff $\bigcap_{n \geq 0} \mathfrak{A}^n M = (0)$.

If the $\mathfrak{A}$-adic topology is Hausdorff, then we have Cauchy sequences, completeness and completions. The reader should check: The completion of M in the $\mathfrak{A}$-adic topology (Hausdorff case) is equal to $\varprojlim_n M/\mathfrak{A}^n M \stackrel{\text{def}}{=} \widehat{M}$. The first person to make use of these ideas was Kurt Hensel (1898) in the case $A = \mathbb{Z}$, $M = \mathbb{Q}$, $\mathfrak{p} = (p)$, where p is a prime. But here, Hensel used $\text{ord}_p(\frac{r}{s}) = \text{ord}_p(r) - \text{ord}_p(s)$.

Corollary 3.115 *The $\mathfrak{A}$-adic topology on a f.g. module M over a noetherian ring is Hausdorff if $\mathfrak{A} \subseteq \mathcal{J}(A)$. In particular, this holds if A is local and $\mathfrak{A} = \mathfrak{m}_A$.*

Corollary 3.116 *Say A is a noetherian domain and $\mathfrak{A}$ is any proper ideal (i.e., $\mathfrak{A} \neq A$). Then, the $\mathfrak{A}$-adic topology on A is Hausdorff.*

Proof. We have $S = 1 - \mathfrak{A} \subseteq$ nonzero elements of A. Thus, S consists of nonzero divisors. If $\xi \in S(0)$, then $s\xi = 0$, for some $s \in S$, so, $\xi = 0$. Therefore, $S(0) = (0)$ and the topology is Hausdorff. □

Theorem 3.117 *(Artin–Rees) Let A be a noetherian ring, $\mathfrak{A}$ be some ideal, M be a f.g. A-module and N a submodule of M. Then, there is some k (depending on A, $\mathfrak{A}$, M and N) so that for all $n \geq k$,*

$$\mathfrak{A}^n M \cap N = \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N).$$

Proof. Define the graded ring $\text{Pow}_{\mathfrak{A}}(A) \subseteq A[X]$, where X is an indeterminate by

$$\begin{aligned} \text{Pow}_{\mathfrak{A}}(A) &= \coprod_{n \geq 0} \mathfrak{A}^n X^n \\ &= \{z_0 + z_1 X + \cdots + z_r X^r \mid r \geq 0,\ z_j \in \mathfrak{A}^j\}. \end{aligned}$$

Now, M gives rise to a graded module, M', over $\text{Pow}_{\mathfrak{A}}(A)$, namely

$$\begin{aligned} M' &= \coprod_{n \geq 0} \mathfrak{A}^n M X^n \\ &= \{z_0 + z_1 X + \cdots + z_r X^r \mid r \geq 0,\ z_j \in \mathfrak{A}^j M\}. \end{aligned}$$

Observe that $\text{Pow}_{\mathfrak{A}}(A)$ is a noetherian ring. For, if $\alpha_1, \ldots, \alpha_q$ generate $\mathfrak{A}$ in A, then the elements of $\mathfrak{A}^n$ are sums of degree n monomials in the α_j's, i.e., if $Y_1, \ldots, Y_q$ are independent indeterminates the map

$$A[Y_1, \ldots, Y_q] \longrightarrow \text{Pow}_{\mathfrak{A}}(A)$$

via $Y_j \mapsto \alpha_j X$ is surjective, and as $A[Y_1, \ldots, Y_q]$ is noetherian, so is $\text{Pow}_{\mathfrak{A}}(A)$.

Let $m_1, \ldots, m_t$ generate M over A. Then, $m_1, \ldots, m_t$ generate M' over $\text{Pow}_{\mathfrak{A}}(A)$. Therefore, M' is a noetherian module. Set

$$N' = \coprod_{n \geq 0} (\mathfrak{A}^n M \cap N) X^n \subseteq M',$$

a submodule of M'. Moreover, N' is a homogeneous submodule of M and it is f.g. as M' is noetherian. Consequently, N' possesses a finite number of homogeneous generators: $u_1 X^{n_1}, \ldots, u_s X^{n_s}$, where $u_j \in \mathfrak{A}^{n_j} M \cap N$. Let $k = \max\{n_1, \ldots, n_s\}$. Given any $n \geq k$ and any $z \in \mathfrak{A}^n M \cap N$, look at $zX^n \in N'_n$. We have

$$zX^n = \sum_{l=1}^{s} a_l X^{n - n_l} u_l X^{n_l},$$

where $a_l X^{n-n_l} \in \big(\mathrm{Pow}_{\mathfrak{A}}(A)\big)_{n-n_l}$. Thus,

$$a_l \in \mathfrak{A}^{n-n_l} = \mathfrak{A}^{n-k}\mathfrak{A}^{k-n_l}$$

and

$$a_l u_l \in \mathfrak{A}^{n-k}(\mathfrak{A}^{k-n_l}u_l) \subseteq \mathfrak{A}^{n-k}(\mathfrak{A}^{k-n_l}(\mathfrak{A}^{n_l}M \cap N)) \subseteq \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N).$$

It follows that $z = \sum_{l=1}^{s} a_l u_l \in \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N)$, so

$$\mathfrak{A}^n M \cap N \subseteq \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N).$$

Now, it is clear that the righthand side is contained in $\mathfrak{A}^n M \cap N$, as $\mathfrak{A}^{n-k}N \subseteq N$. □

Remark: If we choose $n = k+1$ in the Artin–Rees theorem, we get $\mathfrak{A}^n M \cap N = \mathfrak{A}(\mathfrak{A}^k M \cap N) \subseteq \mathfrak{A}N$, hence a new proof of Herstein's lemma.

Corollary 3.118 *If A is a noetherian ring, $\mathfrak{A}$ is an ideal, M is a f.g. module and N is a submodule, then the topology on N induced by the $\mathfrak{A}$-adic topology on M is just the $\mathfrak{A}$-adic topology on N.*

Proof. The induced topology has as neighborhood basis at 0 the sets $\mathfrak{A}^n M \cap N$. By the Artin–Rees theorem,

$$\mathfrak{A}^n M \cap N = \mathfrak{A}^{n-k}(\mathfrak{A}^k M \cap N) \subseteq \mathfrak{A}^{n-k}N,$$

for all $n \geq k$, for some fixed k. It follows that the induced topology is finer. But, $\mathfrak{A}^\rho N \subseteq \mathfrak{A}^\rho M \cap N$, for all ρ; so, the $\mathfrak{A}$-adic topology on N is in its turn finer than the induced topology. □

We turn now to two very famous theorems of Wolfgang Krull. Recall that a power of a prime ideal need not be primary. In the proof of the first of the Krull theorems, the principal ideal theorem, we need to remedy this situation. We are led to the notion of the *symbolic powers*, $\mathfrak{p}^{(n)}$, of a prime ideal, $\mathfrak{p}$.

Let A be a ring and let $\mathfrak{p} \in \operatorname{Spec} A$. Look at $A_\mathfrak{p} = S^{-1}A$, where $S = A - \mathfrak{p}$. Take the powers of $\mathfrak{p}$, extend and contract them to and from $A_\mathfrak{p}$, to get

$$\mathfrak{p}^{(n)} \stackrel{\text{def}}{=} (\mathfrak{p}^n)^{ec} = S(\mathfrak{p}^n).$$

Lemma 3.119 *The ideal $\mathfrak{p}^{(n)}$ is always a $\mathfrak{p}$-primary ideal.*

Proof. The ideal $\mathfrak{p}^e$ is maximal in $A_\mathfrak{p}$. Hence, $(\mathfrak{p}^e)^n$ is $\mathfrak{p}^e$-primary, by previous work. But, $(\mathfrak{p}^e)^n = (\mathfrak{p}^n)^e$. Therefore, $(\mathfrak{p}^n)^e$ is $\mathfrak{p}^e$-primary. Now, $S \cap \mathfrak{p} = \emptyset$, so $(\mathfrak{p}^n)^{ec}$ is $\mathfrak{p}$-primary. □

Further, we have the descending chain

$$\mathfrak{p} \supseteq \mathfrak{p}^{(2)} \supseteq \mathfrak{p}^{(3)} \supseteq \cdots.$$

Theorem 3.120 *(Krull Principal Ideal Theorem (1928)) If A is a noetherian domain and $\mathfrak{p} \in \operatorname{Spec} A$, then* $\operatorname{ht}(\mathfrak{p}) \leq 1$ *iff $\mathfrak{p}$ is an isolated prime of a principal ideal.*

Proof. ($\Rightarrow$) (easy part). By hypothesis, $\operatorname{ht}(\mathfrak{p}) \leq 1$ and $\mathfrak{p} \supseteq (0)$; hence, if $\operatorname{ht}(\mathfrak{p}) = 0$, then $\mathfrak{p} = (0)$, an isolated prime of (0). If $\operatorname{ht}(\mathfrak{p}) = 1$, pick $a \neq 0$ in $\mathfrak{p}$. As $\mathfrak{p} \supseteq (a)$, the ideal $\mathfrak{p}$ must contain one of the isolated primes of (a), say $\mathfrak{P}$. So, $\mathfrak{p} \supseteq \mathfrak{P} > (0)$, and as $\operatorname{ht}(\mathfrak{p}) = 1$, we must have $\mathfrak{p} = \mathfrak{P}$.

($\Leftarrow$) (hard part). Here, we may assume $\mathfrak{p}$ is an isolated prime of (a), where $a \neq 0$ (else, if $a = 0$, then $\mathfrak{p} = (0)$ and $\operatorname{ht}(\mathfrak{p}) = 0$). We must show $\operatorname{ht}(\mathfrak{p}) = 1$. Hence, we must prove that

$$\text{if } \mathfrak{P} \in \operatorname{Spec} A \text{ and } \mathfrak{p} > \mathfrak{P}, \text{ then } \mathfrak{P} = (0). \qquad (\dagger)$$

Step 1. If we localize at $\mathfrak{p}$, there is a one-to-one correspondence between primes contained in $\mathfrak{p}$ and all primes in $A_{\mathfrak{p}}$. Therefore, we may assume $A = A_{\mathfrak{p}}$, i.e., A is local, $\mathfrak{p}$ is maximal and $\mathfrak{p}$ is an isolated prime of (a), with $a \neq 0$. We must prove (†). Now, given $\mathfrak{P} \in \operatorname{Spec} A$ with $\mathfrak{p} > \mathfrak{P}$, could $a \in \mathfrak{P}$? If so, we would have $\mathfrak{p} > \mathfrak{P} \supseteq (a)$. As $\mathfrak{p}$ is isolated, $\mathfrak{p} = \mathfrak{P}$, a contradiction; so, $a \notin \mathfrak{P}$. It follows that the ring $A/(a)$ has precisely *one* prime ideal and it is maximal. Since A is noetherian, by Akizuki's theorem, $A/(a)$ is artinian (i.e., it has the DCC).

Step 2. Pick $\mathfrak{P} \in \operatorname{Spec} A$ with $\mathfrak{P} < \mathfrak{p}$. Of course, $a \notin \mathfrak{P}$. Examine the symbolic powers $\mathfrak{P}^{(n)}$. We have

$$\mathfrak{P} \supseteq \mathfrak{P}^{(2)} \supseteq \mathfrak{P}^{(3)} \supseteq \cdots .$$

I claim this chain stops. To see this, consider the descending chain

$$\mathfrak{P} + (a) \supseteq \mathfrak{P}^{(2)} + (a) \supseteq \mathfrak{P}^{(3)} + (a) \supseteq \cdots .$$

This chain is in one-to-one correspondence with a chain in $A/(a)$. By step 1, the ring $A/(a)$ has the DCC, so, there is some n_0 so that for all $n \geq n_0$,

$$\mathfrak{P}^{(n)} \subseteq \mathfrak{P}^{(n+1)} + aA.$$

Given $x \in \mathfrak{P}^{(n)}$, there is some $y \in \mathfrak{P}^{(n+1)}$ and some $z \in A$ so that $x = y + za$. As $x - y \in \mathfrak{P}^{(n)}$, we have $za \in \mathfrak{P}^{(n)}$; since $a \notin \mathfrak{P} = \sqrt{\mathfrak{P}^{(n)}}$, we get $z \in \mathfrak{P}^{(n)}$. Hence,

$$\mathfrak{P}^{(n)} \subseteq \mathfrak{P}^{(n+1)} + \mathfrak{P}^{(n)}a \subseteq \mathfrak{P}^{(n+1)} + \mathfrak{P}^{(n)}\mathfrak{p}.$$

Read this in the local ring $\overline{A} = A/\mathfrak{P}^{(n+1)}$ whose maximal ideal is $\overline{\mathfrak{p}}$. We get

$$\overline{\mathfrak{P}^{(n)}} = \overline{\mathfrak{P}^{(n)}}\,\overline{\mathfrak{p}}. \tag{‡}$$

As $\overline{\mathfrak{P}^{(n)}}$ is a f.g. $\overline{A}$-module, by Nakayama's lemma, $\overline{\mathfrak{P}^{(n)}} = (0)$. Therefore,

$$\mathfrak{P}^{(n)} = \mathfrak{P}^{(n+1)}, \quad \text{for all } n \geq n_0. \tag{$*$}$$

Step 3. By $(*)$, we get $\bigcap_{n\geq 1} \mathfrak{P}^{(n)} = \mathfrak{P}^{(n_0)}$. But, $(\mathfrak{P}^{(n_0)})^e = \left(\bigcap_{n\geq 1} \mathfrak{P}^{(n)}\right)^e \subseteq \bigcap_{n\geq 1} (\mathfrak{P}^{(n)})^e$. Consequently,

$$(\mathfrak{P}^{(n_0)})^e \subseteq \bigcap_{n\geq 1} (\mathfrak{P}^n)^e = \bigcap_{n\geq 1} (\mathfrak{P}^e)^n.$$

However, $\mathfrak{P}^e$ is the maximal ideal of A, so by the Krull intersection theorem, the righthand side is (0). Therefore,

$$(\mathfrak{P}^e)^{n_0} = (\mathfrak{P}^{n_0})^e = (0).$$

But, A is an integral domain, therefore, $\mathfrak{P}^e = (0)$; so, $\mathfrak{P} = (0)$, as contended. □

Now, consider the case where A is just a ring (not necessarily an integral domain).

Corollary 3.121 *If A is a noetherian ring and $\mathfrak{p}$ is an isolated prime of some $(a) \subseteq A$, then* $\operatorname{ht}(\mathfrak{p}) \leq 1$.

Proof. Now, $\mathfrak{p}$ is an isolated prime of some $(a) \subseteq A$. If $a = 0$, then $\mathfrak{p}$ is a minimal prime, i.e., $\operatorname{ht}(\mathfrak{p}) = 0$. Therefore, we may assume $a \neq 0$. Suppose $\operatorname{ht}(\mathfrak{p}) \geq 2$, then we must have a chain

$$\mathfrak{p} > \mathfrak{q} > \mathfrak{q}'.$$

Look in $\overline{A} = A/\mathfrak{q}'$, a noetherian domain. Here, we have

$$\overline{\mathfrak{p}} > \overline{\mathfrak{q}} > (0) = \overline{\mathfrak{q}'}, \tag{$**$}$$

yet, $\overline{\mathfrak{p}}$ is an isolated prime of $(\overline{a})$, so the theorem in the domain case implies that $\operatorname{ht}(\overline{\mathfrak{p}}) = 1$, contradicting $(**)$. □

To prove the next and last Krull theorem, we need the *chain detour lemma*:

Lemma 3.122 *(Chain detour lemma) Say A is a noetherian ring and*

$$\mathfrak{p}_0 > \mathfrak{p}_1 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

is a given chain in $\operatorname{Spec} A$. *Given a finite set of primes $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$, suppose $\mathfrak{p}_0 \not\subseteq \mathfrak{q}_i$, for $i = 1, \ldots, t$. Then, there exists an alternate chain (the detour)*

$$\mathfrak{p}_0 > \widetilde{\mathfrak{p}_1} > \cdots \widetilde{\mathfrak{p}}_{m-1} > \mathfrak{p}_m$$

so that no $\widetilde{\mathfrak{p}_i}$ is contained in any $\mathfrak{q}_j$.

Proof. Say the lemma is known when $m = 2$, i.e., given a chain $\mathfrak{p}_0 > \mathfrak{p}_1 > \mathfrak{p}_2$, we can change $\mathfrak{p}_1$. Given our chain

$$\mathfrak{p}_0 > \mathfrak{p}_1 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

and the set S, we can replace $\mathfrak{p}_1$ by $\widetilde{\mathfrak{p}_1}$ with $\widetilde{\mathfrak{p}_1} \not\subseteq \mathfrak{q}_i$ for $i = 1, \ldots, t$. But, then, we have the chain

$$\widetilde{\mathfrak{p}_1} > \mathfrak{p}_2 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

and we can use induction to obtain the desired chain.

Thus, we are reduced to the main case: $\mathfrak{p}_0 > \mathfrak{p}_1 > \mathfrak{p}_2$. Now, $\mathfrak{p}_0 > \mathfrak{p}_2$ and $\mathfrak{p}_0 \not\subseteq \mathfrak{q}_\mathfrak{j}$ for $j = 1, \ldots, t$. By the prime avoidance lemma,

$$\mathfrak{p}_0 \not\subseteq \mathfrak{p}_2 \cup \bigcup_{j=1}^{t} \mathfrak{q}_j.$$

Hence, there is some $x \in \mathfrak{p}_0$ so that $x \notin \mathfrak{p}_2$ and $x \notin \mathfrak{q}_j$ for $j = 1, \ldots, t$. Look in $\overline{A} = A/\mathfrak{p}_2$, a noetherian domain. In $\overline{A}$, we have

$$\overline{\mathfrak{p}_0} > \overline{\mathfrak{p}_1} > \overline{\mathfrak{p}_2} = (0)$$

and so, $\operatorname{ht}(\overline{\mathfrak{p}_1}) \geq 2$. Now, $\overline{x} \in \overline{\mathfrak{p}_0}$ and it follows that some isolated prime of $\overline{x}$, say $\mathfrak{B}$, is contained in $\overline{\mathfrak{p}_0}$. As $x \notin \mathfrak{p}_2$, we have $\overline{x} \neq 0$ and $\mathfrak{B}$ is an isolated prime of $\overline{x}$; by the principal ideal theorem, $\operatorname{ht}(\mathfrak{B}) = 1$. As $\operatorname{ht}(\overline{\mathfrak{p}_0}) \geq 2$, we have $\overline{\mathfrak{p}_0} > \mathfrak{B} > (0)$ and $\overline{x} \in \mathfrak{B}$. Let $\widetilde{\mathfrak{p}_1}$ be the inverse image of $\mathfrak{B}$ in A. We get:

(1) $\mathfrak{p}_0 > \widetilde{\mathfrak{p}_1} > \mathfrak{p}_2$.

(2) $x \in \widetilde{\mathfrak{p}_1}$; $x \notin \mathfrak{q}_j$, for $j = 1, \ldots, t$.

(3) $\widetilde{\mathfrak{p}_1} \not\subseteq \mathfrak{q}_j$, for $j = 1, \ldots, t$. □

Theorem 3.123 *(Krull Height Theorem (1928)) If $\mathfrak{A}$ is an ideal of the noetherian ring, A, suppose $\mathfrak{A}$ is generated by r elements and $\mathfrak{p}$ is an isolated prime of $\mathfrak{A}$. Then* $\operatorname{ht}(\mathfrak{p}) \leq r$.

Proof. We proceed by induction on r. Hypothesis: The theorem holds for all isolated primes, $\mathfrak{p}$, of $\mathfrak{A}$ and all $\mathfrak{A}$ generated by at most r elements.

The principal ideal theorem yields the cases $r = 0, 1$. Next, let $\mathfrak{A} = (x_1, \ldots, x_r)$ and $\mathfrak{B} = (x_1, \ldots, x_{r-1})$. If $\mathfrak{A} = \mathfrak{B}$, there is nothing to prove. Thus, we may assume that $x_r \notin \mathfrak{B}$. If $\mathfrak{p}$ (some isolated prime of $\mathfrak{A}$) is an isolated prime of $\mathfrak{B}$, the induction hypothesis implies $\operatorname{ht}(\mathfrak{p}) \leq r - 1$. So, we may assume that $\mathfrak{p}$ is an isolated prime of $\mathfrak{A}$, *not* an isolated prime of $\mathfrak{B}$ and $x_r \notin \mathfrak{B}$ (obviously, $\mathfrak{A} \neq \mathfrak{B}$). Let $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$ be the finite set of isolated primes of $\mathfrak{B}$, let $\mathfrak{p} = \mathfrak{p}_0$ and look at some chain

$$\mathfrak{p} = \mathfrak{p}_0 > \mathfrak{p}_1 > \cdots \mathfrak{p}_{m-1} > \mathfrak{p}_m$$

of $\operatorname{Spec} A$, so that $\operatorname{ht}(\mathfrak{p}_0) \geq m$. If $\mathfrak{p}_0 \subseteq \mathfrak{q}_j$, then

$$\mathfrak{B} \subseteq \mathfrak{A} \subseteq \mathfrak{p}_0 \subseteq \mathfrak{q}_j,$$

contradicting the fact that $\mathfrak{p}_0$ is not an isolated prime of $\mathfrak{B}$. Therefore, $\mathfrak{p}_0 \not\subseteq \mathfrak{q}_j$, for $j = 1, \ldots, t$, and by the detour lemma, there is a chain of the same length

$$\mathfrak{p}_0 > \widetilde{\mathfrak{p}_1} > \cdots \widetilde{\mathfrak{p}}_{m-1} > \mathfrak{p}_m$$

so that no $\widetilde{\mathfrak{p}_i}$ is contained in any $\mathfrak{q}_j$. Our goal is to show that $m \leq r$. let $\overline{A} = A/\mathfrak{B}$. Then $\overline{\mathfrak{A}}$ becomes principal $(\overline{A}\overline{x}_r)$ in $\overline{A}$ and as $\overline{\mathfrak{p}_0}$ is an isolated prime of $\overline{\mathfrak{A}}$, the principal ideal theorem in $\overline{A}$ implies $\mathrm{ht}(\overline{\mathfrak{p}_0}) = 1$. ($\mathrm{ht}(\overline{\mathfrak{p}_0}) > 0$ because $\mathfrak{p}_0$ is *not* an isolated prime of $\mathfrak{B}$).

Now, $\mathfrak{p}_0 \supseteq \widetilde{\mathfrak{p}}_{m-1}$ and $\mathfrak{p}_0 \supseteq \mathfrak{B}$, so,

$$\mathfrak{p}_0 \supseteq \widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}.$$

Then, observe that $\overline{\mathfrak{p}_0} \supseteq \overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$ and as $\mathfrak{B} \subseteq \mathfrak{q}_i$, for all i and $\widetilde{\mathfrak{p}}_{m-1} \not\subseteq \mathfrak{q}_i$, for all i, we have $\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B} \not\subseteq \mathfrak{q}_i$, for all i; thus, $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}} \not\subseteq \overline{\mathfrak{q}_i}$, for all i (here, the $\overline{\mathfrak{q}_i}$ are the isolated primes of (0) in $\overline{A}$, i.e., those of height 0 in $\overline{A}$).

Claim. The ideal $\overline{\mathfrak{p}_0}$ is an isolated prime of $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$.

As $\overline{\mathfrak{p}_0} \supseteq \overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$, we find $\overline{\mathfrak{p}_0} \supseteq \mathfrak{m}$, where $\mathfrak{m}$ is some isolated prime of $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$. If $\overline{\mathfrak{p}_0} \neq \mathfrak{m}$, then as $\mathrm{ht}(\mathfrak{m}) \geq 1$ (because $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}} \not\subseteq \overline{\mathfrak{q}_i}$, for all i) we'd see that $\mathrm{ht}(\overline{\mathfrak{p}_0}) \geq 2$. But, $\mathrm{ht}(\overline{\mathfrak{p}_0}) = 1$, a contradiction. Therefore, $\overline{\mathfrak{p}_0} = \mathfrak{m}$, as claimed.

Now, let $\overline{\overline{A}} = A/\widetilde{\mathfrak{p}}_{m-1}$. As $\mathfrak{p}_0 \supseteq \widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}$, we get

$$\overline{\overline{\mathfrak{p}_0}} \supseteq \overline{\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}} = \overline{\overline{\mathfrak{B}}}.$$

Moreover, as $\overline{\mathfrak{p}_0}$ is an isolated prime of $\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}$, we see that $\overline{\overline{\mathfrak{p}_0}}$ is an isolated prime of $\overline{\overline{\widetilde{\mathfrak{p}}_{m-1} + \mathfrak{B}}} = \overline{\overline{\mathfrak{B}}}$. But, the number of generators of $\overline{\overline{\mathfrak{B}}}$ is at most $r - 1$. If we apply the induction hypothesis to $\overline{\overline{A}}$, we get $\mathrm{ht}(\overline{\overline{\mathfrak{p}_0}}) \leq r - 1$. Finally, by applying double bar to our detored chain, we get

$$\overline{\overline{\mathfrak{p}_0}} > \overline{\overline{\widetilde{\mathfrak{p}_1}}} > \cdots > \overline{\overline{\widetilde{\mathfrak{p}}}}_{m-2} > (0),$$

a chain of length $m - 1$. Therefore, $m - 1 \leq r - 1$, that is, $m \leq r$. □

Corollary 3.124 *In a noetherian ring, the prime ideals satisfy the descending chain condition. In particular, every prime ideal contains a minimal prime.*

Proof. Given a prime, $\mathfrak{p}$, it is finitely generated, say by r elements. Therefore, $\mathrm{ht}(\mathfrak{p}) \leq r$ and any descending chain starting at $\mathfrak{p}$ must stop. □

Corollary 3.125 *If A is a noetherian ring, then for every $\mathfrak{p} \in \operatorname{Spec} A$, the Krull dimension, $\dim(A_\mathfrak{p})$, is finite.*

Corollary 3.126 *Say A is noetherian, $a \neq 0$ is any given element in A and $\mathfrak{p}$ is an isolated prime of Aa. Then, every prime ideal, $\mathfrak{q}$, strictly contained in $\mathfrak{p}$ is an isolated prime of (0), i.e., consists of zero-divisors.*

Proof. By the principal ideal theorem, $\mathrm{ht}(\mathfrak{p}) \leq 1$, and $\mathrm{ht}(\mathfrak{p}) = 1$, as $\mathfrak{q} < \mathfrak{p}$. It follows that $\mathrm{ht}(\mathfrak{q}) = 0$, which means that $\mathfrak{q}$ is an isolated prime of (0).

Proposition 3.127 *(Converse of the height theorem) Let A be a noetherian ring. For every $\mathfrak{p} \in \operatorname{Spec} A$, if $\mathrm{ht}(\mathfrak{p}) \leq r$, then there is some ideal, $\mathfrak{A}$, of A generated by at most r elements and $\mathfrak{p}$ is an isolated prime of $\mathfrak{A}$.*

Proof. (DX). □

3.8 Further Readings

There is a vast literature on commutative rings and commutative algebra. Besides some of the references already given in Section 2.9, such as Atiyah MacDonald [3], Lafon [32, 33], Eisenbud [13], Matsumura [39], Malliavin [38], let us mention Bourbaki [6, 8, 7] Zariski and Samuel [50, 51], Jacobson [28] and Serre [46].

Chapter 4

Fields and Galois Theory

4.1 Introduction

The rational, real, complex and, much later, the finite fields were the basic inspiration for the study of fields in general. Their ideal theory and the module theory (vector spaces) over them are very simple; so, it was natural to look more deeply inside them. In particular, one can consider solutions of polynomial equations in a field, the automorphisms of a field, the relation of one field to another. We owe to E. Galois the capital idea of applying symmetry in the form of group theory to the study of polynomial equations (coefficients in a field) and their solutions in a (perhaps bigger) field. He was preceded in partial results by such figures as Lagrange, Abel and Gauss and the impetus he provided has sustained the subject until the current day. What concerns one now is not so much the "classical theory" (all of which in smooth modern form is treated below), but questions of basically geometric origin that use an admixture of group theory, ring theory and fields to try to settle vexing questions of apparently "simple" nature. For example, if we adjoin to the rationals all the roots of unity and call the resulting field K, is it true that every homogeneous form of degree $d > 0$ in more than d variables has a non-zero solution in K? This is a conjecture of E. Artin–still open at present.

4.2 Algebraic Extensions

Recall that if A is a commutative ring and B is an over-ring of A (i.e., an A-algebra), an element $\beta \in B$ is *algebraic over* A iff the map $A[X] \longrightarrow A[\beta] \subseteq B$ is *not* injective; the element β is *transcendental over* A iff the map $A[X] \longrightarrow A[\beta]$ is injective. Moreover, $\beta_1, \ldots, \beta_n$ are *independent transcendentals over* A (*algebraically independent over* A) iff $A[X_1, \ldots, X_n] \longrightarrow A[\beta_1, \ldots, \beta_n]$ is injective. The case of interest here is: $A = k$, a field, and B a subring of a field.

Algebraic elements admit of many characterizations:

Proposition 4.1 *Say B is an integral domain containing a field k and $\alpha \in B$. Then, the following are equivalent:*

(1) α is algebraic over k.

(2) $k[\alpha]$ $(\subseteq B)$ is a field.

(3) $k(\alpha) = k[\alpha]$.

(4) $1/\alpha \in k[\alpha]$.

(5) $k[\alpha]$ $(\subseteq B)$ is a finite dimensional k-vector space.

(6) $k[\alpha] \subseteq L$, where $L\,(\subseteq B)$ is a subring of B and L is a finite dimensional k-vector space.

Proof. (1) $\Rightarrow$ (2). By definition there is some polynomial $f \in k[X]$ so that $f(\alpha) = 0$. By unique factorization in $k[X]$, we know that $f = f_1 \cdots f_r$, where each f_j is irreducible. So, $0 = f(\alpha) = \prod_{j=1}^{r} f_j(\alpha)$ and as B is a domain, $f_j(\alpha) = 0$, for some j; so, we may assume that f is irreducible. Look at $k[X]/(f(X))$. Now, as $k[X]$ is a P.I.D and f is irreducible, it follows that $(f(X))$ is a maximal ideal. Thus, $k[X]/(f(X))$ is a field; moreover, $k[\alpha] \cong k[X]/(f(X))$ and (2) holds.

(2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (4) are clear.

(4) $\Rightarrow$ (5). By (4),

$$\frac{1}{\alpha} = \sum_{j=0}^{N} a_j \alpha^j$$

(with $\alpha_N \neq 0$) and this yields $\sum_{j=0}^{N} a_j \alpha^{j+1} = 1$; we deduce

$$\alpha^{N+1} = \frac{1}{a_N} - \sum_{j=0}^{N-1} \frac{a_j}{a_N}\, \alpha^{j+1},$$

i.e., α^{N+1} depends linearly on $1, \alpha, \ldots, \alpha^N$. By an obvious induction, α^{N+i} depends linearly on $1, \alpha, \ldots, \alpha^N$ for all $i \geq 1$ and so, $1, \alpha, \ldots, \alpha^N$ span $k[\alpha]$.

(5) $\Rightarrow$ (6) is a tautology.

(6) $\Rightarrow$ (1). Since $k[\alpha]$ is a subspace of a finite dimensional vector space, $k[\alpha]$ is finite dimensional over k (i.e., (5)). Look at $1, \alpha, \ldots, \alpha^N, \alpha^{N+1}, \ldots$ There must be a linear dependence, so

$$a_N \alpha^N + \cdots + a_1 \alpha + a_0 = 0$$

and α is a root of $f(X) = a_N X^N + \cdots + a_1 X + a_0$. □

Proposition 4.2 *Write $B_{\text{alg}} = \{\alpha \in B \mid \alpha$ is algebraic over $k\}$. Then, B_{alg} is a ring (a domain).*

Proof. Say $\alpha, \beta \in B_{\text{alg}}$. Then, $k[\alpha]$ is finite dimensional over k and $k[\alpha, \beta] = k[\alpha][\beta]$ is finite dimensional over $k[\alpha]$, which implies that $k[\alpha, \beta]$ is finite dimensional over k. As $\alpha \pm \beta$ and $\alpha\beta$ belong to $k[\alpha, \beta]$, by (6), they are algebraic over k. □

Proposition 4.3 *Say $\alpha, \beta \in B_{\text{alg}}$ (with $\beta \neq 0$), then $\alpha/\beta \in B_{\text{alg}}$. Therefore, B_{alg} is actually a field.*

Proof. As before, $k[\alpha, \beta]$ is finite dimensional over $k[\alpha]$. But, $k(\alpha) = k[\alpha]$ and $k[\alpha, \beta] = k[\alpha][\beta]$, so $k[\alpha, \beta] = k(\alpha)[\beta]$. Yet, β is algebraic over $k(\alpha)$; thus, $k(\alpha)[\beta] = k(\alpha)(\beta) = k(\alpha, \beta)$. Consequently, $k[\alpha, \beta] = k(\alpha, \beta)$ and it is finite dimensional over k. As $\alpha/\beta \in k(\alpha, \beta)$, it is algebraic over k. □

Proposition 4.4 *Being algebraic is transitive.*

Given an extension, K/k, the *degree,* $\deg(K/k) = [K\colon k]$, *of* K/k is the dimension of K as a vector space over k. Observe that if $[K\colon k]$ is finite, then K is algebraic over k (for every $\alpha \in K$, there is a linear dependence among $1, \alpha, \ldots, \alpha^n, \ldots$, so, α is the root of some polynomial in $k[X]$). However, an algebraic extension K/k *need not be finite*.

Definition 4.1 Let K/k be a field extension (i.e., $k \subseteq K$ where both are fields and K is a k-algebra). Say $\alpha \in K$ is a root of $f(X) \in k[X]$. Then, α is a *root of multiplicity, m,* iff $f(X) = (X - \alpha)^m g(X)$ in $K[X]$ and $g(\alpha) \neq 0$.

Let A be a commutative ring, B be an A-algebra and C be a B-algebra.

Definition 4.2 An additive map $\delta\colon B \to C$ is an *A-derivation of B with values in C* iff

(1) $\delta(\xi\eta) = \xi\delta(\eta) + \delta(\xi)\eta$ (Leibnitz)

(2) $\delta(\alpha) = 0$ whenever $\alpha \in A$.

Notice that (1) and (2) imply the A-linearity of an A-derivation. The A-derivations of B with values in C form a B-module denoted $\mathrm{Der}_A(B, C)$.

Examples of Derivations.

(1) Let A be a commutative ring, let $B = A[X]$ and let $C = B$.

$$\delta f = \delta\Big(\sum_{j=0}^{N} a_j X^j\Big) = \sum_{j=0}^{N} j a_j X^{j-1} = f'(X)$$

is an A-derivation.

(2) Let A be a commutative ring, $B = A[\{X_\alpha\}_{\alpha\in I}]$, $C = B$ and

$$\delta_\alpha = \frac{\partial}{\partial X_\alpha}.$$

Remark: For Example 1, if h is an independent transcendental from X, we have (DX)

$$f(X + h) = f(X) + f'(X)h + O(h^2).$$

Theorem 4.5 *(Jacobian criterion for multiplicity) Given $f(X) \in k[X]$ and K/k a field extension, for any root α of $f(X)$, we have:*

(1) If the multiplicity of α as a root is $\geq m$, then

$$f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0.$$

(2) If $\mathrm{char}(k) = 0$ and if $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ but $f^{(m)}(\alpha) \neq 0$, then α is a root of f of exact multiplicity m.

Proof. We proceed by induction on m. Consider a root, α, of multiplicity 1. This means $f(X) = (X-\alpha)g(X)$ in $K[X]$ and $g(\alpha) \neq 0$. Thus,

$$f'(X) = (X - \alpha)g'(X) + g(X),$$

so, $f'(\alpha) = g(\alpha)$ and $f'(\alpha) \neq 0$. Therefore, (2) holds independently of the characteristic of k in this one case and (1) is trivial.

Now, assume α is a root of multiplicity at least m. As $f(X) = (X - \alpha)^m g(X)$ in $K[X]$, we get

$$f'(X) = (X - \alpha)^{m-1}((X - \alpha)g'(X) + mg(X)),$$

which shows that the multiplicity of α in f' is at least $m - 1$. By the induction hypothesis applied to $f'(X)$, we have $f'(\alpha) = f''(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$. Also, $f(\alpha) = 0$, so (1) holds.

(2) Again, we proceed by induction. Assume that $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ but $f^{(m)}(\alpha) \neq 0$, with $\mathrm{char}(k) = 0$. Let q be the exact multiplicity of α. Then, $f(X) = (X-\alpha)^q h(X)$ in $K[X]$, with $h(\alpha) \neq 0$. Now, $f'(\alpha) = (f')'(\alpha) = \cdots = (f')^{(m-2)}(\alpha) = 0$ and the induction hypothesis applied to $f'(X)$ shows that

α is a root of exact multiplicity $m-1$ of f'. So, $f'(X) = (X-\alpha)^{m-1}g(X)$, with $g(\alpha) \neq 0$. We know that α is a root of multiplicity q of f, so by (1), $f(\alpha) = f'(\alpha) = \cdots = f^{(q-1)}(\alpha) = 0$. If $q > m$, then $q-1 \geq m$, so $f^{(m)}(\alpha) = 0$, a contradiction. Thus, $q \leq m$. As

$$f'(X) = (X-\alpha)^{q-1}((X-\alpha)h'(X) + qh(X)),$$

we have

$$(X-\alpha)^{m-1}g(X) = (X-\alpha)^{q-1}((X-\alpha)h'(X) + qh(X)),$$

and since $q \leq m$, we get

$$(X-\alpha)^{m-q}g(X) = (X-\alpha)h'(X) + qh(X).$$

If we let $X = \alpha$, we have $qh(\alpha) \neq 0$, as $h(\alpha) \neq 0$ and $\text{char}(k) = 0$; but then, the left hand side must not be zero, and this implies $m = q$. □

Proposition 4.6 *Say $f \in k[X]$ (k = a field), then there is an extension K/k of finite degree and an element $\theta \in K$ so that $f(\theta) = 0$. If $\widetilde{k}$ is another field and $\mu\colon k \to \widetilde{k}$ is an isomorphism of fields, write $\widetilde{f} \in \widetilde{k}[X]$ for the image of f under μ (i.e., $\mu\Big(\sum g_j X_j\Big) = \sum \mu(g_j)X^j$), then f is irreducible over $k[X]$ iff $\widetilde{f}$ is irreducible over $\widetilde{k}[X]$. Let θ be a root of an irreducible polynomial, $f(X)$, in some extension K/k and let $\widetilde{\theta}$ be a root of $\widetilde{f}$ in some extension $\Omega/\widetilde{k}$. Then, there exists a unique extension of μ to a field isomorphism $k(\theta) \longrightarrow \widetilde{k}(\widetilde{\theta})$, so that $\mu(\theta) = \widetilde{\theta}$.*

Proof. Factor f into irreducible factors in $k[X]$, then a root of an irreducible factor is a root of f, so we may assume that f is irreducible. Now, the ideal $(f(X))$ is maximal in $k[X]$. Therefore, $K = k[X]/(f(X))$ *is* a field and $\overline{X}$ = the image of X in K is θ, a root, and $[K\colon k] = \deg(f) < \infty$.

Next, we have $\mu\colon k \to \widetilde{k}$ and $f \in k[X]$. Of course,

$$k[X] \cong k \otimes_{\mathbb{Z}} \mathbb{Z}[X] \cong \widetilde{k} \otimes_{\mathbb{Z}} \mathbb{Z}[X] \cong \widetilde{k}[X],$$

so f is irreducible iff $\widetilde{f}$ is irreducible. Now, $\theta \in K$ is a root of an irreducible polynomial, f, and $\widetilde{\theta} \in \Omega$ is a root of an irreducible polynomial $\widetilde{f}$. But, $k(\theta) \cong k[X]/(f(X)) \xrightarrow{\mu} \widetilde{k}[X]/(\widetilde{f}(X)) \cong \widetilde{k}(\widetilde{\theta})$. As θ generates $k(\theta)$ over k, the element $\mu(\theta)$ determines the extension of μ to $k(\theta)$. □

Proposition 4.7 *Say k is a field, $f \in k[X]$ and K/k is a field extension. Then, f possesses at most* $\deg(f)$ *roots in K counted with multiplicity and there exists an algebraic extension L/k (in fact, $[L\colon k] < \infty$) where f has exactly* $\deg(f)$ *roots counted with multiplicity.*

Proof. We use induction on $\deg(f)$. If $\alpha \in K/k$ is a root of f, then in $K[X]$, we have

$$f(X) = (X-\alpha)g(X), \quad \text{where } g(X) \in K[X]. \tag{$*$}$$

But, $\deg(g) = \deg(f) - 1$, so there exist at most $\deg(f) - 1$ roots of g in the field, K, containing k. If β is a root of f, either $\beta = \alpha$ or $g(\beta) = 0$ as K is a domain. Then, the first statement is proved. The last statement is again proved by induction. In the above, we can take $K = k(\alpha)$, of finite degree over k. Then, induction and $(*)$ imply our counting statement. □

Corollary 4.8 *(of the proof) The degree $[K\colon k]$ of a minimum field containing all* $\deg(f)$ *roots of f always satisfies $[K\colon k] \leq \deg(f)!$.*

Remarks:

(1) Proposition 4.7 is false if K is a ring but *not* a domain. For example, take

$$K = \underbrace{k \prod k \prod \cdots \prod k}_{n}.$$

Then, if $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the j-th place, each e_j solves $X^2 = X$.

(2) Let $K = k[T]/(T^2)$. The elements $\alpha = \lambda\overline{T} \in K$ all satisfy $X^2 = 0$. If k is infinite, there are infinitely many solutions.

(3) Let $k = \mathbb{R}$ and $K = \mathbb{H}$ (the quaternions). We know that $\mathbb{H}$ is a division ring, i.e., every nonzero element has a multiplicative inverse. Consider the equation $X^2 + 1 = 0$. Then, every $\alpha = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$ with $a^2 + b^2 + c^2 = 1$ satisfies our equation!

(4) Given a field, k, there exists a field extension K/k having two properties:

(a) K/k is algebraic (but in general, $[K\colon k] = \infty$).

(b) For every $f \in K[X]$, there exists $\theta \in K$ so that $f(\theta) = 0$.

We'll prove these facts at the end of the Chapter in Section 4.11

Such a field, K, is called an *algebraic closure of* k and if only (2) holds, K is called *algebraically closed*. The field K is unique up to noncanonical isomorphism. The usual notation for an algebraic closure of k is $\overline{k}$.

4.3 Separable Extensions, Kähler Differentials, Mac Lane's Criterion

Definition 4.3 An algebraic element α over a field k (i.e., $\alpha \in K$ is algebraic over k for some field extension K/k) is *separable over* k iff α is a simple root of its minimal k-polynomial.[1] A polynomial, f, is *separable* iff all its irreducible factors are distinct and separable, and an irreducible polynomial is *separable* if it has one (hence all) separable roots. The field extension K/k is *separable* iff all $\alpha \in K$ are separable over k. We use the adjective *inseparable* to mean not separable.

Proposition 4.9 *Suppose α is inseparable over k. Then,* $\mathrm{char}(k) = p > 0$. *If f is the minimal polynomial for α, then there is some $n \geq 1$ and some irreducible polynomial $g(X) \in k[X]$ so that $f(X) = g(X^{p^n})$. If we choose n maximal then*

(1) $g(X)$ is a separable polynomial and

(2) α^{p^n} is separable over k. Any root β of f has the property that β^{p^n} is separable over k.

Proof. The element α is inseparable iff $f'(\alpha) = 0$ by the $n = 1$ case of the Jacobian criterion. Thus, f divides f', yet $\deg(f') < \deg(f)$. Therefore, $f' \equiv 0$. If $f(X) = \sum_{j=0}^{d} a_j X^j$, then $f'(X) = \sum_{j=0}^{d-1} j a_j X^{j-1}$ and it follows that $j a_j = 0$, for all j. If $\mathrm{char}(k) = 0$, then $a_j = 0$ for all $j \neq 0$ and $f \equiv 0$, as α is a root. Thus, we must have $\mathrm{char}(k) = p > 0$ and if p does not divide j, then $a_j = 0$. We deduce that

$$f(X) = \sum_{r=0}^{e} a_{pr} X^{pr} = h_1(X^p),$$

where $h_1(X) = \sum_{r=0}^{e} a_{pr} X^r$. Note that h_1 must be irreducible and repeat the above procedure if necessary. As $\deg(h_1) < \deg(f)$, this process must stop after finitely many steps. Thus, there is a maximum n with $f(X) = g(X^{p^n})$ and $g(X)$ is irreducible in $k[X]$. Were $g(X)$ inseparable, the first part of the argument would imply that $g(X) = h(X^p)$ and so, $f(X) = h(X^{p^{n+1}})$, contradicting the maximality of n. Therefore, $g(X)$ is separable. Yet, $g(\alpha^{p^n}) = f(\alpha) = 0$, so α^{p^n} is a root of an irreducible separable polynomial and (2) holds. Given β, we have β^{p^n} again a root of g. □

Definition 4.4 A field k of characteristic $p > 0$ is *perfect* iff $k = k^p$, i.e., for every $\lambda \in k$, the element λ has a p-th root in k.

Examples of Perfect and Imperfect Fields.

(1) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is prime, is perfect.

(2) Any finite field is perfect.

(3) The field $k(T)$, where $\mathrm{char}(k) = p > 0$ is *always imperfect*.

Proposition 4.10 *If k is a field with characteristic* $\mathrm{char}(k) = p > 0$ *and if $c \notin k^p$ (with $c \in k$), then for every $n \geq 0$, the polynomial $f(X) = X^{p^n} - c$ is irreducible in $k[X]$. Conversely, if for some $n > 0$ the polynomial $X^{p^n} - c$ is irreducible, then $c \notin k^p$.*

Proof. Look at $f(X) = X^{p^n} - c$ and pick a field, K, with a root, $\alpha \in K$, of f. Then, $\alpha^{p^n} - c = 0$, so $f(X) = X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}$, since $\mathrm{char}(k) = p > 0$. Say $\varphi(X) \in k[X]$ is an irreducible factor of $f(X)$, then $\varphi(X) \mid f(X)$ in $k[X]$, and similarly in $K[X]$. By unique factorization in $K[X]$, we have $\varphi(X) = (X - \alpha)^r$, for some $r > 0$, where $\alpha^{p^n} - c = 0$ and $\alpha \in K$.

[1] Recall that the *minimal k-polynomial of α* is the monic polynomial of minimal degree generating the principal ideal consisting of the polynomials in $k[X]$ that vanish on α.

Claim: $X^{p^n} - c$ is a power of $\varphi(X)$.

If not, there is some irreducible polynomial, $\psi(X)$, relatively prime to $\varphi(X)$ and $\psi(X) \mid X^{p^n} - c$ in $k[X]$ (DX). Then, there exist $s(X), t(X)$ with $s(X)\varphi(X) + t(X)\psi(X) = 1$ in $k[X]$. However, $\psi(X)$ divides $X^{p^n} - c$, so $\psi(\alpha) = 0$. If we let $X = \alpha$, we get $1 = s(\alpha)\varphi(\alpha) + t(\alpha)\psi(\alpha) = 0$, a contradiction.

Therefore, $\varphi(X)^l = X^{p^n} - c$. It follows that $rl = p^n$, so $r = p^a$ and $l = p^b$ with $a + b = n$. Then,

$$\varphi(X) = (X - \alpha)^r = (X - \alpha)^{p^a} = X^{p^a} - \alpha^{p^a},$$

which implies $\alpha^{p^a} \in k$. But then, $c = (\alpha^{p^a})^{p^b} \in k^{p^b}$, a contradiction if $b \geq 1$. Thus, $b = 0$ and consequently, $a = n$ and $f(X) = \varphi(X)$ is irreducible.

Conversely, if for some $n > 0$ the polynomial $X^{p^n} - c$ is irreducible and if $c \in k^p$, then $c = b^p$, for some $b \in k$. It follows that

$$X^{p^n} - c = X^{p^n} - b^p = (X^{p^{n-1}} - b)^p$$

contradicting the irreducibility of $X^{p^n} - c$. □

Definition 4.5 An element $\alpha \in K/k$ is *purely inseparable over* k ($\mathrm{char}(k) = p > 0$) iff there is some $n \geq 0$ so that $\alpha^{p^n} \in k$. Equivalently, α is purely inseparable over k iff the minimal k-polynomial for α is of the form $X^{p^n} - c$, for some $c \in k$.

Remark: We have $\alpha \in k$ iff α is separable *and* purely inseparable over k.

Proposition 4.11 *If k is a field, then k is perfect iff every algebraic extension of k is separable.*

Proof. ($\Rightarrow$). Say k is perfect and pick $\alpha \in K/k$, with α algebraic. We know that α has a minimal k-polynomial $f(X)$ and that $f(X) = g(X^{p^n})$, for some irreducible polynomial, $g(X)$, and some $n \geq 0$. We have $g(X) = \sum_{j=0}^{N} b_j X^j$, so $f(X) = \sum_{j=0}^{N} b_j (X^{p^n})^j$. As k is perfect, $k = k^p = k^{p^2} = \cdots = k^{p^n}$. So, $b_j = c_j^{p^n}$, for some $c_j \in k$ and we have

$$f(X) = \sum_{j=0}^{N} c_j^{p^n} (X^{p^n})^j = \Big(\sum_{j=0}^{N} c_j X^j\Big)^{p^n}.$$

This contradicts the irreducibility of $f(X)$ unless $n = 0$, and we know that $\alpha^{p^0} = \alpha$ is separable over k.

($\Leftarrow$). In this case, all algebraic extensions of k are separable and say k is not perfect. Then, there is some $c \in k$, with $c \notin k^p$. Hence, by Proposition 4.10, the polynomial $X^p - c$ is irreducible over k. Let $K = k(\alpha)$ where α is some root of $X^p - c$. Then, $\alpha^p = c \in k$ and it follows that α is purely inseparable over k. But, α is separable over k, a contradiction, as $\alpha \notin k$. □

Corollary 4.12 *For a field, k, the following are equivalent:*

(1) k is imperfect.

(2) k possesses nontrivial inseparable extensions.

(3) k possesses purely inseparable extensions.

Say K/k is algebraic and inseparable. It can happen that there does not exist $\alpha \in K$ with α purely inseparable over k.

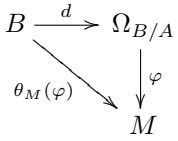
To go further, we need derivations and Kähler differentials. Consider the situation where A, B are commutative rings and B is an A-algebra. On B-modules, we have an endofunctor:

$$M \rightsquigarrow \mathrm{Der}_A(B, M).$$

Is the above functor representable? This means, does there exist a B-module, $\Omega_{B/A}$, and an element, $d \in \mathrm{Der}_A(B, \Omega_{B/A})$, so that functorially in M

$$\theta_M \colon \mathrm{Hom}_B(\Omega_{B/A}, M) \xrightarrow{\sim} \mathrm{Der}_A(B, M)?$$

(Note: For every $\varphi \in \mathrm{Hom}_B(\Omega_{B/A}, M)$, we have $\theta_M(\varphi) = \varphi \circ d$, see below).



Theorem 4.13 *The functor $M \rightsquigarrow \mathrm{Der}_A(B, M)$ is representable by a pair $(\Omega_{B/A}, d)$, as above.*

Proof. Consider $B \otimes_A B$ and the algebra map $B \otimes_A B \xrightarrow{\mu} B$, where μ is multiplication, i.e., $\mu(b \otimes \widetilde{b}) = b\widetilde{b}$. Let $I = \mathrm{Ker}\ \mu$ and write $I/I^2 = \Omega_{B/A}$. We let B act on $B \otimes_A B$ *via* the left action $b(\xi \otimes \eta) = b\xi \otimes \eta$. Then, $\Omega_{B/A}$ is a B-module. Given $b \in B$, set

$$db = d(b) = (1 \otimes b - b \otimes 1) \bmod I^2.$$

Now, for $b, \widetilde{b} \in B$, we have

$$(1 \otimes b - b \otimes 1)(1 \otimes \widetilde{b} - \widetilde{b} \otimes 1) \in I^2,$$

and we get

$$1 \otimes b\widetilde{b} + b\widetilde{b} \otimes 1 - (b \otimes \widetilde{b} + \widetilde{b} \otimes b) \in I^2.$$

So, modulo I^2, the above is zero and

$$1 \otimes b\widetilde{b} - \widetilde{b} \otimes b = b \otimes \widetilde{b} - b\widetilde{b} \otimes 1 \quad \text{in } \Omega_{B/A}.$$

Obviously, d is additive and zero on A, so we only need to check the Leibnitz rule. We have

$$\begin{aligned} bd(\widetilde{b}) &= b(1 \otimes \widetilde{b} - \widetilde{b} \otimes 1) \quad \bmod I^2 \\ &= b \otimes \widetilde{b} - b\widetilde{b} \otimes 1 \quad \text{in } \Omega_{B/A} \\ &= 1 \otimes b\widetilde{b} - \widetilde{b} \otimes b \quad \text{in } \Omega_{B/A} \\ &= 1 \otimes b\widetilde{b} - b\widetilde{b} \otimes 1 + b\widetilde{b} \otimes 1 - \widetilde{b} \otimes b \quad \text{in } \Omega_{B/A} \\ &= d(b\widetilde{b}) - \widetilde{b}(1 \otimes b - b \otimes 1) \quad \text{in } \Omega_{B/A}. \end{aligned}$$

So, $bd(\widetilde{b}) = d(b\widetilde{b}) - \widetilde{b}db$ in $\Omega_{B/A}$, namely $d(b\widetilde{b}) = \widetilde{b}db + bd(\widetilde{b})$. The rest of the proof is routine. □

Definition 4.6 The B-module $\Omega_{B/A}$ (together with the derivation d) is called the *module of relative Kähler differentials of B over A*.

Examples of Relative Kähler Differentials.

(1) Let $B = A[T_1, \ldots, T_n]$. Say D is a derivation of $B \longrightarrow M$ trivial on A. So, we know $D(T_1), \ldots, D(T_n)$; these are some elements in M. Say we are given $T_l^r \in B$. Then,

$$D(\underbrace{T_l \cdots T_l}_{r}) = rT_l^{r-1}D(T_l) = \frac{\partial}{\partial T_l}(T_l^r)D(T_l).$$

Now,

$$D(T_k^r T_l^s) = T_k^r D(T_l^s) + T_l^s D(T_k^r) = T_k^r \frac{\partial}{\partial T_l}(T_l^s) D(T_l) + T_l^s \frac{\partial}{\partial T_k}(T_k^r) D(T_k).$$

In general

$$D(T_1^{a_1} \cdots T_n^{a_n}) = \sum_{j=1}^{n} T_1^{a_1} \cdots \widehat{T_l^{a_l}} \cdots T_n^{a_n} \frac{\partial}{\partial T_l}(T_l^{a_l}) D(T_l), \tag{$\dagger$}$$

and

$$D\Big(\sum \alpha_{(a)} T^{(a)}\Big) = \sum_{(a)} \alpha_{(a)} D(T^{(a)}) D(T_l), \tag{$\dagger\dagger$}$$

as $D \restriction A \equiv 0$. Conversely, ($\dagger$) on the linear base of monomials in the $T_1, \ldots, T_n$ of B gives a derivation. Therefore,

$$\mathrm{Der}_A(B, M) \longrightarrow \coprod_{i=1}^{n} M,$$

via $D \mapsto (D(T_1), \ldots, D(T_n))$ is a functorial isomorphism. Consequently,

$$\Omega_{B/A} \cong \coprod_{j=1}^{n} B dT_j,$$

where the dT_j are A-linearly independent elements of $\Omega_{B/A}$ (case $M = \Omega_{B/A}$).

(2) Let B be a f.g. algebra over A, i.e., $B = A[T_1, \ldots, T_n]/(f_1, \ldots, f_p)$. We have

$$\mathrm{Der}_A(B, M) = \{\varphi \in \mathrm{Der}_A(A[T_1, \ldots, T_n], M) \mid \varphi(f_i) = 0,\ i = 1, \ldots, p\}.$$

But,

$$\varphi(f_i) = \sum_{j=1}^{n} \frac{\partial f_i}{\partial T_j} \varphi(T_j) = \sum_{j=1}^{n} \frac{\partial f_i}{\partial T_j} \overline{\varphi}(dT_j),$$

where $\overline{\varphi}\colon \Omega_{B/A} \longrightarrow M$ (and $\varphi = \overline{\varphi} \circ d$). We let $M = \Omega_{B/A}$ to determine it, and we see that

$$\overline{\varphi} \text{ must kill } df_i.$$

It follows that

$$\Omega_{B/A} = \left(\coprod_{j=1}^{n} B dT_j\right) \Big/ (\text{submodule } df_1 = \cdots = df_n = 0).$$

(3) Let $B = \mathbb{C}[X, Y]/(Y^2 - X^3)$ and $A = \mathbb{C}$. From (2) we get

$$\Omega_{B/A} = (B dX \amalg B dY)/(2Y dY - 3X^2 dX).$$

The module $\Omega_{B/A}$ is *not* a free B-module (due to the singularity at the origin of the curve $Y^2 = X^3$).

(4) Let $A = \mathbb{R}$ or $\mathbb{C}$ and $B =$ the ring of functions on a small neighborhood of a smooth r-dimensional manifold (over A). Derivations on B over A have values in B. Let $\xi_1, \ldots, \xi_r$ be coordinates on this neighborhood. Then, $\partial/\partial\xi_j$ is a derivation defined so that

$$\frac{\partial f}{\partial \xi_j} = \lim_{h \longrightarrow 0} \frac{f(\ldots, \xi_j + h, \ldots) - f(\ldots, \xi_j, \ldots)}{h}.$$

Look near a point, we may assume $\xi_1 = \cdots = \xi_r = 0$, there. By Taylor,

$$f(\xi_1 + h_1, \ldots, \xi_r + h_r) = f(\xi_1, \ldots, \xi_r) + \sum_{j=1}^{r} \frac{\partial f}{\partial \xi_j} h_j + O(\|h\|^2).$$

Hence, $\Omega_{B/A}$ is generated by $d\xi_1, \ldots, d\xi_r$ and they are linearly independent over B because the implicit function theorem would otherwise imply that some ξ_j is a function of the other ξ_i's near our point, a contradiction.

Definition 4.7 Given an A-algebra, B, the algebra B is *étale over* A iff

(1) The algebra B is flat over A.

(2) The algebra B is f.p. as an A-algebra.

(3) $\Omega_{B/A} = (0)$.

The algebra B is *smooth over* A iff (1), (2) and (3′): $\Omega_{B/A}$ is a locally-free B-module, hold.

Remark: Putting aside (2), we see that checking that an algebra is *étale* or smooth is local on A, i.e., it is enough to check it for $B_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Spec} A$. This is because (DX)

$$(\Omega_{B/A})_{\mathfrak{p}} = \Omega_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}.$$

It turns out that smooth means: Locally on A, the algebra B looks like

$$A \hookrightarrow A[T_1, \ldots, T_r] \longrightarrow B$$

where $B/A[T_1, \ldots, T_r]$ is *étale*.

We can apply the concepts of relative Kähler differentials and étale homomorphisms to field theory. For this, given a field, write $p = \operatorname{char}(k)$ and if $p > 0$, let $k^{1/p}$ be the field

$$k^{1/p} = \{x \in \overline{k} \mid x^p \in k\}.$$

Theorem 4.14 *(Main theorem on separability (alg. case).) Let K/k be an algebraic extension. Then, in the following statements: (1) implies any of the others; (2), (2a) and (3) are equivalent; (1) and (4) are equivalent; all are equivalent if K/k is finite.*

(1) The extension K/k is separable.

(2) For all K-modules, M, we have $\operatorname{Der}_k(K, M) = (0)$.

(2a) $\Omega_{K/k} = (0)$, i.e., when K/k is finite, it is étale.

(3) Every derivation of k to M (where M is a K-vector space) which admits an extension to K (i.e., becomes a derivation $K \longrightarrow M$) admits a unique extension.

When $\operatorname{char}(k) = p > 0$,

(4) Mac Lane I*: The natural map $k^{1/p} \otimes_k K \longrightarrow K^{1/p}$ is injective.*

(5) Mac Lane II*: $kK^p = K$.*

In order to prove Theorem 4.14, we first need the following subsidiary statement:

Proposition 4.15 *If K/k is separable and if M is a K-vector space, then every derivation $D\colon k \to M$ admits an extension to a derivation of K with values in M.*

Proof. We use Zorn's lemma. Let $\mathcal{S}$ be the set of all pairs, (L, D_L), where

(1) L is a subextension of K/k (i.e., $k \subseteq L \subseteq K$).

(2) D_L is an extension of D to L with values in M.

As $(k, D) \in \mathcal{S}$, the set $\mathcal{S}$ is nonempty. Define a partial order on $\mathcal{S}$ by: $(L, D_L) \leq (L', D_{L'})$ iff $L \subseteq L'$ and $D_{L'} \restriction L = D_L$. The set $\mathcal{S}$ is inductive. (If $\{L_\alpha\}_\alpha$ is a chain, then $L = \bigcup_\alpha L_\alpha$ *is* a field, and define $D_L(\xi) = D_{L_\alpha}(\xi)$, where $\xi \in L_\alpha$; this is well-defined (DX).) By Zorn's lemma, there exists a maximal extension, say (L, D_L).

If $K \neq L$, then there is some $\beta \in K$ with $\beta \notin L$. Let $g(X) \in L[X]$ be the minimum L-polynomial for β. We try to extend D_L to $L(\beta)$. For this, we must define $D_{L(\beta)}(\beta)$ and the only requirement it needs to satisfy is

$$0 = D_{L(\beta)}(g(\beta)) = g'(\beta)D_{L(\beta)}(\beta) + D_L(g)(\beta).$$

Here, if $g(X) = \sum_{j=1}^r a_j X^j$, then $D_L(g)(\alpha)$ is $\sum_{j=1}^r \alpha^j D_L(a_j) \in M$. Since β is separable, $g'(\beta) \neq 0$, so we can find the value of $D_{L(\beta)}(\beta)$, contradicting the maximality of our extension. Therefore, $L = K$. □

Proof of Theorem 4.14. (1) ⇒ (2). Pick $D \in \mathrm{Der}_k(K, M)$ and $\alpha \in K$; by (1), the element α is separable over k, i.e., α has a minimal k-polynomial, $g(X)$, so that $g(\alpha) = 0$ and $g'(\alpha) \neq 0$. As D is a derivation, the argument of Proposition 4.15 implies that

$$0 = D(g(\alpha)) = g'(\alpha)D(\alpha) + D(g)(\alpha).$$

But, $D(g) = 0$, because the coefficients of g are in k and $D \restriction k \equiv 0$. Since $g'(\alpha) \neq 0$, we get $D(\alpha) = 0$, i.e., (2) holds.

(2) ⇒ (2a). We have the functor $M \rightsquigarrow \mathrm{Der}_k(K, M)$ and $\mathrm{Der}_k(K, M) = (0)$. By Yoneda's lemma, the representing object, $\Omega_{K/k}$, must vanish.

(2a) ⇒ (2). We have $\mathrm{Hom}_k(\Omega_{K/k}, M) \cong \mathrm{Der}_k(K, M)$ and $\Omega_{K/k} = (0)$, so (2) holds.

(2) ⇒ (3). Say D and $\widetilde{D}$ are two extensions of the same derivation on k. Then, $D - \widetilde{D}$ is a derivation and $(D - \widetilde{D}) \restriction k \equiv 0$. By (2), $(D - \widetilde{D}) \in \mathrm{Der}_k(K, M) = (0)$, so $D - \widetilde{D} = 0$.

(3) ⇒ (2). Choose $D \in \mathrm{Der}_k(K, M)$, so $D \restriction k \equiv 0$. But then, D extends 0 and 0 extends 0; by (3), $D \equiv 0$.

(1) ⇒ (5). If $\alpha \in K$, then α is separable over k, so α is separable over kK^p (as $kK^p \supseteq k$). Yet, $\alpha^p \in K^p$, so $\alpha^p \in kK^p$; thus, α is purely inseparable over kK^p. As α is both separable and purely inseparable over kK^p, by a previous remark, $\alpha \in kK^p$. This shows $K \subseteq kK^p$. On the other hand, $kK^p \subseteq K$, always. Therefore, $K = kK^p$, i.e., (5) holds.

Before discussing the equivalence of (4) with (1), we need to elucidate the meaning of the Mac Lane conditions.

For (5), say $\{\xi_\lambda\}_\lambda$ spans K as a k-vector space. Then, $\{\xi_\lambda^p\}_\lambda$ spans K^p as a k^p-space. As $k^p \subseteq k$, $\{\xi_\lambda^p\}_\lambda$ spans kK^p as a *k-space*. Hence, *Mac Lane II means: If $\{\xi_\lambda\}_\lambda$ spans K as a k-space, so does $\{\xi_\lambda^p\}_\lambda$.*

For (4), say $\{\xi_\lambda\}_\lambda$ is a linearly independent family (for short, an *l.i.* family) over k in K. Then, we know that the elements $1 \otimes \xi_\lambda$ are linearly independent in $k^{1/p} \otimes_k K$ as $k^{1/p}$-vectors ($k^{1/p}$ acts on the left on $k^{1/p} \otimes_k K$). The map $k^{1/p} \otimes_k K \longrightarrow K^{1/p}$ is just

$$\sum_\lambda a_\lambda \otimes \xi_\lambda \mapsto \sum_\lambda a_\lambda \xi_\lambda.$$

If the map is injective and if there is a linear dependence of the ξ_λ (in $K^{1/p}$) *over* $k^{1/p}$, we get $\sum_\lambda a_\lambda \xi_\lambda = 0$, for some $a_\lambda \in k^{1/p}$. But then, $\sum_\lambda a_\lambda \otimes \xi_\lambda$ would go to zero and by injectivity

$$\sum_\lambda a_\lambda \otimes \xi_\lambda = \sum_\lambda (a_\lambda \otimes 1)(1 \otimes \xi_\lambda) = 0$$

in $k^{1/p} \otimes_k K$. But, $\{1 \otimes \xi_\lambda\}_\lambda$ is linearly independent in $k^{1/p} \otimes_k K$, so $a_\lambda = 0$, for all λ. Consequently, the family $\{\xi_\lambda\}_\lambda$ is still linearly independent over $k^{1/p}$. Conversely (DX), if any l.i. family $\{\xi_\lambda\}_\lambda$ (with $\xi_\lambda \in K$) over k remains l.i. over $k^{1/p}$, then our map $k^{1/p} \otimes_k K \longrightarrow K^{1/p}$ is injective. By using the isomorphism $x \mapsto x^p$, we get: *Mac Lane I says that any l.i. family* $\{\xi_\lambda\}_\lambda$ *over* k*, has the property that* $\{\xi_\lambda^p\}_\lambda$ *is still l.i. over* k*.*

Now, say K/k is finite, with $[K\colon k] = n$. Then, $\xi_1, \ldots, \xi_n$ is l.i. over k iff $\xi_1, \ldots, \xi_n$ span K. Condition (4) implies $\xi_1^p, \ldots, \xi_n^p$ are l.i. and since there are n of them, they span K, i.e. (5) holds. Conversely, if (5) holds then $\xi_1^p, \ldots, \xi_n^p$ span K and there are n of them, so they are l.i., i.e., (4) holds. *Therefore, (4) and (5) are equivalent if* K/k *is finite*. We can show that (1) and (4) are equivalent (when $\mathrm{char}(k) = p > 0$).

(4) $\Rightarrow$ (1). Pick $\alpha \in K$. We know that α^{p^n} is separable over k for some $n \geq 0$. Further, the minimal polynomial for $\beta = \alpha^{p^n}$ is $h(X)$, where $f(X) = h(X^{p^n})$ and f is the minimal k-polynomial for α. Say, $\deg(f) = d$. So, $d = p^n d_0$, with $d_0 = \deg(h)$. Now, $1, \alpha, \ldots, \alpha^{d-1}$ are l.i. over k. By (4), repeatedly, $1, \alpha^{p^n}, (\alpha^2)^{p^n}, \ldots, (\alpha^{d-1})^{p^n}$ are l.i., i.e., $1, \beta, \ldots, \beta^{d-1}$ are l.i. Yet, $1, \beta, \ldots, \beta^{d_0}$ is the maximum l.i. family for the powers of β, so $d \leq d_0$. This can only happen if $n = 0$ and α is separable over k. □

(1) $\Rightarrow$ (4). Say $\{\xi_\lambda\}_\lambda$ is l.i. in K/k. As linear independence is checked by examining finite subfamilies, we may assume that our family is $\xi_1, \ldots, \xi_t$. We must prove, $\xi_1^p, \ldots, \xi_t^p$ are still l.i. over k. Let $L = k(\xi_1, \ldots, \xi_t)$, then L/k is a *finite* extension. For such an extension, (4) and (5) are equivalent. But, we just proved that (1) implies (5), so (1) implies (4).

Finally, in the case K/k is finite there remains the proof of (2) $\Rightarrow$ (1). For this, it is simplest to prove a statement we'll record as Corollary 4.16 below. This is:

Corollary 4.16 *If* $\alpha_1, \ldots, \alpha_t$ *are each separable over* k*, then the field* $k(\alpha_1, \ldots, \alpha_t)$ *is separable over* k*. In particular, if* K/k *is algebraic and* K_{sep} *denotes the set of all elements of* K *that are separable over* k*, then* K_{sep} *is a field.*

To prove these statements, we will apply Mac Lane II; this will suffice as $L = k(\alpha_1, \ldots, \alpha_t)$ is finite over k. Now $kL^p = k(\alpha_1^p, \ldots, \alpha_t^p)$ and each α_j is therefore purely inseparable over kL^p. However, each α_j is separable over k and therefore over kL^p. It follows that each $\alpha_j \in kL^p$ so that $L = kL^p$ and Mac Lane II applies. For the proof, proper, that (2) $\Rightarrow$ (1), assume (2) and that (1) is false. Then $K_{\mathrm{sep}} \neq K$, so we can find $\alpha_1, \ldots, \alpha_s \in K$, each purely inseparable over K_{sep}, and so that

$$K = K_{\mathrm{sep}}(\alpha_1, \ldots, \alpha_s) > K_{\mathrm{sep}}(\alpha_1, \ldots, \alpha_{s-1}) > \cdots > K_{\mathrm{sep}}(\alpha_1) > K_{\mathrm{sep}}.$$

Consider the zero derivation on $K_{\mathrm{sep}}(\alpha_1, \ldots, \alpha_{s-1})$. Now, $\beta = \alpha_s^{p^r} \in K_{\mathrm{sep}}(\alpha_1, \ldots, \alpha_{s-1})$ for some minimal $r > 0$, thus to extend the zero derivation to K we need only assign a value to $D(\alpha_s)$ so that $D(\alpha_s^{p^r}) = p^r \alpha_s^{p^{r-1}} D(\alpha_s) = 0$. Any nonzero element of M will do, contradicting (2). □

Corollary 4.17 *Every algebraic extension of a perfect field is perfect. In particular, every finite field is perfect and every absolutely algebraic field (i.e., algebraic over a prime field) is perfect.*

Proof. If K/k is algebraic and k is perfect, then K/k is separable. By Mac Lane II, we have $K = kK^p$. But, $k = k^p$ (k perfect), so $K = k^p K^p = (kK)^p = K^p$. A finite field is algebraic over $\mathbb{F}_p$ and by little Fermat, $\mathbb{F}_p^p = \mathbb{F}_p$, i.e., perfect. (Second proof by counting: The map $\xi \mapsto \xi^p$ is injective, taking $\mathbb{F}_q$ to itself. But, the image has cardinality q; by finiteness, the image is all of $\mathbb{F}_q$.) By the first part of the proof, an absolutely algebraic field is perfect.

Corollary 4.18 *Say $\alpha_1, \ldots, \alpha_t$ are each separable over k. Then, the field $k(\alpha_1, \ldots, \alpha_t)$ is a separable extension of k. In particular, if K/k is algebraic and we set*

$$K_{\text{sep}} = \{\alpha \in K \mid \alpha \text{ is separable over } k\}$$

then K_{sep} is a subfield of K/k called the separable closure of k in K.

Corollary 4.19 *Say K/k is an algebraic extension and $\alpha_1, \ldots, \alpha_t \in K$. If each α_j is separable over $k(\alpha_1, \ldots, \alpha_{j-1})$, then $k(\alpha_1, \ldots, \alpha_t)$ is separable over k. In particular, separability is transitive.*

Proof. We use induction on t. When $t = 1$, this is Corollary 4.18. Assume that the induction hypothesis holds for $t - 1$. So, $L = k(\alpha_1, \ldots, \alpha_{t-1})$ is separable over k and it is a finite extension, therefore Mac Lane II yields $kL^p = L$. Let $M = k(\alpha_1, \ldots, \alpha_t)$, then $M = L(\alpha_t)$. So, M is separable over L, by the case $t = 1$. Therefore, $M = LM^p$, by Mac Lane II. Now,

$$M = LM^p = kL^pM^p = k(LM)^p = kM^p.$$

By Mac Lane II, again, M is separable over k. □

Corollary 4.20 *If K/k is an algebraic extension, then K is purely inseparable over K_{sep}.*

Corollary 4.21 *Pure inseparability is transitive.*

The implication (2) ⇒ (1) does not hold if K/k is not finite. Here is an example: Set $k = \mathbb{F}_p(T)$, where T is an indeterminate. Define, inductively, the chain of fields

$$k = k_0 < k_1 < \cdots < k_n < \cdots$$

via the rule

$$\alpha_0 = T; \quad \alpha_j = \alpha_{j-1}^{1/p}; \quad k_j = k_{j-1}(\alpha_j).$$

Let $K = k_\infty = \bigcup_{j=0}^{\infty} k_j$. Then a derivation on K, trivial on k is determined by its values on the α_j. Yet, we have $\alpha_{j+1}^p = \alpha_j$, therefore $D(\alpha_j) = 0$ for every j; hence, $\text{Der}_k(K, -) = 0$. But, K/k is not separable; indeed it is purely inseparable.

Notation: For a field, k, of characteristic $p > 0$, set $[K\colon k]_s \stackrel{\text{def}}{=} [K_{\text{sep}}\colon k]$, the *separable degree of K/k* and $[K\colon k]_i \stackrel{\text{def}}{=} [K\colon K_{\text{sep}}]$, the *purely inseparable degree of K/k* (if K/k is finite, $[K\colon k]_i$ is a power of p). Clearly,

$$[K\colon k] = [K\colon k]_i[K\colon k]_s.$$

4.4 The Extension Lemma and Splitting Fields

We begin with a seemingly "funny" notion: Two fields K, L are *related*, denoted $K \underset{\text{rel}}{\sim} L$, iff there is some larger field, W, so that $K \subseteq W$ and $L \subseteq W$ (as sets, *not* isomorphic copies). This notion is reflexive and symmetric, but *not* transitive.

Theorem 4.22 *(Extension Lemma) Let K/k be a finite extension and say $\widetilde{k}$ is another field isomorphic to k via $\theta\colon k \to \widetilde{k}$. Suppose Γ is another field related to $\widetilde{k}$, but otherwise arbitrary. Then, there exists a finite extension, $\widetilde{K}/\widetilde{k}$, with $\widetilde{K} \underset{\text{rel}}{\sim} \Gamma$ and an extension of θ to an isomorphism $\widetilde{\theta}\colon K \to \widetilde{K}$.*

$$\begin{array}{ccccc} K & \xrightarrow{\widetilde{\theta}} & \widetilde{K} & \underset{\text{rel}}{\sim} & \Gamma \\ {\scriptstyle\text{finite}}\uparrow & & \uparrow{\scriptstyle\text{finite}} & & \| \\ k & \xrightarrow[\theta]{} & \widetilde{k} & \underset{\text{rel}}{\sim} & \Gamma \end{array}$$

Proof. We proceed by induction on the number, n, of adjunctions needed to obtain K from k.

Case $n = 1$: $K = k(\alpha)$. Let $g(X) \in k[X]$ be the minimum k-polynomial for α. Write $\widetilde{g}(X) \in \widetilde{k}[X]$ for the image, $\theta(g)(X)$, of $g(X)$. Of course, $\widetilde{g}(X)$ is $\widetilde{k}$-irreducible. Now, there exists a field, W, with $W \supseteq \widetilde{k}$ and $W \supseteq \Gamma$. Thus, $\widetilde{g}(X) \in W[X]$; moreover, there exists an extension W'/W of W and some $\widetilde{\alpha} \in W'$, so that $\widetilde{g}(\widetilde{\alpha}) = 0$. It follows that $\widetilde{k}(\widetilde{\alpha}) \subseteq W'$ and $\Gamma \subseteq W \subseteq W'$, so $\widetilde{k}(\widetilde{\alpha}) \underset{\text{rel}}{\sim} \Gamma$. But we know by Proposition 4.6 that θ extends to an isomorphism $\widetilde{\theta}\colon k(\alpha) \to \widetilde{k}(\widetilde{\alpha})$. This proves case 1.

Induction step. Assume that the induction hypothesis holds for all $t \leq n-1$. We have $K = k(\alpha_1, \ldots, \alpha_n)$ and let $L = k(\alpha_1, \ldots, \alpha_{n-1})$. By the induction hypothesis, there is a finite extension, $\widetilde{L}$, and an isomorphism, $\theta'\colon L \to \widetilde{L}$, extending θ;

$$\begin{array}{ccccc} L(\alpha_n) = K & \xrightarrow{\widetilde{\theta}} & \widetilde{K} & \underset{\text{rel}}{\sim} & \Gamma \\ \uparrow & & \uparrow & & \| \\ L & \xrightarrow{\theta'} & \widetilde{L} & \underset{\text{rel}}{\sim} & \Gamma \\ \uparrow & & \uparrow & & \| \\ k & \xrightarrow[\theta]{} & \widetilde{k} & \underset{\text{rel}}{\sim} & \Gamma \end{array}$$

We complete the proof using the argument in case 1 (a single generator), as illustrated in the above diagram. □

Corollary 4.23 *If K/k is a finite extension and $k \underset{\text{rel}}{\sim} \Gamma$, then there is a k-isomorphism $K/k \longrightarrow \widetilde{K}/\widetilde{k}$ and $\widetilde{K} \underset{\text{rel}}{\sim} \Gamma$.*

Proof. This is the case $k = \widetilde{k}$; $\theta = \text{id}$. □

Definition 4.8 A field extension L/k is a *splitting field for the polynomial* $f(X) \in k[X]$ iff $L = k(\alpha_1, \ldots, \alpha_n)$ and $\alpha_1, \ldots, \alpha_n$ are all the roots of $f(X)$ in some larger field ($n = \deg(f)$).

Remarks:

(1) When we view $f(X) \in L[X]$, then $f(X)$ splits into linear factors

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$$

in $L[X]$, hence the name. Conversely, if M/k is a field extension and in $M[X]$, the polynomial $f(X)$ splits into linear factors, then M contains some splitting field for f. (Here, $f(X) \in k[X]$.)

(2) Suppose L/k and L'/k are two splitting fields for the same polynomial $f(X) \in k[X]$. Then $L = L'$ iff $L \underset{\text{rel}}{\sim} L'$ (L and L' are *identical*, not just isomorphic).

Proof. The implication ($\Rightarrow$) is obvious. Conversely, assume $L \underset{\text{rel}}{\sim} L'$. Say Ω is a common extension of L and L' in which $f(X)$ splits. In Ω, the polynomial f has just n roots, say $\beta_1, \ldots, \beta_n$. Yet, $L = k(\beta_1, \ldots, \beta_n)$ and $L' = k(\beta_1, \ldots, \beta_n)$, too. Therefore, $L = L'$.

(3) Suppose L/k is a splitting field for $f(X) \in k[X]$ and $k \cong \widetilde{k}$ *via* some isomorphism, θ. If $\widetilde{f}(X)$ is the image of $f(X)$ by θ, and if θ extends to an isomorphism $L \cong \widetilde{L}$ for some extension $\widetilde{L}/\widetilde{k}$, then $\widetilde{L}$ is a splitting field for $\widetilde{f}(X)$.

Proposition 4.24 *Say $f(X) \in k[X]$ and $\theta\colon k \to \widetilde{k}$ is an isomorphism. Write $\widetilde{f}(X)$ for the image of $f(X)$ by θ. Then, θ extends to an isomorphism from any splitting field of f to any splitting field of $\widetilde{f}$. In particular, any two splitting fields of $f(X)$ are k-isomorphic (case $k = \widetilde{k}$; $f = \widetilde{f}$).*

Proof. Apply the extension lemma to the case where K is any chosen splitting field for f and Γ is any chosen splitting field for $\widetilde{f}$. The extension lemma yields an extension $\widetilde{K}/\widetilde{k}$ and an extension $\widetilde{\theta}\colon K \to \widetilde{K}$ with $\widetilde{K} \underset{\text{rel}}{\sim} \Gamma$. By Remark (3), the field $\widetilde{K}$ is a splitting field for $\widetilde{f}$. By Remark (2), as $\widetilde{K}$ and Γ are both splitting fields and $\widetilde{K} \underset{\text{rel}}{\sim} \Gamma$, they are equal. □

Definition 4.9 An algebraic field extension, M/k, is *normal* iff for all irreducible k-polynomials, $g(X)$, whenever some root of g is in M, all the roots of g are in M.

Proposition 4.25 *Say M/k is a finite extension and write $M = k(\beta_1, \ldots, \beta_t)$. Then, the following are equivalent:*

(1) M/k is normal.

(2) M is the splitting field of a family, $\{g_\alpha\}_\alpha$, of k-polynomials (the family might be infinite).

(3) M is the splitting field of a single k-polynomial (not necessarily irreducible).

(4) M is identical to all its k-conjugates; here two fields are k-conjugate iff they are both related and k-isomorphic.

Proof. (1) $\Rightarrow$ (2). For each β_i, there is an irreducible k-polynomial, say g_i with $g_i(\beta_i) = 0$. By (1), all the other roots of g_i are in M. Therefore, M contains the splitting fields of each g_i. But, clearly, M is contained in the field generated by all these splitting fields. It follows that M is equal to the splitting field of the (finite) family of k-polynomials $g_1, \ldots, g_t$.

(2) $\Rightarrow$ (3). Say $\{g_\alpha\}$ is the family of k-polynomials for which M is the splitting field. (Note that we may assume that $\deg(g_\alpha) > 1$ for all g_α.) Pick a countable (at most) subset $\{g_1, g_2, \ldots, \}$ of our family. Then, M contains the splitting field of g_1, call it M_1. We have $M \supseteq M_1 \supseteq k$ and $[M\colon M_1] < [M\colon k]$. If $M \neq M_1$, then M contains the splitting field, M_2, of g_1 and g_2, where we may assume that the splitting field of g_2 is distinct from M_1. Thus, we have $M \supseteq M_2 \supseteq M_1 \supseteq k$. Since M is finite over k, the above process stops and we deduce that M is the splitting field of a finite subfamily $\{g_1, \ldots, g_t\}$. Then, take $g = \prod_{i=1}^t g_i$, and (3) holds.

(3) $\Rightarrow$ (4). If $\widetilde{M}$ is a k-conjugate of M, then

(a) $\widetilde{M}$ is a splitting field (k-isomorphic to M)

(b) $\widetilde{M} \underset{\text{rel}}{\sim} M$.

But, we know that (a) and (b) imply that $\widetilde{M} = M$.

(4) $\Rightarrow$ (1). Pick an irreducible k-polynomial, g, and $\alpha \in M$ with $g(\alpha) = 0$. Consider the extension lemma in the situation where $k = \widetilde{k}$ and $\Gamma = M$. Pick in an algebraic closure, $\overline{M}$, of M, any root β of g. We get the diagram

$$\begin{array}{ccccc}
M & \xrightarrow{\widetilde{\theta}} & \widetilde{M} & \underset{\text{rel}}{\sim} & M \\
\uparrow & & \uparrow & & \| \\
k(\alpha) & \xrightarrow{\theta} & \widetilde{k}(\beta) & \underset{\text{rel}}{\sim} & M \\
\uparrow & & \uparrow & & \| \\
k & = & k & \underset{\text{rel}}{\sim} & M.
\end{array}$$

By the extension lemma applied to the upper portion of the above diagram, there exists $\widetilde{M}$ with $\widetilde{M} \underset{\text{rel}}{\sim} M$ and an extension $\widetilde{\theta}\colon M \to \widetilde{M}$. But, $\widetilde{\theta} \restriction k = \theta \restriction k = \text{id}$, so $\widetilde{\theta}$ is a k-isomorphism and $\widetilde{M} \underset{\text{rel}}{\sim} M$. By (4), we get $\widetilde{M} = M$. Since $\beta \in \widetilde{M}$, we have $\beta \in M$. $\square$

Corollary 4.26 *Say $M \supseteq K \supseteq k$ and M is normal over k. Then, M is normal over K.*

Proof. Use (3), i.e., M is the splitting field of some $g \in k[X]$. Yet, $g \in K[X]$, and use (3) again. $\square$

M normal over K and K normal over k does *not* imply M normal over k.

Here is a counter-example to the transitivity of normality. Let $k = \mathbb{Q}$; $K = \mathbb{Q}(\sqrt{2})$; the extension K/k is normal. Let $\alpha = \sqrt{2}$ and $L = K(\sqrt{\alpha})$; again, L/K is normal of degree 2. Observe that L is the splitting field over K of $X^2 - \alpha \in K[X]$. But, $L/\mathbb{Q}$ is *not* normal. This is because the polynomial $X^4 - 2$ has a root, $\sqrt{\alpha}$, in L, yet $i\sqrt{\alpha}$ is *not* in L because $L \subseteq \mathbb{R}$.

M normal over k and $M \supseteq K \supseteq k$ does *not* imply K normal over k.

Corollary 4.27 *(SMA, I[2]) Say M is normal over k and g is any irreducible k-polynomial with a root $\alpha \in M$. Then, a n.a.s.c. that an element $\beta \in M$ be a root of g is that there exists σ, a k-automorphism of M (i.e., $\sigma \restriction k = \text{id}$) so that $\sigma(\alpha) = \beta$.*

Proof. ($\Leftarrow$). If α is a root and $g \in k[X]$, then

$$0 = \sigma(0) = \sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\beta).$$

So, β is a root.

[2]SMA = **s**ufficiently **m**any **a**utomorphisms.

($\Rightarrow$). Say $\beta \in M$ is a root, then there is a k-isomorphism $k(\alpha) \longrightarrow k(\beta)$. Now, $k(\beta) \underset{\text{rel}}{\sim} M$; so, in the extension lemma, take $\Gamma = M$:

$$\begin{array}{ccccc} M & \xrightarrow{\widetilde{\theta}} & \widetilde{M} & \underset{\text{rel}}{\sim} & M \\ \uparrow & & \uparrow & & \| \\ k(\alpha) & \xrightarrow{\theta} & \widetilde{k}(\beta) & \underset{\text{rel}}{\sim} & M \\ \uparrow & & \uparrow & & \| \\ k & = & k & \underset{\text{rel}}{\sim} & M. \end{array}$$

We get $\widetilde{\theta}\colon M \to \widetilde{M}$, a k-isomorphism and $M \underset{\text{rel}}{\sim} \widetilde{M}$. By (4), $M = \widetilde{M}$. So, $\widetilde{\theta} = \sigma$ is our required automorphism (it takes α to β). $\square$

Corollary 4.28 *(SMA, II) Let M be normal over k and say K, K' are subextensions of the layer M/k (i.e, $M \supseteq K \supseteq k$ and $M \supseteq K' \supseteq k$). If $\theta\colon K \to K'$ is a k-isomorphism, then there is a k-automorphism, σ, of M so that $\sigma \restriction K = \theta$.*

Proof. Apply the extension lemma with $\Gamma = M$ to the situation

$$\begin{array}{ccccc} M & \xrightarrow{\widetilde{\theta}} & \widetilde{M} & \underset{\text{rel}}{\sim} & M \\ \uparrow & & \uparrow & & \| \\ K & \xrightarrow{\theta} & K' & \underset{\text{rel}}{\sim} & M. \end{array}$$

There exist $\widetilde{\theta}$ and $\widetilde{M}$ with $\widetilde{\theta}$ a k-isomorphism and $M \underset{\text{rel}}{\sim} \widetilde{M}$. By (4), $M = \widetilde{M}$. Therefore, $\sigma = \widetilde{\theta}$ is our automorphism.

Corollary 4.29 *Say K/k is a finite extension of degree $[K\colon k] = n$, then there exists $M \supseteq K$ with*

(1) M is normal over k and

(2) Whenever W is normal over k, $W \supseteq K$ and $W \underset{\text{rel}}{\sim} M$, then automatically $W \supseteq M$.

(3) $[M\colon k] \leq n!$.

The field, M, is called a normal closure of K/k.

Proof. (DX).

4.5 The Theorems of Dedekind and Artin; Galois Groups & the Fundamental Theorem

Recollect that a K-representation of a group, G, is just a $K[G]$-module. So, a K-representation of a group, G, is just a K-vector space plus a (linear) G-action on it (by K-automorphisms); that is, a homomorphism $G \longrightarrow \mathrm{Aut}(V)$. If $\dim_K V < \infty$, we have a finite dimensional representation. In this case, $\mathrm{Aut}(V) = \mathrm{GL}(V) \cong \mathrm{GL}_n(K)$, where $n = \dim_K(V)$ is the degree of the representation. Say $\rho\colon G \to \mathrm{GL}_n(K)$ is our representation. Then, $\chi_\rho(\sigma) = \mathrm{tr}(\rho(\sigma))$, the trace of $\rho(\sigma)$, is a function $G \longrightarrow K$ independent of the basis chosen, called the *character* of our representation. The case $n = 1$ is very important. In this case, the characters *are* the representations, $\chi_\rho = \rho$. Therefore, we have functions $\chi\colon G \to K^*$, with $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$. From now on, we use only one-dimensional characters.

Definition 4.10 Suppose $\{\chi_\alpha\}_\alpha$ is a given family of characters, $\chi_\alpha\colon G \to K^*$, of the group G. Call the family *independent* iff the relation

$$\sum_{j=1}^{n} a_j\chi_j(\sigma) = 0, \quad \textit{for all } \sigma \in G$$

implies $a_j = 0$, for $j = 1, \ldots, n$ (all applicable n).

Theorem 4.30 *(R. Dedekind, about 1890) If G is a group and $\{\chi_\alpha\}_\alpha$ is a family of mutually distinct characters of G (with values in K^*), then they are independent.*

Proof. We may assume our family is finite and we use induction on the number of elements, n, in this family. The case $n = 1$ holds trivially. Assume that the result holds for all $t \leq n-1$ characters. Say $\chi_1, \ldots, \chi_n$ are distinct characters of G and suppose

$$\sum_{j=1}^{n} a_j\chi_j(\sigma) = 0, \quad \text{for all } \sigma \in G. \tag{$*$}$$

The induction hypothesis implies that if the conclusion of the theorem is false, then $a_j \neq 0$, for all $j = 1, \ldots, n$. Since the χ_j are distinct, there is some $\alpha \neq 1$ with $\chi_1(\alpha) \neq \chi_n(\alpha)$. Divide $(*)$ by $a_n \neq 0$, to obtain

$$\sum_{j=1}^{n-1} b_j\chi_j(\sigma) + \chi_n(\sigma) = 0, \quad \text{for all } \sigma \in G. \tag{$**$}$$

Consider the group element $\alpha\sigma$, then $(**)$ is true for it and we have

$$\sum_{j=1}^{n-1} b_j\chi_j(\alpha)\chi_j(\sigma) + \chi_n(\alpha)\chi_n(\sigma) = 0, \quad \text{for all } \sigma \in G.$$

If we multiply by $\chi_n(\alpha)^{-1}$, we get

$$\sum_{j=1}^{n-1} (b_j\chi_n(\alpha)^{-1}\chi_j(\alpha))\chi_j(\sigma) + \chi_n(\sigma) = 0, \quad \text{for all } \sigma \in G. \tag{$\dagger$}$$

If we subtract $(\dagger)$ from $(**)$, we get

$$\sum_{j=1}^{n-1} b_j(1 - \chi_n(\alpha)^{-1}\chi_j(\alpha))\chi_j(\sigma) = 0, \quad \text{for all } \sigma \in G.$$

By the induction hypothesis, $b_j(1 - \chi_n(\alpha)^{-1}\chi_j(\alpha)) = 0$, for $j = 1, \ldots, n-1$. If we take $j = 1$ and we remember that $b_1 = a_1/a_n \neq 0$, we get

$$1 - \chi_n(\alpha)^{-1}\chi_1(\alpha) = 0,$$

i.e., $\chi_n(\alpha) = \chi_1(\alpha)$, a contradiction. □

Corollary 4.31 *Say $\{\chi_\alpha\}_\alpha$ is a family of mutually distinct isomorphisms of a field L with another, $\widetilde{L}$. Then, the χ_α are independent.*

Proof. Take $G = L^*$ and $K = \widetilde{L}$ in Dedekind's theorem. □

Definition 4.11 If $\{\chi_\alpha\}_\alpha$ is a family of isomorphisms $K \longrightarrow \widetilde{K}$, then set

$$\mathrm{Fix}(\{\chi_\alpha\}) = \{\xi \in K \mid (\forall \alpha, \beta)(\chi_\alpha(\xi) = \chi_\beta(\xi))\}.$$

Observe that $\mathrm{Fix}(\{\chi_\alpha\})$ is always a subfield of K, so we call it the *fixed field* of $\{\chi_\alpha\}_\alpha$.

Note that $\mathrm{Fix}(\{\chi_\alpha\})$ contains the prime field of K.

Theorem 4.32 *(E. Artin, 1940) If $\{\chi_\alpha\}_\alpha$ is a family of pairwise distinct isomorphisms $K \longrightarrow \widetilde{K}$ and if $k = \mathrm{Fix}(\{\chi_\alpha\})$, then*

(1) $[K\colon k] \geq \min(\aleph_0, \#(\{\chi_\alpha\}))$.

(2) Say $\{\chi_\alpha\}$ forms a group under composition (so, $K = \widetilde{K}$ and all χ_α's are automorphisms of K), then if $\#(\{\chi_\alpha\}) = n < \infty$, we have $[K\colon k] = n$ and if $n = \infty$ then $[K\colon k] = \infty$.

Proof. (1) First, we consider the case where we have a finite set, $\{\chi_1, \ldots, \chi_n\}$, of isomorphisms $K \longrightarrow \widetilde{K}$. Let $k = \mathrm{Fix}(\{\chi_j\}_{j=1}^n)$ and assume that $[K\colon k] < n$. Then, there exists a basis, $\omega_1, \ldots, \omega_r$, of K/k and $r < n$. Consider the r equations in n unknowns (y_j's)

$$\sum_{j=1}^{n} y_j \chi_j(\omega_i) = 0, \quad 1 \leq i \leq r.$$

As $r < n$, this system has a nontrivial solution, call it $(\alpha_1, \ldots, \alpha_n)$ (with $\alpha_i \in \widetilde{K}$). So, we have

$$\sum_{j=1}^{n} \alpha_j \chi_j(\omega_i) = 0, \quad 1 \leq i \leq r.$$

Pick any $\xi \in K$, as the ω_i's form a basis, we can write $\xi = \sum_{i=1}^r a_i\omega_i$, for some (unique) $a_i \in k$. We have

$$\sum_{j=1}^{n} \alpha_j \chi_j(\xi) = \sum_{j=1}^{n} \alpha_j \chi_j\Big(\sum_{i=1}^{r} a_i\omega_i\Big) = \sum_{j=1}^{n}\sum_{i=1}^{r} \alpha_j \chi_j(a_i)\chi_j(\omega_i).$$

But, $\chi_j(a_i) = \chi_l(a_i)$, for all j, l, as $a_i \in k$ and $k = \mathrm{Fix}(\{\chi_j\})$. Write $b_i = \chi_j(a_i)$ (independent of j). So, we have

$$\sum_{j=1}^{n} \alpha_j \chi_j(\xi) = \sum_{i=1}^{r} b_i\Big(\sum_{j=1}^{n} \alpha_j \chi_j(\omega_i)\Big).$$

But, $\sum_{j=1}^n \alpha_j\chi_j(\omega_i) = 0$, by the choice of $\alpha_1, \ldots, \alpha_n$, so

$$\sum_{j=1}^{n} \alpha_j \chi_j(\xi) = 0, \quad \text{for all } \xi.$$

This contradicts Dedekind's theorem and thus, $[K\colon k] \geq n$.

Now, consider the case where $\#(\{\chi_\alpha\})$ is infinite. If $[K\colon k]$ were finite, then pick any $n > [K\colon k]$ and repeat the above argument with the subset $\{\chi_1, \ldots, \chi_n\}$. We deduce that $[K\colon k]$ must be infinite.

(2) Now, suppose $\{\chi_1, \ldots, \chi_n\}$ forms a group under composition (i.e., they are a group of automorphisms of K). Then, one of the χ_j's is the identity, say $\chi_1 = \mathrm{id}$. It follows that for every $a \in k$, we have $\chi_j(a) = \chi_1(a) = a$, so

$$k = \mathrm{Fix}(\{\chi_j\}) = \{a \in K \mid \chi_j(a) = a, \quad j = 1, \ldots, n\}.$$

By part (1), we know $[K\colon k] \geq n$; so, assume $[K\colon k] > n$. In this case, there exist $r > n$ elements, $\omega_1, \ldots, \omega_r \in K$, linearly independent over k. Consider the n equations in r unknowns (x_i's)

$$\sum_{i=1}^{r} x_i \chi_j(\omega_i) = 0, \quad j = 1, \ldots, n.$$

Again, there is a nontrivial solution, say $a_1, \ldots, a_r$, with $a_j \in K$. So, we have

$$\sum_{i=1}^{r} a_i \chi_j(\omega_i) = 0, \quad j = 1, \ldots, n. \tag{$\dagger$}$$

Note that for any nontrivial solution, the a_i's can't all be in k. If they were, then ($\dagger$) with $j = 1$ gives $\sum_{i=1}^{r} a_i \omega_i = 0$, contradicting the linear independence of the ω_i's.

Pick a solution containing a minimal number of nonzero a_i's, say $a_1, \ldots, a_s \neq 0$ and $a_{s+1} = \cdots = a_r = 0$. If we divide ($\dagger$) by a_s, we get

$$\sum_{i=1}^{s-1} b_i \chi_j(\omega_i) + \chi_j(\omega_s) = 0, \quad j = 1, \ldots, n. \tag{$\ddagger$}$$

By the remark above, there is some i, with $1 \leq i \leq s-1$, so that $b_i \notin k$. By relabelling, we may assume that $b_1 \notin k$. As $b_1 \notin k$, there is some ρ ($1 \leq \rho \leq n$) with $\chi_\rho(b_1) \neq b_1$. Apply χ_ρ to ($\ddagger$); we get

$$\sum_{i=1}^{s-1} \chi_\rho(b_i)(\chi_\rho \circ \chi_j)(\omega_i) + (\chi_\rho \circ \chi_j)(\omega_s) = 0, \quad j = 1, \ldots, n.$$

As χ_j ranges over $\{\chi_1, \ldots, \chi_n\}$, so does $\chi_\rho \circ \chi_j$; consequently, we have

$$\sum_{i=1}^{s-1} \chi_\rho(b_i) \chi_\xi(\omega_i) + \chi_\xi(\omega_s) = 0, \quad \xi = 1, \ldots, n. \tag{$*$}$$

If we subtract ($*$) from ($\ddagger$), we obtain

$$\sum_{i=1}^{s-1} (b_i - \chi_\rho(b_i)) \chi_\xi(\omega_i) = 0, \quad \xi = 1, \ldots, n.$$

But, we know that $b_1 \neq \chi_\rho(b_1)$. For this ρ, not all the coefficients are zero, so we get a solution with strictly fewer nonzero components, a contradiction to the minimality of $(a_1, \ldots, a_s)$. $\square$

Definition 4.12 If Ω is a finite, normal extension of k, the *Galois group* of Ω/k, denoted $\mathcal{G}(\Omega/k)$, is the group of all k-automorphisms of Ω (i.e., the automorphisms, σ, of Ω so that $\sigma \restriction k = \mathrm{id}$). Say $f \in k[X]$ and let Ω be a splitting field for $f(X)$ over k. The *Galois group of the polynomial, $f(X)$,* over k, denoted $\mathcal{G}_k(f)$, is just $\mathcal{G}(\Omega/k)$.

Lemma 4.33 *Suppose Ω is finite, normal over k and $\mathcal{G} = \mathcal{G}(\Omega/k)$ is its Galois group. Then, a n.a.s.c. that $\xi \in \Omega$ lie in $\mathrm{Fix}(\mathcal{G})$ is that ξ be purely inseparable over k.*

Proof. If ξ is purely inseparable over k, then there is some $s \geq 0$ so that $\xi^{p^s} \in k$. Then, for every $\sigma \in \mathcal{G}$, we have $\sigma\big(\xi^{p^s}\big) = \xi^{p^s}$. But, $\sigma\big(\xi^{p^s}\big) = (\sigma(\xi))^{p^s}$, so $(\sigma(\xi))^{p^s} = \xi^{p^s}$; since $\mathrm{char}(k) = p$, it follows that $(\sigma(\xi) - \xi)^{p^s} = 0$. Therefore, $\sigma(\xi) - \xi = 0$, i.e., ξ is fixed by σ and $\xi \in \mathrm{Fix}(\mathcal{G})$. Conversely, assume that $\xi \in \mathrm{Fix}(\mathcal{G})$. First, pick an element $\alpha \in \Omega$, with α separable over k and $\alpha \notin k$, if such an element exists. Then, α is a simple root of some irreducible k-polynomial g. But, Ω is normal, so all the roots of g lie in Ω and as $\alpha \notin k$, we have $\deg(g) > 1$. Consequently, there is another root, $\beta \in \Omega$, of g with $\beta \neq \alpha$ and by SMA, I, there exists $\sigma \in \mathcal{G}$ so that $\sigma(\alpha) = \beta$. Now, consider our $\xi \in \mathrm{Fix}(\mathcal{G})$. As $\xi \in \Omega$, there is some power, ξ^{p^r}, of ξ that is separable over k. Since ξ is fixed by all $\sigma \in \mathcal{G}$, so is ξ^{p^r}. If ξ^{p^r} were not in k, then ξ^{p^r} could play the role of α above, so it could be moved to some $\beta \neq \alpha$, a contradiction. This implies that $\xi^{p^r} \in k$, i.e., ξ is purely inseparable over k. □

Nomenclature & Notation.

Say Ω/k is a normal (not necessarily finite) extension. Pick an extension, K, in the layer Ω/k, i.e, $k \subseteq K \subseteq \Omega$. Define

$$K^{(*)} = \left\{\xi \in \Omega \mid \xi^{p^r} \in K, \quad \text{for some } r \geq 0\right\}.$$

(Obviously, $p = \mathrm{char}(k)$.) Note that $K^{(*)} = \Omega \cap K^{p^{-\infty}}$ in some algebraic closure (where $K^{p^{-\infty}}$ is defined as $\{\xi \in \overline{K} \mid (\exists r \geq 0)(\xi^{p^r} \in K)\}$). Also define

$$K_{(*)} = \{\xi \in K \mid \xi \quad \text{is separable over } k\}.$$

Note: $K^{(*)}$ and $K_{(*)}$ are subfields of Ω/k and we have $K_{(*)} \subseteq K \subseteq K^{(*)} \subseteq \Omega$.

We say that K *is Galois equivalent to* K' (where $k \subseteq K \subseteq \Omega$ and $k \subseteq K' \subseteq \Omega$) iff $K^{(*)} = K'^{(*)}$; write K gal K'. This equivalence relation fibers the subextensions of Ω/k into Galois equivalence classes.

Corollary 4.34 *If Ω/k is finite, normal, then $\mathrm{Fix}(\mathcal{G}(\Omega/k)) = k^{(*)}$. In particular, if $k \subseteq L \subseteq \Omega$, then $\mathrm{Fix}(\mathcal{G}(\Omega/L)) = L^{(*)}$.*

Corollary 4.35 *If Ω/k is finite, normal, then $\#(\mathcal{G}(\Omega/k))$ divides $[\Omega\colon k]$; in particular, $\#(\mathcal{G}(\Omega/k)) \leq [\Omega\colon k] < \infty$.*

Proof. By Artin's theorem (Theorem 4.32) $\#(\mathcal{G}(\Omega/k)) = [\Omega\colon \mathrm{Fix}(\mathcal{G}(\Omega/k))]$. By Lemma 4.33, we have $\mathrm{Fix}(\mathcal{G}(\Omega/k)) = k^{(*)}$. Therefore, $\#(\mathcal{G}(\Omega/k)) = [\Omega\colon k^{(*)}]$ which divides $[\Omega\colon k]$. □

Corollary 4.36 *If Ω/k is finite, normal and k is perfect, e.g.* $\mathrm{char}(k) = 0$, *then $\#(\mathcal{G}(\Omega/k)) = [\Omega\colon k]$.*

Corollary 4.37 *Say f is a separable, irreducible k-polynomial with degree* $\deg(f) = n$. *Then, there is an injection $\mathcal{G}_k(f) \hookrightarrow \mathfrak{S}_n$ (where $\mathfrak{S}_n$ denotes the symmetric group on n elements) and this injection is unique up to inner automorphisms in $\mathfrak{S}_n$. In particular, $\#(\mathcal{G}_k(f)) \mid n!$.*

Proof. Write $\alpha_1, \ldots, \alpha_n$ for all the roots of f (they are all distinct) in some order. Given $\sigma \in \mathcal{G}_k(f)$, the element $\sigma(\alpha_i)$ is some other root of f, call it $\alpha_{p_\sigma(i)}$. Then, p_σ is a permutation of the n roots, i.e., $p_\sigma \in \mathfrak{S}_n$. Clearly, the map $\sigma \mapsto p_\sigma$ is a homomorphism $\mathcal{G}_k(f) \longrightarrow \mathfrak{S}_n$. If $p_\sigma = \mathrm{id}$, then $\sigma(\alpha_i) = \alpha_i$ for all i, so $\sigma \restriction \Omega = \mathrm{id}$, as Ω, the splitting field of f, is generated over k by the α_i's. So, $\sigma = id$ in $\mathcal{G}_k(f) = \mathcal{G}(\Omega/k)$, and the our map $\mathcal{G}_k(f) \longrightarrow \mathfrak{S}_n$ is an injection. We can reorder (relabel) the $\alpha_1, \ldots, \alpha_n$; to do so introduces an inner automorphism of $\mathfrak{S}_n$. □

Remarks: (On Galois equivalence)

(1) *If $K \subseteq K'$, then $K^{(*)} \subseteq K'^{(*)}$.* Indeed, if $\xi \in K^{(*)}$, then $\xi^{p^r} \in K \subseteq K'$ (for some $r \geq 0$), so $\xi \in K'^{(*)}$.

(2) *For all K in the layer Ω/k (of course, Ω/k is a finite normal extension), we have K gal $K^{(*)}$. Hence, the Galois equivalence class of any field possesses a unique least upper bound, namely $K^{(*)}$ for any K in the class.* For, $K \subseteq K^{(*)}$, so $K^{(*)} \subseteq (K^{(*)})^{(*)}$. Also, if $\xi \in (K^{(*)})^{(*)}$, then $\xi^{p^r} \in K^{(*)}$, for some r; but then, $(\xi^{p^r})^{p^s} \in K$, for some s, i.e., $\xi^{p^{r+s}} \in K$, which means that $\xi \in K^{(*)}$. Consequently, $(K^{(*)})^{(*)} \subseteq K^{(*)}$ and so $(K^{(*)})^{(*)} = K^{(*)}$, i.e. K gal $K^{(*)}$. If K gal L then $K^{(*)} = L^{(*)}$; $K \subseteq K^{(*)}$ and $L \subseteq L^{(*)}$, so $K^{(*)} = L^{(*)}$ is indeed the least upper bound of the equivalence class of K and L.

(3) *If K belongs to the layer Ω/k (where Ω/k is normal), then $K_{(*)}$ gal K and $K_{(*)}$ is the unique greatest lower bound for the Galois equivalence class of K.*

Proof. If we prove that $(K_{(*)})^{(*)} = K^{(*)}$ and $(K^{(*)})_{(*)} = K_{(*)}$, we are done. The first equation will prove that $K_{(*)}$ gal K. As $K_{(*)} \subseteq K$, we get $(K_{(*)})^{(*)} \subseteq K^{(*)}$. Pick $\xi \in K^{(*)}$, then $\xi^{p^r} \in K$, for some r and $(\xi^{p^r})^{p^s} = \xi^{p^{r+s}} \in K_{(*)}$, for some s, so $\xi \in (K_{(*)})^{(*)}$; hence, $(K_{(*)})^{(*)} = K^{(*)}$. Now, pick $\xi \in K_{(*)}$, then $\xi \in K^{(*)}$ (as $K_{(*)} \subseteq K \subseteq K^{(*)}$) and since ξ is separable over k, we have $\xi \in (K^{(*)})_{(*)}$. Conversely, if $\xi \in (K^{(*)})_{(*)}$, then $\xi \in K^{(*)}$, which means that ξ is inpurely separable over K. Yet, ξ is separable over k, so ξ is separable over K. As ξ is purely inseparable over K and separable over K, we get $\xi \in K$; moreover, as ξ is separable over k, we get $\xi \in K_{(*)}$.

(4) *We have K gal L iff $K_{(*)} = L_{(*)}$, hence in each Galois equivalence class, there is a unique greatest lower bound, it is the common $K_{(*)}$.* If K gal L, then $K^{(*)} = L^{(*)}$, so

$$K_{(*)} = (K^{(*)})_{(*)} = (L^{(*)})_{(*)} = L_{(*)},$$

by (3). Conversely, if $K_{(*)} = L_{(*)}$, then

$$K^{(*)} = (K_{(*)})^{(*)} = (L_{(*)})^{(*)} = L^{(*)},$$

again, by (3), i.e., K gal L.

(5) *Suppose K gal L and $K, L \subseteq \Omega/k$, Then, $\mathcal{G}(\Omega/K) = \mathcal{G}(\Omega/L)$, hence the maps*

$$\mathcal{G}(\Omega/L^{(*)}) \hookrightarrow \mathcal{G}(\Omega/L) \hookrightarrow \mathcal{G}(\Omega/L_{(*)})$$

are equalities. All we need show is $\mathcal{G}(\Omega/L) = \mathcal{G}(\Omega/L^{(*)})$. We already know $\mathcal{G}(\Omega/L^{(*)}) \subseteq \mathcal{G}(\Omega/L)$, as $L \subseteq L^{(*)}$. Say $\sigma \in \mathcal{G}(\Omega/L)$ and pick any $\xi \in L^{(*)}$. Then, $\xi^{p^r} \in L$, for some $r \geq 0$. Consequently, $\sigma(\xi^{p^r}) = \xi^{p^r}$, as $\sigma \restriction L = \mathrm{id}$. As σ is an automorphism, we get $(\sigma(\xi))^{p^r} = \xi^{p^r}$, i.e., $(\sigma(\xi) - \xi)^{p^r} = 0$, and so, $\sigma(\xi) = \xi$. As ξ is arbitrary in $L^{(*)}$, we have $\sigma \restriction L^{(*)} = \mathrm{id}$; since σ is arbitrary, the proof is complete.

Theorem 4.38 *(Fundamental Theorem of Galois Theory) Suppose Ω/k is a finite, normal extension. Write $\mathcal{G}$ for $\mathcal{G}(\Omega/k)$ and write $[K]$ for the Galois class of $K \subseteq \Omega/k$. Then, the maps*

$$\mathcal{H} \mapsto [\mathrm{Fix}(\mathcal{H})] \quad \textit{and} \quad [L] \mapsto \mathcal{G}(\Omega/L)$$

establish a one-to-one order-reversing correspondence between all subgroups of $\mathcal{G}$ and all the Galois classes of subextensions $L/k \subseteq \Omega/k$. Here, $[K] \subseteq [L]$ means $K^{(*)} \subseteq L^{(*)}$ as fields. In this correspondence, $\mathcal{G}(\Omega/L) \lhd \mathcal{G}$ iff $L^{(*)}$ is a normal extension of k iff $L_{(*)}$ is a normal extension of k. When the latter is the case, then there is a canonical exact sequence

$$0 \longrightarrow \mathcal{G}(\Omega/L) \longrightarrow \mathcal{G}(\Omega/k) \longrightarrow \mathcal{G}(L^{(*)}/k) \longrightarrow 0.$$

Claim 1. If $L = \mathrm{Fix}(\mathcal{H})$, then $L = L^{(*)}$.

Pick $\xi \in L^{(*)}$, so $\xi^{p^r} \in L$, for some $r \geq 0$. Then, for all $\sigma \in \mathcal{H}$, we have $\sigma\big(\xi^{p^r}\big) = \xi^{p^r}$, and by a standard argument, $\xi \in \mathrm{Fix}(\mathcal{H}) = L$. Consequently, $L^{(*)} \subseteq L$, yet $L \subseteq L^{(*)}$, so $L = L^{(*)}$.

Proof of Theorem 4.38. Now say $\mathcal{H} \subseteq \widetilde{\mathcal{H}}$ and look at $\mathrm{Fix}(\widetilde{\mathcal{H}})$. If $\xi \in \mathrm{Fix}(\widetilde{\mathcal{H}})$, then for every $\tau \in \widetilde{\mathcal{H}}$, we have $\tau(\xi) = \xi$ and so, for every $\sigma \in \mathcal{H}$, we have $\sigma(\xi) = \xi$, i.e., $\xi \in \mathrm{Fix}(\mathcal{H})$. Consequently, $\mathrm{Fix}(\widetilde{\mathcal{H}}) \subseteq \mathrm{Fix}(\mathcal{H})$ and so, $[\mathrm{Fix}(\widetilde{\mathcal{H}})] \subseteq [\mathrm{Fix}(\mathcal{H})]$, by Claim (1). Now, if $[L] \subseteq [\widetilde{L}]$, then $L^{(*)} \subseteq \widetilde{L}^{(*)}$. If $\sigma \in \mathcal{G}(\Omega/\widetilde{L})$, then $\sigma \in \mathcal{G}(\Omega/\widetilde{L}^{(*)})$ (by Remark (5), above); so, $\sigma \in \mathcal{G}(\Omega/L^{(*)}) = \mathcal{G}(\Omega/L)$ (again, by Remark (5)). Thus, $\mathcal{G}(\Omega/\widetilde{L}) \subseteq \mathcal{G}(\Omega/L)$.

Given $\mathcal{H} \subseteq \widetilde{\mathcal{H}}$, say we know $\mathrm{Fix}(\mathcal{H}) = \mathrm{Fix}(\widetilde{\mathcal{H}})$. By Artin's theorem, we have

$$\#(\mathcal{H}) = [\Omega\colon \mathrm{Fix}(\mathcal{H})] = [\Omega\colon \mathrm{Fix}(\widetilde{\mathcal{H}})] = \#(\widetilde{\mathcal{H}}).$$

As $\mathcal{H} \subseteq \widetilde{\mathcal{H}}$ and $\#(\mathcal{H}) = \#(\widetilde{\mathcal{H}})$, we get $\mathcal{H} = \widetilde{\mathcal{H}}$.

Choose a subgroup, $\mathcal{H}$, of $\mathcal{G}$ and let $L = \mathrm{Fix}(\mathcal{H})$; write $\widetilde{\mathcal{H}}$ for $\mathcal{G}(\Omega/L) = \mathcal{G}(\Omega/\mathrm{Fix}(\mathcal{H}))$. If $\sigma \in \mathcal{H}$, then σ fixes L, so $\sigma \in \widetilde{\mathcal{H}}$ and $\mathcal{H} \subseteq \widetilde{\mathcal{H}}$. But, $\mathrm{Fix}(\widetilde{\mathcal{H}}) = \mathrm{Fix}(\mathcal{G}(\Omega/L)) = L^{(*)}$, by Corollary 4.34. Thus, $\mathrm{Fix}(\widetilde{\mathcal{H}}) = (\mathrm{Fix}(\mathcal{H}))^{(*)}$. Claim 1 implies that $(\mathrm{Fix}(\mathcal{H}))^{(*)} = \mathrm{Fix}(\mathcal{H})$, so $\mathrm{Fix}(\widetilde{\mathcal{H}}) = \mathrm{Fix}(\mathcal{H})$ and, by the above, we get $\mathcal{H} = \widetilde{\mathcal{H}}$. Therefore, $\mathcal{H} = \mathcal{G}(\Omega/\mathrm{Fix}(\mathcal{H}))$.

Consider L, make $\mathcal{G}(\Omega/L)$ and form $\mathrm{Fix}(\mathcal{G}(\Omega/L))$. By Corollary 4.34, we have $\mathrm{Fix}(\mathcal{G}(\Omega/L)) = L^{(*)}$ and L gal $L^{(*)}$, so $[L] = [\mathrm{Fix}(\mathcal{G}(\Omega/L))]$.

Having proved all the statements about the order inverting correspondence, we see that only normality statements remain.

Claim 2. If $L \subseteq \Omega/k$, then L is normal over k iff for every $\sigma \in \mathcal{G}(\Omega/k)$, we have $\sigma(L) = L$.

($\Rightarrow$). For every $\sigma \in \mathcal{G}(\Omega/k)$, the field $\sigma(L)$ is k-conjugate to L. As L is normal over k, we find $\sigma(L) = L$.

($\Leftarrow$). Assume $\sigma(L) = L$, for every $\sigma \in \mathcal{G}(\Omega/k)$. Let g be any irreducible k-polynomial and assume that $\alpha \in L$ is a root of g. But, $\alpha \in \Omega$ and Ω is normal; consequently, *all* the roots of g lie in Ω. Say $\beta \in \Omega$ is any other root of g. By SMA, I, there is some $\sigma \in \mathcal{G}$ so that $\sigma(\alpha) = \beta$. So, $\beta \in \sigma(L)$, and as $\sigma(L) = L$, we get $\beta \in L$. Thus, L contains all the roots of g which means that L is normal over k.

Assume $\mathcal{G}(\Omega/L) \lhd \mathcal{G}$. Look at $L^{(*)}$ and choose any $\sigma \in \mathcal{G}$ and any $\eta \in \sigma(L^{(*)})$. Then, $\sigma^{-1}(\eta) \in L^{(*)}$ and for all $\tau \in \mathcal{G}(\Omega/L) = \mathcal{G}(\Omega/L^{(*)})$, we have

$$(\sigma\tau\sigma^{-1})(\eta) = \sigma(\tau(\sigma^{-1}(\eta))) = (\sigma\sigma^{-1})(\eta) = \eta,$$

because $\sigma^{-1}(\eta) \in L^{(*)}$. Thus, $(\sigma\mathcal{G}(\Omega/L)\sigma^{-1})(\eta) = \eta$, and as $\mathcal{G}(\Omega/L) \lhd \mathcal{G}$, we get $\mathcal{G}(\Omega/L)(\eta) = \eta$, so $\eta \in \mathrm{Fix}(\mathcal{G}(\Omega/L)) = L^{(*)}$, as we know. In summary, if $\eta \in \sigma(L^{(*)})$, then $\eta \in L^{(*)}$, i.e., $\sigma(L^{(*)}) \subseteq L^{(*)}$. If we apply this to σ^{-1}, we get $\sigma^{-1}(L^{(*)}) \subseteq L^{(*)}$, i.e. $L^{(*)} \subseteq \sigma(L^{(*)})$. Therefore, $L^{(*)} = \sigma(L^{(*)})$ and by Claim 2, the extension $L^{(*)}/k$ is normal.

Now, say $L^{(*)}$ is normal over k. Then, we know $\sigma(L^{(*)}) = L^{(*)}$, for all $\sigma \in \mathcal{G}(\Omega/k)$. For any $\xi \in L^{(*)}$ and any $\tau \in \mathcal{G}(\Omega/L)$, we have

$$(\sigma\tau\sigma^{-1})(\xi) = \sigma(\tau(\sigma^{-1}(\xi))) = (\sigma\sigma^{-1})(\xi) = \xi,$$

because $\sigma^{-1}(\xi) \in \sigma^{-1}(L^{(*)}) = L^{(*)}$, by hypothesis. So, $\sigma\tau\sigma^{-1} \in \mathcal{G}(\Omega/L^{(*)}) = \mathcal{G}(\Omega/L)$ and thus, $\mathcal{G}(\Omega/L) \lhd \mathcal{G}$.

Suppose $L^{(*)}$ is normal. We have a map $\mathcal{G}(\Omega/k) \longrightarrow \mathcal{G}(L^{(*)}/k)$ *via* $\sigma \mapsto \sigma \restriction L^{(*)}$ ($\sigma \restriction L^{(*)} \in \mathcal{G}(L^{(*)}/k)$, by normality). This map is onto because, given any $\sigma \in \mathcal{G}(L^{(*)}/k)$, we have the diagram

$$\begin{array}{ccc} \Omega & \xrightarrow{\widetilde{\sigma}} & \Omega \\ \uparrow & & \uparrow \\ L^{(*)} & \xrightarrow{\sigma} & L^{(*)} \\ \uparrow & & \uparrow \\ k & = & k, \end{array}$$

and by SMA, II, the automorphism σ lifts to an automorphism, $\widetilde{\sigma}$, of Ω. The kernel of our map is clearly $\mathcal{G}(\Omega/L)$.

Lastly, we need to show that $L^{(*)}$ is normal iff $L_{(*)}$ is normal. Say $L^{(*)}$ is normal and $\sigma \in \mathcal{G}$. If $\xi \in L_{(*)}$, then $\xi \in L^{(*)}$ and $\sigma(\xi) \in L^{(*)}$ (as $L^{(*)}$ is normal). But, $\sigma(\xi)$ is separable over k as ξ is. It follows that $\sigma(\xi) \in (L^{(*)})_{(*)} = L_{(*)}$ and so, $\sigma(L_{(*)}) \subseteq L_{(*)}$. By the usual argument, $\sigma(L_{(*)}) = L_{(*)}$ and $L_{(*)}$ is normal. If $L_{(*)}$ is normal and $\xi \in L^{(*)}$, then $\xi^{p^r} \in L_{(*)}$, for some $r \geq 0$. It follows that $\sigma\big(\xi^{p^r}\big) \in \sigma(L_{(*)}) = L_{(*)}$, so $(\sigma(\xi))^{p^r} \in L_{(*)}$, i.e., $\sigma(\xi) \in (L_{(*)})^{(*)} = L^{(*)}$; thus, $\sigma(L^{(*)}) \subseteq L^{(*)}$ and, by the usual argument, we conclude that $L^{(*)}$ is normal. $\square$

Proposition 4.39 *Suppose Ω is normal over k and $L/k \subseteq \Omega/k$. Then $L = L^{(*)}$ iff Ω is separable over L.*

Proof. ($\Rightarrow$). Say Ω is separable over L, then as $L^{(*)} \subseteq \Omega$, we find $L^{(*)}$ is separable over L. Yet, $L^{(*)}$ is purely inseparable over L. It follows that $L = L^{(*)}$.

($\Leftarrow$). We must prove that Ω is separable over $L^{(*)}$. Pick $\alpha \in \Omega$ and consider $\mathcal{G}(\Omega/L^{(*)})$. Choose $\sigma_1, \ldots, \sigma_n \in \mathcal{G}(\Omega/L^{(*)})$ so that

(1) $\sigma_1 = \mathrm{id}$ and $\alpha = \sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ are mutually distinct,

(2) n is maximal, i.e., no further $\sigma \in \mathcal{G}(\Omega/L^{(*)})$ can be added while preserving (1).

Consider $g(X) = \prod_{i=1}^{n}(X - \sigma_j(\alpha))$. If $\sigma \in \mathcal{G}(\Omega/L^{(*)})$, the elements $\sigma\sigma_1(\alpha), \ldots, \sigma\sigma_n(\alpha)$ are a permutation of $\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$, so $\sigma g(X) = g(X)$. This implies that the coefficients of $g(X)$ belong to $\mathrm{Fix}(\mathcal{G}(\Omega/L^{(*)})) = L^{(*)}$. Thus, $g(X) \in L^{(*)}[X]$, but the roots of $g(X)$ are distinct and α is among them. Therefore, α is separable over $L^{(*)}$. $\square$

Corollary 4.40 *Assume Ω/k is a finite normal extension. Then, the following are equivalent:*

(1) Ω is separable over k.

(2) $k^{(*)} = k$.

(3) For all subextensions, L, of Ω/k, we have $L^{(*)} = L_{(*)}$.

(3a) For all subextensions, L, of Ω/k, the equivalence class $[L]$ has but one element.

(4) Same as (3) but for some extension $L/k \subseteq \Omega/k$.

(4a) Same as (3a) but for some extension $L/k \subseteq \Omega/k$.

(5) $\Omega = \Omega_{(*)}$.

Proof. First, observe that the equivalences (3) $\Longleftrightarrow$ (3a) and (4) $\Longleftrightarrow$ (4a) are obvious.

(1) $\Rightarrow$ (2). This is Proposition 4.39 when $L = k$.

(2) $\Rightarrow$ (3). Given $L \subseteq \Omega/k$, then $L^{(*)} \subseteq \Omega$. By Proposition 4.39, Ω is separable over k. Thus, $L^{(*)}$ is separable over k and so $L^{(*)}$ is separable over $L_{(*)}$; yet, $L^{(*)}$ is purely inseparable over $L_{(*)}$, so $L^{(*)} = L_{(*)}$.

(3) $\Rightarrow$ (4) is a tautology.

(4) $\Rightarrow$ (5). We have $L^{(*)} = L_{(*)}$, for some $L \subseteq \Omega/k$. Proposition 4.39 implies that Ω is separable over $L_{(*)}$. But, $L_{(*)}$ is always separable over k and separability is transitive, so Ω is separable over k, i.e., $\Omega = \Omega_{(*)}$.

(5) $\Rightarrow$ (1). By definition, $\Omega_{(*)}$ is separable over k and $\Omega = \Omega_{(*)}$, so Ω is separable over k. $\square$

Proposition 4.41 *Say Ω/k is a finite normal extension. Then, $\Omega = \Omega_{(*)}k^{(*)}$ (= the smallest field containing $\Omega_{(*)}$ and $k^{(*)}$). The natural map*

$$\Omega_{(*)} \otimes_k k^{(*)} \longrightarrow \Omega$$

is an isomorphism. Indeed, for all $L/k \subseteq \Omega/k$, we have

(1) $L^{(*)} = Lk^{(*)} = L_{(*)}k^{(*)}$.

(2) $L_{(*)} = L \cap \Omega_{(*)}$.

(3) The natural map

$$L_{(*)} \otimes_k k^{(*)} \longrightarrow L^{(*)}$$

is an isomorphism.

Proof. We just have to prove (1)–(3) for $L/k \subseteq \Omega/k$ and then set $L = \Omega$ to get the rest.

(1) Since $L^{(*)} \supseteq k^{(*)}$ and $L^{(*)} \supseteq L \supseteq L_{(*)}$, we deduce that $L^{(*)} \supseteq L_{(*)}k^{(*)}$ and $L^{(*)} \supseteq Lk^{(*)}$. If $\xi \in L^{(*)}$, then ξ is purely inseparable over $L_{(*)}$, so ξ is purely inseparable over $L_{(*)}k^{(*)}$. If $\xi \in L^{(*)}$, then ξ is separable over $k^{(*)}$ (by Proposition 4.39), so ξ is separable over $L_{(*)}k^{(*)}$. Thus, $L^{(*)}$ is both separable and purely inseparable over $L_{(*)}k^{(*)}$, which means that $L^{(*)} = L_{(*)}k^{(*)}$

(2) This is the definition of $L_{(*)}$, as $L \subseteq \Omega$.

(3) The (illegal definition of the) map is $\alpha \otimes \beta \mapsto \alpha\beta$. The image is $L_{(*)}k^{(*)} = L^{(*)}$. So, we need to prove our map is injective. Now, $k^{(*)} \subseteq k^{p^{-\infty}}$ (where $k^{p^{-\infty}} = \{\xi \in \overline{k} \mid \xi^{p^r} \in k, \text{ for some } r \geq 0\}$). By Mac Lane I and right limits, we get

$$L_{(*)} \otimes_k k^{p^{-\infty}} \longrightarrow L_{(*)}k^{p^{-\infty}}$$

is injective (because $L_{(*)}$ is separable over k). But, $0 \longrightarrow k^{(*)} \longrightarrow k^{p^{-\infty}}$ is exact and vector spaces over a field are flat, so

$$0 \longrightarrow L_{(*)} \otimes_k k^{(*)} \longrightarrow L_{(*)} \otimes_k k^{p^{-\infty}}$$

is still exact. Then, the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & L_{(*)} \otimes_k k^{(*)} & \longrightarrow & L_{(*)} \otimes_k k^{p^{-\infty}} \\ & & \downarrow & & \downarrow \\ & & L_{(*)}k^{(*)} & \hookrightarrow & L_{(*)}k^{p^{-\infty}} \end{array}$$

commutes, and this shows that $L_{(*)} \otimes_k k^{(*)} \longrightarrow L_{(*)}k^{(*)} = L^{(*)}$ is injective. $\square$

Proposition 4.42 *Suppose Ω/k is a finite normal extension and $\mathcal{G} = \mathcal{G}(\Omega/k)$. Let $L/k \subseteq \Omega/k$ and $\mathcal{H} = \mathcal{G}(\Omega/L)$. Then,*

(1) $[\Omega\colon L^{(*)}] = \#(\mathcal{H})$.

(2) $[L_{(*)}\colon k] = (\mathcal{G}\colon \mathcal{H})$.

Moreover, we have $[\Omega\colon \Omega_{(*)}] = [L^{(*)}\colon L_{(*)}] = [k^{(*)}\colon k] =$ *a p-power (the degree of inseparability of Ω/k).*

Proof. We know $\mathrm{Fix}(\mathcal{H}) = L^{(*)}$. So, (1) is just Artin's theorem (Theorem 4.32).

Claim: The map $\sigma \mapsto \sigma \restriction \Omega_{(*)}$ is an isomorphism $\mathcal{G} \xrightarrow{\sim} \mathcal{G}(\Omega_{(*)}/k)$.

We know $\Omega_{(*)}$ is normal over k, so $\sigma \restriction \Omega_{(*)}$ takes $\Omega_{(*)}$ to itself. Therefore, the map $\mathcal{G} \longrightarrow \mathcal{G}(\Omega_{(*)}/k)$ given by $\sigma \mapsto \sigma \restriction \Omega_{(*)}$ is well defined. If $\sigma \mapsto \mathrm{id} \in \mathcal{G}(\Omega_{(*)}/k)$, then $\sigma \restriction \Omega_{(*)}$ leaves $\Omega_{(*)}$ element-wise fixed. If $\xi \in \Omega$, then $\xi^{p^r} \in \Omega_{(*)}$, for some r. Therefore, $\sigma\big(\xi^{p^r}\big) = \xi^{p^r}$. By the usual argument, we conclude that $\sigma(\xi) = \xi$. Therefore, $\sigma = \mathrm{id}$ on Ω and our map is injective. Pick $\widetilde{\sigma} \in \mathcal{G}(\Omega_{(*)}/k)$. We have the diagram

$$\begin{array}{ccc} \Omega & \xrightarrow{\sigma} & \Omega \\ \uparrow & & \uparrow \\ \Omega_{(*)} & \xrightarrow{\widetilde{\sigma}} & \Omega_{(*)} \\ \uparrow & & \uparrow \\ k & = & k. \end{array}$$

By SMA, II, our automorphism $\widetilde{\sigma}$ comes from a $\sigma\colon \Omega \to \Omega$; so, our map is onto.

We have $\mathrm{Fix}(\mathcal{G}(\Omega_{(*)}/k)) = k$ (as $k^{(*)} = k$ in $\Omega_{(*)}$). By Artin's theorem, $[\Omega_{(*)}\colon k] = \#(\mathcal{G})$. Now,

$$[\Omega\colon L_{(*)}] = [\Omega\colon L^{(*)}][L^{(*)}\colon L_{(*)}] = [\Omega\colon \Omega_{(*)}][\Omega_{(*)}\colon L_{(*)}],$$

and

$$\mathcal{H} = \mathcal{G}(\Omega/L) = \mathcal{G}(\Omega/L_{(*)}) = \mathcal{G}(\Omega/L^{(*)}) = \mathcal{G}(\Omega_{(*)}/L_{(*)}),$$

by what's just been proved. By Artin's theorem, $[\Omega\colon L^{(*)}] = \#(\mathcal{H})$, so

$$[\Omega\colon L_{(*)}] = \#(\mathcal{H})[L^{(*)}\colon L_{(*)}] = [\Omega\colon \Omega_{(*)}]\#(\mathcal{H});$$

it follows that $[L^{(*)}\colon L_{(*)}] = [\Omega\colon \Omega_{(*)}]$, for all L. As remarked above,

$$\#(\mathcal{G}) = [\Omega_{(*)}\colon k] = [\Omega_{(*)}\colon L_{(*)}][L_{(*)}\colon k] = \#(\mathcal{H})[L_{(*)}\colon k].$$

Consequently, $[L_{(*)}\colon k] = (\mathcal{G}\colon \mathcal{H})$. □

A picture of the situation is shown in Figure 4.1.

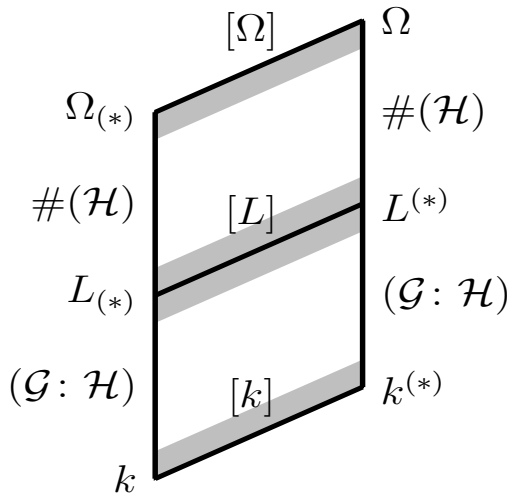


Figure 4.1: Structure of Normal Extensions

4.6 Primitive Elements, Natural Irrationalities, Normal Bases

Proposition 4.43 *If G is a finite subgroup of $K^* = \mathbb{G}_m(K)$, where K is a field, then G is cyclic.*

Proof. An abelian finite group is cyclic iff its p-Sylow subgroups are cyclic (DX). So, we may assume that $\#(G) = p^r$, for some $r > 0$ and some prime p. Let $x \in G$ be an element of maximal order, $q = p^t$, with $t \leq r$. Pick any $y \in G$; the order of y is equal to p^s for some s. But order$(y) \leq$ order(x), so $s \leq t$. As order$(y) \mid$ order(x), we must have $y^q = 1$. So, for every $y \in G$, the element y is a root of $T^q - 1$. As K is a field, this polynomial has at most q roots. But, there exist q roots in G: $1, x, \ldots, x^{q-1}$. Therefore, G is generated by x. □

Corollary 4.44 *In any field, the n-th roots of unity in the field form a cyclic group. It is a finite subgroup of $\mathbb{G}_m(K)$.*

Corollary 4.45 *The multiplicative group of a finite field is always cyclic. Every nonzero element of a finite field is a root of unity.*

Theorem 4.46 *(Artin's Theorem of the Primitive Element) Suppose K/k is a finite extension of fields, then there is some $\alpha \in K$ so that $K = k(\alpha)$ iff there are only finitely many fields, L, with $k \subseteq L \subseteq K$. (Such an α is called a primitive element).*

Proof. ($\Rightarrow$). Assume $K = k(\alpha)$. Let L be any subfield of K, write $f(X)$ for the minimal k-polynomial of α. We know that $f(X)$ is irreducible in $k[X]$. Let $g(X)$ be the minimum L-polynomial for α. As $k(\alpha) = L(\alpha)$, we have $[k(\alpha)\colon L] = [L(\alpha)\colon L] = \deg(g)$. Take L' to be the field obtained by adjoining the coefficients of g to k; we have $L' \subseteq L$. Thus, $g(X) \in L'[X]$ and $g(X)$ is irreducible over L'. Consequently, $[L'(\alpha)\colon L'] = \deg(g)$. But, $L'(\alpha) = k(\alpha)$, so

$$\deg(g) = [k(\alpha)\colon L'] = [k(\alpha)\colon L][L\colon L'] = \deg(g)[L\colon L'],$$

and we deduce that $L = L'$. This means that L is uniquely determined by g. However, every $g(X)$ is a factor of $f(X) \in K[X]$ and since there are only finitely many factors of $f(X)$, there are only finitely many subfields L.

($\Leftarrow$). Say K/k possesses just finitely many subfields.

Claim: Given $\alpha, \beta \in K$, there is some $\gamma \in K$ with $k(\alpha, \beta) \subseteq k(\gamma)$.

If the claim holds, we can finish the proof by induction on the number of generators, n, for K/k. The cases $n = 1, 2$, are clear. Assume that the induction hypothesis holds for $n - 1 \geq 1$, and let $K = k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-2})(\alpha_{n-1}, \alpha_n)$. The claim implies that $K = k(\alpha_1, \ldots, \alpha_{n-2})(\gamma)$, and the induction hypothesis finishes the proof. So, we just have to prove the claim.

If k is finite, so is K. Consequently, $K^* = \mathbb{G}_m(K)$ is cyclic, which means that $K^* = \mathrm{Gp}\{\alpha\}$ and $K = k(\alpha)$. Thus, we may assume k is infinite. Make a map from k to the subfields of $k(\alpha, \beta)$ *via*

$$\lambda \mapsto k(\alpha + \lambda\beta)\ (\subseteq k(\alpha, \beta)).$$

Since k is infinite and since there are only finitely many subfields, there is a pair $(\lambda, \widetilde{\lambda})$, with $\lambda \neq \widetilde{\lambda}$, and

$$k(\alpha + \lambda\beta) = k(\alpha + \widetilde{\lambda}\beta) = L.$$

Thus, both $\alpha + \lambda\beta, \alpha + \widetilde{\lambda}\beta \in L$, so $(\lambda - \widetilde{\lambda})\beta \in L$. But $\lambda - \widetilde{\lambda} \neq 0$, so $\beta \in L$, and then, $\alpha \in L$. It follows that $k(\alpha, \beta) \subseteq L = k(\alpha + \lambda\beta)$, and $\gamma = \alpha + \lambda\beta$ does the job. □

Corollary 4.47 *(Kronecker's Theorem of the Primitive Element) Suppose K/k is a finite separable field extension, then there is some $\alpha \in K$ so that $K = k(\alpha)$.*

Proof. If Ω is the normal closure of K, then it is normal and separable over k. By the main theorem of Galois theory, there is a one-to-one correspondence between subfields of Ω/k and subgroups of $\mathcal{G}(\Omega/k)$. As $\mathcal{G}(\Omega/k)$ is finite, there are only finitely many subfields of Ω/k. But, any subfield of K/k is a subfield of Ω/k, which means that there are only finitely many subfields of K/k. Then, Theorem 4.46 (Artin) implies that α exists. □

Corollary 4.48 *Say K/k is a finite degree field extension and Ω is some field with $k \subseteq \Omega$. Then, the number of k-monomorphisms $K \longrightarrow \Omega$ is at most $[K\colon k]_s$. If $\widetilde{K}$ is a field k-isomorphic to K and $\widetilde{K} \underset{\text{rel}}{\sim} \Omega$, then the number of k-monomorphisms $K \longrightarrow \Omega$ is equal to $[K\colon k]_s$ iff Ω contains the normal closure of $\widetilde{K}$. In particular, if $K \subseteq \Omega$, then the number of k-monomorphisms $K \longrightarrow \Omega$ is equal to $[K\colon k]_s$ iff Ω contains the normal closure of K.*

Proof. Look at $K_{(*)}$, then we know that $[K_{(*)}\colon k] = [K\colon k]_s$. By Kronecker's theorem of the primitive element, there is some $\alpha \in K_{(*)}$ so that $K_{(*)} = k(\alpha)$. To give a k-monomorphism $K \longrightarrow \Omega$ implies that we have a k-monomorphism $K_{(*)} \longrightarrow \Omega$ and the latter is determined by its value on α. Furthermore, two k-monomorphisms of K to Ω which agree on $K_{(*)}$ necessarily agree on K. Hence, the choice of an image of α in Ω determines a k-monomorphism of $K \longrightarrow \Omega$. The image of α, say β, satisfies the minimal k-polynomial, $g(X)$, for α. Consequently, the number of k-monomorphisms $K \longrightarrow \Omega$ is at most equal to the number of roots of $g(X)$ in Ω, which is at most $\deg(g) = [K\colon k]_s$.

Take $\widetilde{K}$ with $\widetilde{K} \underset{\text{rel}}{\sim} \Omega$ and say $\widetilde{K}$ is k-isomorphic to K. Since $\widetilde{K} \cong K$, we are reduced to the case $K = \widetilde{K}$, i.e., $\Omega \underset{\text{rel}}{\sim} K$. We obtain the maximum number of k-monomorphisms iff Ω contains all the roots of any irreducible k-polynomial one root of which lies in k. For then all the conjugates of α are there and their p^rth roots for suitable r. □

Theorem 4.49 *(Natural Irrationalities) Say Ω/k is finite normal and $\widetilde{k} \supseteq k$ is some field with $\widetilde{k} \underset{\text{rel}}{\sim} \Omega$. Write $\widetilde{\Omega}$ for the compositum of $\widetilde{k}$ and Ω, denoted $\Omega\widetilde{k}$ (the smallest field containing Ω and $\widetilde{k}$). Then,*

(1) $\widetilde{\Omega}/\widetilde{k}$ is a normal extension (finite degree).

(2) The map $\sigma \mapsto \sigma \restriction \Omega$ gives a canonical injection $\mathcal{G}(\widetilde{\Omega}/\widetilde{k}) \hookrightarrow \mathcal{G}(\Omega/k)$. The image of this injection is $\mathcal{G}(\Omega/D)$, where $D = \Omega \cap \widetilde{k}$.

Proof. (1) We know $\Omega = k(\alpha_1, \ldots, \alpha_t)$, where $\alpha_1, \ldots, \alpha_t$ are all the roots of a k-polynomial, f. Now, $\widetilde{\Omega} = \widetilde{k}(\alpha_1, \ldots, \alpha_t) =$ a splitting field of the same f, but now viewed as a $\widetilde{k}$-polynomial. So (1) holds.

(2) Given $\sigma \in \mathcal{G}(\widetilde{G}/\widetilde{k})$, look at $\sigma \restriction \Omega$. We know $\sigma(\Omega)$ is a k-conjugate to Ω (inside $\widetilde{\Omega}$). As Ω is normal, $\sigma(\Omega) = \Omega$, and so, $\sigma \restriction \Omega$ is an automomorphism of Ω. As σ fixes $\widetilde{k}$, it fixes $k \subseteq \widetilde{k}$. Thus, $\sigma \restriction \Omega \in \mathcal{G}(\Omega/k)$. If $\sigma \restriction \Omega$ were the identity, we would have $\sigma(\alpha_j) = \alpha_j$, for all j. Also, $\sigma \restriction \widetilde{k} = \mathrm{id}$ and thus, σ fixes all of $\widetilde{k}(\alpha_1, \ldots, \alpha_t) = \widetilde{\Omega}$. Therefore, $\sigma = \mathrm{id}$ in $\mathcal{G}(\widetilde{G}/\widetilde{k})$, i.e., our map is injective.

Let $D = \Omega \cap \widetilde{k}$ and let $\mathcal{H}$ be the image of $\mathcal{G}(\widetilde{\Omega}/\widetilde{k})$ in $\mathcal{G}(\Omega/k)$. We have $\mathcal{H} \cong \mathcal{G}(\widetilde{\Omega}/\widetilde{k})$. As $D \subseteq \widetilde{k}$, we see that $\mathcal{H}$ fixes D, so $\mathcal{H} \subseteq \mathcal{G}(\Omega/D)$. Let $L = \mathrm{Fix}(\mathcal{H})$. We know that $L = L^{(*)}$. As D is fixed, $D \subseteq L = L^{(*)} \subseteq \Omega$. Now, all elements of $\mathcal{H}$ come from $\mathcal{G}(\widetilde{\Omega}/\widetilde{k})$, which implies that $\mathrm{Fix}(\mathcal{H}) \subseteq \mathrm{Fix}(\mathcal{G}(\widetilde{\Omega}/\widetilde{k})) = \widetilde{k}^{(*)}$, by Corollary 4.34. So, $D \subseteq L = L^{(*)} \subseteq \widetilde{k}^{(*)}$ and $D \subseteq L = L^{(*)} \subseteq \Omega$. Pick $\xi \in L$. Then, $\xi \in \widetilde{k}^{(*)}$, so $\xi^{p^r} \in \widetilde{k}$, for some r. But, $\xi \in L \subseteq \Omega$, so $\xi^{p^r} \in \Omega$, and thus, $\xi^{p^r} \in \widetilde{k} \cap \Omega = D$. It follows that $L \subseteq D^{(*)}$. As $L = L^{(*)}$, we have $L^{(*)} \subseteq D^{(*)}$. Yet, $D \subseteq L$, so $D^{(*)} \subseteq L^{(*)}$ and therefore $L^{(*)} = D^{(*)}$. It follows that

$$\mathcal{G}(\Omega/D) = \mathcal{G}(\Omega/L) = \mathcal{G}(\Omega/\mathrm{Fix}(\mathcal{H})) = \mathcal{H},$$

by the fundamental theorem of Galois theory. □

Corollary 4.50 *(Original Form of Natural Irrationalities) Say f is a k-polynomial and $k \subseteq \widetilde{k}$. Then, $\mathcal{G}_{\widetilde{k}}(f)$ is a subgroup of $\mathcal{G}_k(f)$ in a natural way and in fact, $\mathcal{G}_{\widetilde{k}}(f) = \mathcal{G}_D(f)$, where $D = \Omega \cap \widetilde{k}$ and $\Omega \underset{\text{rel}}{\sim} \widetilde{k}$ is a splitting field of f.*

Explanation: Let Ω be a given splitting field of f. The elements of Ω were termed the *natural irrationalities* of f. The reduction in $\mathcal{G}_k(f)$ effected by considering f over $\widetilde{k}$ is the same as that achieved by considering f over the field of those natural irrationalities of f contained in $\widetilde{k}$.

Theorem 4.51 *(Normal Basis Theorem) Suppose K/k is a finite normal and separable extension and let $\mathcal{G}(K/k)$ be its Galois group. Then, there is some $\theta \in K$ so that $\{\sigma\theta \mid \sigma \in \mathcal{G}(K/k)\}$ is a k-basis for K. (This is called a normal basis for K/k).*

Proof. By Kronecker's theorem, $K = k(\alpha)$, for some $\alpha \in K$; let $f(X)$ be the minimum k-polynomial for α. We know $K = k[X]/(f(X))$. Examine two rings: $K[X]$ and $A = K[X]/(f(X))$. Note,

$$K \otimes_k K = K \otimes_k (k[X]/(f(X))) \cong K[X]/(f(X)) = A.$$

For $\sigma \in \mathcal{G} = \mathcal{G}(K/k)$, write α_σ for $\sigma(\alpha)$. Consider the K-polynomials

$$g_\sigma(X) = \frac{f(X)}{f'(\alpha_\sigma)(X - \alpha_\sigma)}.$$

Note that $g_1(X) = f(X)/(f'(\alpha)(X - \alpha))$, so $\sigma g_1(X) = g_\sigma(X)$. The g_σ's satisfy the following properties:

(1) Each $g_\sigma(X)$ has degree $\deg(f) - 1$.

(2) If $\sigma \neq \tau$, then $g_\sigma(\alpha_\tau) = 0$.
Also, by Taylor's theorem,

$$f(X) = f(\alpha_\sigma + (X - \alpha_\sigma)) = f(\alpha_\sigma) + f'(\alpha_\sigma)(X - \alpha_\sigma) + O((X - \alpha_\sigma)^2),$$

so, $g_\sigma(X) = 1 + O(X - \alpha_\sigma)$ and therefore,

(3) $g_\sigma(\alpha_\sigma) = 1$.

Consider the polynomial $\sum_{\sigma \in \mathcal{G}} g_\sigma(X) - 1 \, (\in K[X])$. By (2) and (3), we see that this polynomial vanishes on the n elements $\alpha, \alpha_{\sigma_2}, \ldots, \alpha_{\sigma_n}$, where $\mathcal{G} = \{1, \sigma_2, \ldots, \sigma_n\}$. By (1), this polynomial has degree $n - 1$. Hence, the polynomial is identically zero and we have

$$\sum_{\sigma \in \mathcal{G}} g_\sigma(X) = 1. \qquad \text{(partition of unity)} \quad (*)$$

In A, we get

$$\sum_{\sigma \in \mathcal{G}} \overline{g_\sigma(X)} = 1. \qquad (\overline{*})$$

Pick σ, τ, with $\sigma \neq \tau$, and look at $g_\sigma(X)g_\tau(X)$. For all $\rho \in \mathcal{G}$, we have $g_\sigma(\alpha_\rho)g_\tau(\alpha_\rho) = 0$. But, $f(X) = \prod_{\rho \in \mathcal{G}}(X - \alpha_\rho)$, so $f(X) \mid g_\sigma(X)g_\tau(X)$ if $\sigma \neq \tau$. If we read this in A, we get

$$\overline{g_\sigma(X)}\,\overline{g_\tau(X)} = 0 \quad \text{in } A, \text{ if } \sigma \neq \tau. \qquad \text{(orthogonality)} \quad (**)$$

If we multiply $(*)$ by $g_\tau(X)$, we get

$$\sum_{\sigma \in \mathcal{G}} g_\tau(X)g_\sigma(X) = g_\tau(X),$$

and if we read this in A and use $(**)$, we get

$$(\overline{g_\sigma(X)})^2 = \overline{g_\sigma(X)} \quad \text{in } A. \qquad \text{(idempotence)} \quad (***)$$

Write $e_\sigma = \overline{g_\sigma(X)}$, so $e_\sigma \in A = K \otimes_k K$. Then, $(*)$, $(**)$ and $(***)$ say:

$$\sum_{\sigma\in\mathcal{G}} e_\sigma = 1; \quad e_\sigma e_\tau = \delta_{\sigma\tau} e_\sigma.$$

Therefore, the e_σ's are an orthogonal decomposition of 1 by idempotents, and so,

$$K \otimes_k K \cong \prod_{\sigma\in\mathcal{G}} K e_\sigma \cong \prod_{\sigma\in\mathcal{G}} K.^3$$

Order the elements of $\mathcal{G}$ in some fashion as we did above: $1, \sigma_2, \ldots, \sigma_n$, and consider the matrix

$$(g_{\sigma\tau}(X)) \in \mathrm{M}_n(K[X]).$$

Let $D(X) = \det(g_{\sigma\tau}(X))$. In order to compute $D(X)$ in A, consider $D(X)^2$. Since $\det(g_{\sigma\tau}(X)) = \det(g_{\sigma\tau}(X))^\top$, we can compute $D(X)^2$ by multiplying columns by columns and summing. We get

$$\sum_{\sigma\in\mathcal{G}} g_{\sigma\tau}(X) g_{\sigma\rho}(X) = \sum_{\sigma\in\mathcal{G}} \sigma(g_\tau(X))\sigma(g_\rho(X)) = \sum_{\sigma\in\mathcal{G}} \sigma(g_\tau(X) g_\rho(X)).$$

If we read this in A, we get

$$\begin{aligned}
\sum_{\sigma\in\mathcal{G}} \overline{g_{\sigma\tau}(X)}\,\overline{g_{\sigma\rho}(X)} &= \sum_{\sigma\in\mathcal{G}} \sigma(\overline{g_\tau(X)}\,\overline{g_\rho(X)}) = 0, \quad \text{if} \quad \tau \neq \rho; \quad \text{and} \\
&= \sum_{\sigma\in\mathcal{G}} \sigma(\overline{g_\rho(X)}), \quad \text{if} \quad \tau = \rho \\
&= \sum_{\sigma\in\mathcal{G}} \overline{g_{\sigma\rho}(X)} \\
&= \sum_{\tau\in\mathcal{G}} \overline{g_\tau(X)} = 1, \quad \text{if} \quad \tau = \rho.
\end{aligned}$$

Therefore, we find that in A, the matrix $(g_{\sigma\tau}(X))(g_{\sigma\tau}(X))^\top$ is the identity matrix and so, $\overline{D(X)^2} = 1$. Consequently, $D(X)^2 \equiv 1 \pmod{f(X)}$, which shows that $D(X) \neq 0$.

If k is infinite, then there is some $\xi \in k$ with $D(\xi) \neq 0$. Let $\theta = g_1(\xi)$. Then, $\sigma\tau\theta = \sigma\tau g_1(\xi) = g_{\sigma\tau}(\xi)$. Consequently, $\det(\sigma\tau(\theta)) = \det(g_{\sigma\tau}(\xi)) = D(\xi) \neq 0$. If $\{\sigma\theta\}_{\sigma\in\mathcal{G}}$ were linearly dependent, we would have

$$\sum_{\tau\in\mathcal{G}} a_\tau \tau\theta = 0,$$

for some $a_\tau \in k$, not all zero. If we apply σ, we get

$$\sum_{\tau\in\mathcal{G}} a_\tau \sigma\tau\theta = 0.$$

So, (a_τ) would be a nontrivial simultaneous solution to the linear system of equations

$$\sum_{\tau\in\mathcal{G}} X_\tau \sigma\tau\theta = 0, \quad \text{for} \quad \sigma \in \mathcal{G},$$

a contradiction to the fact that $\det(\sigma\tau(\theta)) \neq 0$. Therefore, $\{\sigma\theta\}_{\sigma\in\mathcal{G}}$ is linearly independent and the case where k is infinite is proved.

If k is finite, we don't need the $g_\sigma(X)$ and $D(X)$. We do need the following facts to be proved below:

[3] At this stage, we are essentially done. However, we've not kept track of the $\mathcal{G}$ action; so, a little more argument is needed.

(1) The Galois group $\mathcal{G}(K/k)$ is cyclic.

(2) The Galois group $\mathcal{G}(K/k)$ has a canonical generator, $\mathbf{F}$, where $\mathbf{F}(\xi) = \xi^{\#(k)}$, for all $\xi \in K$.

Recall that for a linear transformation, T, on a finite dimensional vector space, V, if $m(X)$ is the minimal polynomial for T then there exists a vector, $v \in V$, so that $m(T)v = 0$ but *no polynomial of smaller degree than $m(X)$ kills v*. Now, our K plays the role of V and the automorphism $\mathbf{F}$ plays the role of T. If we can show that the minimum polynomial of $\mathbf{F}$ is exactly $X^n - 1$, where $n = [K\colon k]$, then we take a Θ in K so that no polynomial of smaller degree than $\mathbf{F}^n - 1$ kills Θ. This means that

$$\Theta, \mathbf{F}(\Theta), \cdots, \mathbf{F}^{n-1}(\Theta)$$

are linearly independent; so by (1) and (2) we have our normal basis.

Of course, by (1) and (2), $\mathbf{F}^{n-1} - 1 \equiv 0$ on K; therefore, whatever is the minimal polynomial for $\mathbf{F}$, it divides $X^n - 1$ and its degree is at most n. Were $m(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d$ the minimal polynomial for $\mathbf{F}$ and $d < n$, then

$$0 = a_0\mathbf{F}^d(\xi) + a_1\mathbf{F}^{d-1}(\xi) + \cdots + a_{d-1}\mathbf{F}(\xi) + a_0\mathbf{F}^0(\xi) \qquad (\dagger)$$

for all $\xi \in K$. But this is a contradiction of Dedekind's Theorem as ($\dagger$) is a linear dependence among I, $\mathbf{F}, \cdots, \mathbf{F}^d$, and we are done. □

Remark: The argumeent actually proves (independently of previous arguments) that *every cyclic extension possesses a normal basis*.

The facts concerning finite fields were proved by E.H. Moore. Here is his theorem:

Theorem 4.52 *(E.H. Moore, 1892) If k is a finite field then* $\mathrm{char}(k) = p > 0$ *and $\#(k) = p^l$, for some prime p and some $l \geq 1$. If $\mathbb{F}_p$ is the prime field of characteristic p, then for each integer $l \geq 1$, there exists one and only one finite field of cardinality p^l, up to $\mathbb{F}_p$-isomorphism. If K/k is a finite extension of degree n and k is a finite field, then K/k is always normal and separable; the Galois group $\mathcal{G}(K/k)$ is cyclic of order n and has a canonical generator, $\mathbf{F}$. This $\mathbf{F}$ is the Frobenius automorphism, and it is given by $\xi \mapsto \mathbf{F}(\xi) = \xi^{\#(k)}$, for all $\xi \in K$. Each finite field has exactly one extension of degree n for each $n \geq 1$.*

Proof. The statement in the first sentence is well-known. Pick $l \geq 1$ and look at the splitting field of the polynomial $X^{p^l} - X \in \mathbb{F}_p[X]$. Note, if ξ and η are roots of this polynomial, then $\xi \pm \eta$, $\xi\eta$, ξ/η are also roots of the polynomial. Thus, the set of roots is a field and it contains $\mathbb{F}_p$, because for all $\xi \in \mathbb{F}_p$, we have $\xi^p = \xi$. It follows that the splitting field is exactly the entire set of roots and as the derivative of $X^{p^l} - X$ is -1, the roots are distinct. Therefore, we get a field with p^l elements. Conversely, any field with p^l elements has multiplicative group of order $p^l - 1$. So, this group has a generator of order $p^l - 1$ and for this generator, θ, we get $\theta^{p^l} = \theta$. Consequently, any power of θ satisfies $X^{p^l} - X = 0$ and so, our field is a splitting field of $X^{p^l} - X$; such fields are unique up to $\mathbb{F}_p$-isomorphism.

Suppose K/k has degree n, then K is a splitting field, so K/k is normal. Moreover, finite fields are perfect, so K/k is separable.

Consider $\mathbf{F}_k \in \mathcal{G}(K/k)$ where $\mathbf{F} = \mathbf{F}_k$ is defined by $\mathbf{F}(\xi) = \xi^{\#(k)}$. Look at $1 = \mathbf{F}^0, \mathbf{F}^1, \mathbf{F}^2, \ldots, \mathbf{F}^{n-1}$. These are distinct, as $\mathbf{F}^r(\theta) = \mathbf{F}^s(\theta)$ implies $\mathbf{F}^{r-s}(\theta) = \theta$; that is, $\theta^{q^{r-s}-1} = 1$. Yet, $q^{r-s} < \#(K)$, a contradiction. Now, $\mathbf{F}^n(\xi) = \xi^{q^n}$. It follows from linear algebra that $q^n = \#(K)$ and by the above, $\xi^{q^n} = \xi$ implies $\mathbf{F}^n = 1$. Observe, $\mathbf{F}(\xi) = \xi$ when $\xi \in k$, which implies that $\mathbf{F}$ is a k-automorphism and $\mathbf{F}$ has the proper order. □

Interpretations of the Normal Basis Theorem

(1) **Algebraic Interpretation**

Assume K/k is normal and separable, let $\mathcal{G} = \mathcal{G}(K/k)$ with $\#(\mathcal{G}) = n$. We claim that there is a natural ring homomorphism

$$K \otimes_k K \longrightarrow \prod_{\sigma \in \mathcal{G}} K.$$

(Here $\prod_{\sigma\in\mathcal{G}} K$ consists of n factors of K under coordinatewise multiplication.) Take $\alpha, \beta \in K$, and send (α, β) to the n-tuple

$$\langle \alpha\beta, \alpha\sigma_2\beta, \ldots, \alpha\sigma_n\beta \rangle,$$

where $\mathcal{G} = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. This is a bilinear map, so we get a map

$$K \otimes_k K \longrightarrow \prod_{\sigma \in \mathcal{G}} K.$$

On the left hand side, we have a K-vector space *via* $\alpha \in K$ acts as $\alpha \otimes 1$. The righthand side is a K-vector space *via* the action of K on each factor; thus, the above map is K-linear. We also have

$$\begin{aligned} (\alpha \otimes \beta)(\gamma \otimes \delta) &= (\alpha\gamma \otimes \beta\delta) \\ (\alpha\sigma\beta)_\sigma(\gamma\sigma\delta)_\sigma &= (\alpha\gamma\sigma(\beta\delta))_\sigma. \end{aligned}$$

The normal basis theorem says that this ring map is an isomorphism. Say θ is our normal basis element, then

$$1 \otimes \theta, 1 \otimes \sigma_2\theta, \ldots, 1 \otimes \sigma_n\theta$$

is a basis for $K \otimes_k K$ over K. Now, as

$$1 \otimes \tau\theta \mapsto \langle \sigma\tau\theta \rangle_{\sigma\in\mathcal{G}},$$

a basis on the left hand side goes to a basis on the right hand side; so, the map is an isomorphism. Check the converse.

(2) **Geometric Interpretation**

Say X is a space; G is a group, and suppose G acts on X: There is a map $G \times X \longrightarrow X$ denoted $(\sigma, x) \mapsto \sigma x$.

Definition 4.13 A space X is a *principal homogeneous space* for G (*PHS* for G) if

(1) X is a *homogeneous space*, i.e., for all $x, y \in G$, there is some $\sigma \in G$ with $\sigma x = y$ (G acts transitively), i.e., X is equal to an orbit of G under the action.

(2) The group element $\sigma \in G$ in (1) is *uniquely* determined by x and y.

Proposition 4.53 *The following statements are equivalent:*

(A) X is a PHS for G.

(B) The map $G \prod X \longrightarrow X \prod X$ via $(\sigma, x) \mapsto (\sigma x, x)$ is an isomorphism.

Proof. $(A) \Rightarrow (B)$. Given $(\xi, \eta) \in X \prod X$, there is a $\sigma \in G$ with $\sigma\xi = \eta$. Thus, $(\sigma, \xi) \mapsto (\eta, \xi)$ under our map, which shows its surjectivity. The map is injective by property (2) of the definition.

$(B) \Rightarrow (A)$. This is a tautology. □

Let G be a group and let k be a field. Write $A(G)$ for the k-algebra of all functions $f\colon G \to k$ under pointwise operations (e.g., $(fg)(\sigma) = f(\sigma)g(\sigma)$, etc.). The k-algebra $A(G)$ has a basis, $\{e_\sigma\}$, where $e_\sigma(\tau) = \delta_{\sigma\tau}$.

Suppose now G is a finite group, then there is a k-algebra map $\Delta\colon A(G) \to A(G) \otimes_k A(G)$ given by (convolution)

$$\Delta(e_\tau) = \sum_{\sigma \in G} e_\sigma \otimes e_{\sigma^{-1}\tau}.$$

I claim: For all k-algebras, R,

$$A(G)(R) = \mathrm{Hom}_k(A(G), R)$$

is a group. Given $\varphi, \psi \in A(G)(R)$, we define $\varphi\psi$ as the composition

$$A(G) \xrightarrow{\Delta} A(G) \otimes_k A(G) \xrightarrow{\varphi\otimes\psi} R \otimes_k R \xrightarrow{\text{mult}} R.$$

Let us see what $(\varphi\psi)(e_\rho)$ is. We have

$$\Delta(e_\rho) = \sum_{\sigma \in \mathcal{G}} e_\sigma \otimes e_{\sigma^{-1}\rho} \quad \text{and} \quad (\varphi \otimes \psi)(\Delta(e_\rho)) = \sum_{\sigma \in \mathcal{G}} \varphi(e_\sigma) \otimes \psi(e_{\sigma^{-1}\rho}),$$

so

$$(\varphi\psi)(e_\rho) = \sum_{\sigma \in \mathcal{G}} \varphi(e_\sigma)\psi(e_{\sigma^{-1}\rho}).$$

(Note: We can form $k[G]$ = the group algebra and the reader should check that:

(1) As linear spaces, $A(G)$ and $k[G]$ are naturally dual.

(2) Multiplication in $A(G)$ goes over to Δ for $k[G]$ and Δ for $A(G)$ goes over to ordinary multiplication in $k[G]$.)

The space $\mathrm{Spec}\, A(G) = \underline{G}$ is a geometric object (at least it's a topological space). Indeed, it is described by the equations $X_\sigma X_\tau = \delta_{\sigma\tau} X_\sigma$ and $\sum_{\sigma \in G} X_\sigma = 1$ (the e_σ have been replaced by the X_σ for convenience of more usual notation). To find solutions in a ring R is to give a homomorphism $A(G) \longrightarrow R$, as above. If $\mathrm{Spec}\, R$ is connected (i.e., $e^2 = e$ implies $e = 0$ or $e = 1$) then solutions correspond just to the set G and we recover the multiplication in G from our funny multiplication using Δ.

We know that

$$\mathrm{Spec}(B \otimes_A C) = \mathrm{Spec}\, B \prod_{\mathrm{Spec}\, A} \mathrm{Spec}\, C.$$

The meaning of this is exactly that

$$\mathrm{Hom}_{A\text{-alg}}(B \otimes_A C, R) = \mathrm{Hom}_{A\text{-alg}}(B, R) \prod \mathrm{Hom}_{A\text{-alg}}(C, R),$$

where on the right we have the ordinary cartesian product of sets.

Look at $A(G) \otimes_k K$, where $G = \mathcal{G}(K/k)$. Remember, $A(G)$ has the e_σ's and $K \otimes_k K$ has the $g_\sigma(X) = e_\sigma$'s, too. So, there is an isomorphism of rings

$$A(G) \otimes_k K \cong K \otimes_k K.$$

Upon taking Spec's we see that

$$\underline{G} \prod \mathrm{Spec}\, K \cong \mathrm{Spec}\, K \prod \mathrm{Spec}\, K.$$

Therefore, the fact $\mathrm{Spec}\, K$ *is a PHS for* $\underline{G}$ *is exactly the normal basis theorem.*

4.7 Galois Cohomology, Norms and Traces

Recall that in Chapter 1, Section 1.4, we introduced the notion of cohomology of a group, G, with coefficients in a G-module, M. I urge you to review the appropriate parts of Section 1.4 now.

If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is an exact sequence of G-modules, then, for each $r \geq 0$, the sequence

$$0 \longrightarrow C^r(G, M') \longrightarrow C^r(G, M) \longrightarrow C^r(G, M'') \longrightarrow 0$$

is again exact and a commutative diagram of G-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

yields a similar commmutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^r(G, M') & \longrightarrow & C^r(G, M) & \longrightarrow & C^r(G, M'') & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C^r(G, N) & \longrightarrow & C^r(G, N) & \longrightarrow & C^r(G, N'') & \longrightarrow & 0 \end{array}$$

for all $r \geq 0$. We'll see in the next chapter (Chapter 5, Lemma 5.7 and Corollary 5.8) that these statements imply the following facts:

Fact I. If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *is an exact sequence of* G*-modules, then we have the long exact sequence of cohomology*

$$\begin{array}{l} 0 \longrightarrow H^0(G, M') \longrightarrow H^0(G, M) \longrightarrow H^0(G, M'') \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \xrightarrow{\delta^{(0)}} \\ \quad H^1(G, M') \longrightarrow H^1(G, M) \longrightarrow H^1(G, M'') \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \xrightarrow{\delta^{(1)}} \\ \quad H^2(G, M') \longrightarrow \cdots \qquad\qquad\qquad\qquad \cdots \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \xrightarrow{\delta^{(r-1)}} \\ \quad H^r(G, M') \longrightarrow H^r(G, M) \longrightarrow H^r(G, M'') \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \xrightarrow{\delta^{(r)}} \\ \quad H^{r+1}(G, M') \longrightarrow \cdots \end{array}$$

(The maps $\delta^{(r)}$ are the *connecting homomorphisms* of the long exact sequence.)

Fact II. A small commutative diagram of G*-modules*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

yields a large (long) commutative diagram of cohomology:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & H^0(G,M') & \longrightarrow & \cdots & \longrightarrow & H^r(G,M) & \longrightarrow & H^r(G,M'') & \longrightarrow & H^{r+1}(G,M') & \longrightarrow & \cdots \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^0(G,N') & \longrightarrow & \cdots & \longrightarrow & H^r(G,N) & \longrightarrow & H^r(G,N'') & \longrightarrow & H^{r+1}(G,N') & \longrightarrow & \cdots
\end{array}$$

The proofs of these facts do not use any of the material below, so we will assume them now without circularity in our reasoning.

Suppose B is an abelian group. We can make, from B, a G-module, $\mathrm{Map}(G,B)$, as follows:

$$\mathrm{Map}(G,B) = \{f \mid f\colon G \to B, \quad \text{i.e., } f \text{ is a function from } G \text{ to } B\}.$$

The module structure is

$$(\sigma f)(\tau) = f(\tau\sigma)$$

and one checks that if B is actually a G-module, there is a G-module *injection*

$$\epsilon_B\colon B \to \mathrm{Map}(G,B)$$

given by

$$\epsilon_B(b)(\sigma) = \sigma b. \quad \text{(DX)}$$

The module $\mathrm{Map}(G,B)$ is special in that it is "cohomologically trivial." This is

Proposition 4.54 *For every abelian group, B and every $n > 0$, we have*

$$H^n(G, \mathrm{Map}(G,B)) = (0).$$

Proof. Choose $f \in Z^n(G, \mathrm{Map}(G,B))$ and assume $n > 0$. Then f is a function of n variables chosen from G and has values in $\mathrm{Map}(G,B)$. We define a function, g, of $n-1$ variables chosen from G with values in $\mathrm{Map}(G,B)$ as follows:

$$g(\sigma_1,\ldots,\sigma_{n-1})(\tau) = f(\tau,\sigma_1,\ldots,\sigma_{n-1})(1).$$

Let us prove that $\delta g = f$, which will finish the argument.

$$(\delta g)(\sigma_1,\ldots,\sigma_n) = \sigma_1 g(\sigma_2,\ldots,\sigma_n) + \sum_{r=1}^{n-1}(-1)^r g(\sigma_1,\ldots,\sigma_r\sigma_{r+1},\ldots,\sigma_n) + (-1)^n g(\sigma_1,\ldots,\sigma_{n-1}).$$

So, upon evaluating δg on an arbitrary element, τ, we get

$$\begin{aligned}(\delta g)(\sigma_1,\ldots,\sigma_n)(\tau) &= g(\sigma_2,\ldots,\sigma_n)(\tau\sigma_1) + \sum_{r=1}^{n-1}(-1)^r g(\sigma_1,\ldots,\sigma_r\sigma_{r+1},\ldots,\sigma_n)(\tau) + (-1)^n g(\sigma_1,\ldots,\sigma_{n-1})(\tau) \\ &= f(\tau\sigma_1,\sigma_2,\ldots,\sigma_n)(1) + \sum_{r=1}^{n-1}(-1)^r f(\tau,\sigma_1,\ldots,\sigma_r\sigma_{r+1},\ldots,\sigma_n)(1) + (-1)^n f(\tau,\sigma_1,\ldots,\sigma_{n-1})(1).\end{aligned}$$

Now, $f(\sigma_1,\ldots,\sigma_n)(\tau) = (\tau f)(\sigma_1,\ldots,\sigma_n)(1)$, and

$$\begin{aligned}0 = \delta f(\tau,\sigma_1,\ldots,\sigma_n) = (\tau f)(\sigma_1,\ldots,\sigma_n) - f(\tau\sigma_1,\sigma_2,\ldots,\sigma_n) + \sum_{s=2}^{n}(-1)^s f(\tau,\sigma_1,\ldots,\sigma_{s-1}\sigma_s,\ldots,\sigma_n) \\ +(-1)^{n+1} f(\tau,\sigma_1,\ldots,\sigma_{n-1}).\end{aligned}$$

Therefore,

$$(\tau f)(\sigma_1,\ldots,\sigma_n) = f(\tau\sigma_1,\sigma_2,\ldots,\sigma_n) + \sum_{s=2}^{n}(-1)^{s-1}f(\tau,\sigma_1,\ldots,\sigma_{s-1}\sigma_s,\ldots,\sigma_n) + (-1)^n f(\tau,\sigma_1,\ldots,\sigma_{n-1}).$$

Let $n = s-1$ in the sum above and evaluate both sides at 1. We get immediately

$$f(\sigma_1,\ldots,\sigma_n)(\tau) = \delta g(\sigma_1,\ldots,\sigma_n)(\tau). \qquad \square$$

Proposition 4.54 is extremely useful and very powerful. Rather than explain this in abstract terms, let's begin to use Proposition 4.54 and, in so doing, show *how* to use it and *why* it is powerful. One of the facts left unproved in Chapter 1 was the fact that $H^r(G,M)$ is $\#(G)$-torsion if $r>0$ (any module, M). Based on Proposition 4.54, we can now prove this and, while our proof is not the most elegant known, it certainly requires the least machinery:

Proposition 4.55 *If G is a finite group and M is any G-module, then $H^r(G,M)$ is $\#(G)$-torsion if $r>0$.*

Proof. Take the case $r=1$, first. If $f\in Z^1(G,M)$, we know

$$f(\sigma\rho) = \sigma f(\rho) + f(\sigma).$$

Write α for the element $-\sum_{\rho\in G} f(\rho)$ of M. We compute $\sigma\alpha$:

$$\begin{aligned}\sigma\alpha = -\sum_{\rho\in G}\sigma f(\rho) &= -\sum_{\rho\in G}(f(\sigma\rho)-f(\sigma)) \\ &= -\sum_{\rho\in G} f(\sigma\rho) + \#(G)f(\sigma) \\ &= \alpha + \#(G)f(\sigma).\end{aligned}$$

Therefore, $(\#(G)f)(\sigma) = (\delta\alpha)(\sigma)$, and the case $r=1$ is done.

Now, use induction on r—here is where Proposition 4.54 enters. Assume as induction hypothesis that given r ($r\geq 1$), for all modules, N, we have $H^r(G,N)$ is $\#(G)$-torsion. The step from r to $r+1$ goes like this:

Choose M, embed M in $\mathrm{Map}(G,M)$, to get

$$0 \longrightarrow M \xrightarrow{\epsilon_M} \mathrm{Map}(G,M) \longrightarrow \mathrm{coker} \longrightarrow 0.$$

Apply cohomology (i.e., use the long exact sequence of Fact I), we get

$$\ldots \longrightarrow H^r(G,\mathrm{Map}(G,M)) \longrightarrow H^r(G,\mathrm{coker}) \longrightarrow H^{r+1}(G,M) \longrightarrow H^{r+1}(G,\mathrm{Map}(G,M)) \longrightarrow \ldots \qquad (*)$$

The ends of $(*)$ vanish by Proposition 4.54 and we obtain the isomorphism

$$H^r(G,\mathrm{coker}) \xrightarrow{\sim} H^{r+1}(G,M), \quad \text{for all } r\geq 1. \qquad (**)$$

But, the left side of $(**)$ is $\#(G)$-torsion by our induction hypothesis, therefore $H^{r+1}(G,M)$ is also $\#(G)$-torsion. $\square$

The special case when G is cyclic is both instructive and important for some material to follow. For arbitrary (finite) G, and any G-module, M, we define the *norm map*, $\mathcal{N}_G$, taking M to itself by

$$\mathcal{N}_G(m) = \sum_{\sigma\in G}\sigma m.$$

Note that the image of $\mathcal{N}_G$ lies in M^G. Further, $\mathcal{N}_G$ is actually a G-module map, for

$$\mathcal{N}_G(\tau m) = \sum_{\sigma\in G} \sigma\tau m = \mathcal{N}_G(m) = \tau\mathcal{N}_G(m).$$

(In cases of interest below, the map $\mathcal{N}_G$ is usually called *trace* and when M is written multiplicatively then $\mathcal{N}_G$ is called the *norm*.) Now, the equation $\mathcal{N}_G(\tau m) = \tau\mathcal{N}_G(m)$ shows that the elements $\tau m - m$ all lie in $\operatorname{Ker}\mathcal{N}_G$. The submodule generated by all $\tau m - m$, as τ runs over G and m over M, is denoted IM; so, $IM \subseteq \operatorname{Ker}\mathcal{N}_G(M)$.

Proposition 4.56 *If G is a (finite) cyclic group and σ is one of its generators, then for any module, M:*

(a) The map $f \mapsto f(\sigma) \in M$ is a G-isomorphism of $Z^1(G, M)$ with $\operatorname{Ker}\mathcal{N}_G(M)$,

(b) The submodule IM is generated by $\sigma m - m$ for this fixed σ and m varying over M,

(c) There is an isomorphism $H^1(G, M) \xrightarrow{\sim} \operatorname{Ker}\mathcal{N}_G/IM$.

Proof. The elements of G are $1, \sigma, \ldots, \sigma^{n-1}$. Let $f \in Z^1(G, M)$, so $f(\rho\tau) = \rho f(\tau) + f(\rho)$ for all ρ and τ of G. Apply this successively to the powers of σ:

$$f(\sigma^2) = f(\sigma\sigma) = \sigma f(\sigma) + f(\sigma); \quad f(\sigma^3) = f(\sigma\sigma^2) = \sigma f(\sigma^2) + f(\sigma) = \sigma^2 f(\sigma) + \sigma f(\sigma) + f(\sigma), \quad \text{etc.} \quad (*)$$

We find that

$$f(1) = f(\sigma^n) = \sigma^{n-1} f(\sigma) + \sigma^{n-2} f(\sigma) + \cdots + f(\sigma) = \mathcal{N}_G(f(\sigma)).$$

But, $f(1) = f(1 \cdot 1) = f(1) + f(1)$; so, $f(1) = 0$. Thus, when $f \in Z^1(G, M)$, we get $f(\sigma) \in \operatorname{Ker}\mathcal{N}_G(M)$.

From $(*)$ above, we see that $f(\sigma)$ determines f when f is a cocycle, conversely an easy argument using the inductive definition of $f(\sigma^i)$ given by $(*)$ (namely, $\sigma f(\sigma^{i-1}) + f(\sigma)$) shows that if $f(\sigma) \in \operatorname{Ker}\mathcal{N}_G$ our definition makes f a 1-cocycle (DX). This gives an abelian group isomorphism $Z^1(G, M) \xrightarrow{\sim} \operatorname{Ker}\mathcal{N}_G$. Since $Z^1(G, M)$ is a G-module *via* M, the map is a G-module isomorphism, and (a) is proved.

To prove (b), all we need to show is that $\tau m - m$ is in the submodule generated by $\sigma\widetilde{m} - \widetilde{m}$ as $\widetilde{m}$ ranges over M, where τ is a fixed arbitrary element of G. But, $\tau = \sigma^i$; so,

$$\tau m - m = \sigma^i m - m = \sigma^i m - \sigma^{i-1} m + \sigma^{i-1} m - m = \sigma^{i-1}(\sigma m - m) + \sigma^{i-1} m - m.$$

A clear induction finishes the argument.

(c) The group $B^1(G, M)$ consists exactly of those f for which $f(\tau) = \tau m - m$ for some $m \in M$. Hence, $f(\sigma) = \sigma m - m \in IM$ and part (a) now shows that in the isomorphism $Z^1(G, M) \xrightarrow{\sim} \operatorname{Ker}\mathcal{N}_G$ the subgroup $B^1(G, M)$ corresponds to IM; (c) is thereby proved. □

Given a finite normal (field) extension K/k, we can consider the cohomology groups of the Galois group $\mathcal{G} = \mathcal{G}(K/k)$. These cohomology groups give a sequence of very interesting invariants of the layer K/k. As nomenclature, the groups $H^r(\mathcal{G}(K/k), M)$ are called the *Galois cohomology groups of K/k with values in M*, and as notation we write $H^r(K/k, M)$ for $H^r(\mathcal{G}(K/k), M)$. Probably, the most useful facts about Galois cohomology are the two forming the statement of the next proposition.

Proposition 4.57 *(Hilbert Theorem 90[4].) If K/k is a finite normal extension, then*

(1) $H^r(K/k, K^+) = (0)$, all $r > 0$ and

(2) $H^1(K/k, K^*) = (0)$.

[4]When K/k is a cyclic extension, statement (2) is the essential content of Theorem 90 (§54) of Hilbert's magnificent paper [23]. The general case of a normal extension is due to E. Noether.

Proof. For (1), we examine the layer $K/k^{(*)}$ and apply the normal basis theorem to it. I claim that, as $\mathcal{G} = \mathcal{G}(K/k)$-modules, $\mathrm{Map}(\mathcal{G}, k^{(*)})$ and K are isomorphic. If we show this, then Proposition 4.54 and our isomorphism establish (1).

If $f \in \mathrm{Map}(\mathcal{G}, k^{(*)})$, we send f to $\sum_{\sigma\in\mathcal{G}} f(\sigma)\sigma^{-1}\theta$, where θ is a normal basis element for $K/k^{(*)}$. The linear independence of the elements $\{\sigma\theta\}_{\sigma\in\mathcal{G}}$ shows our map is injective; that it is surjective is obvious. As for the $\mathcal{G}$-action, call our map Θ then,

$$\begin{aligned}\Theta(\tau f) = \sum_{\sigma\in\mathcal{G}} (\tau f)(\sigma)\sigma^{-1}\theta &= \sum_{\sigma\in\mathcal{G}} f(\sigma\tau)\sigma^{-1}\theta \\ &= \sum_{\rho\in\mathcal{G}} f(\rho)\tau\rho^{-1}\theta \\ &= \tau\cdot\sum_{\rho\in\mathcal{G}} f(\rho)\rho^{-1}\theta \\ &= \tau\Theta(f),\end{aligned}$$

as contended.

The proof of (2) has a similar flavor but depends on Dedekind's theorem (our Theorem 4.30). We take as family of characters of K^* the elements of $\mathcal{G} = \mathcal{G}(K/k)$. By Dedekind's theorem, they are independent; that is, any relation (with $x_\sigma \in K^*$)

$$\sum_{\sigma\in\mathcal{G}} x_\sigma\sigma(\lambda) = 0, \quad \text{all } \lambda \in K^*$$

necessarily implies that all the $x_\sigma = 0$. Given $f \in Z^1(K/k, K^*)$, take as the x_σ the elements $f(\sigma) \in K^*$. None of the x_σ are zero, so there must be a $\lambda \in K^*$ with

$$\beta = \sum_{\sigma\in\mathcal{G}} f(\sigma)\sigma(\lambda) \neq 0.$$

Now, $\tau\beta = \sum_{\sigma\in\mathcal{G}} \tau f(\sigma)\tau\sigma(\lambda)$, and as f is a 1-cocycle, we have $\tau f(\sigma)\cdot f(\tau) = f(\tau\sigma)$. Thus,

$$\begin{aligned}\beta = \sum_{\sigma\in\mathcal{G}} f(\tau\sigma)(\tau\sigma)(\lambda) &= \sum_{\sigma\in\mathcal{G}} (\tau f(\sigma)\cdot f(\tau))(\tau\sigma)(\lambda) \\ &= f(\tau)\sum_{\sigma\in\mathcal{G}} \tau f(\sigma)(\tau\sigma)(\lambda) \\ &= f(\tau)\cdot(\tau\beta).\end{aligned}$$

Let $\alpha = 1/\beta$, then $(\tau\alpha)/\alpha = f(\tau)$, as required. □

Remark: Proposition 4.57 gives yet another interpretation of the normal basis theorem. It shows that *for K normal over k, the $\mathcal{G}(K/k)$-module K is of the form* $\mathrm{Map}(\mathcal{G}, -)$*; namely, it is* $\mathrm{Map}(\mathcal{G}, k^{(*)})$.

Norms and Traces.

If K/k is a field extension and $\alpha \in K$, then the k-vector space map

$$T_\alpha\colon K \to K \quad \textit{via} \quad T_\alpha(\lambda) = \alpha\lambda$$

has a trace and a determinant.

Definition 4.14 The *trace,* $\mathrm{tr}_{K/k}(\alpha)$*, of α from K to k* is the trace of T_α; the *norm,* $\mathcal{N}_{K/k}(\alpha)$*, of α from K to k* is $\det T_\alpha$.

The following three facts are extremely simple to prove and are left as (DX):

Fact I. $\mathrm{Tr}_{K/k}(\alpha)$ *is additive;* $\mathcal{N}_{K/k}(\alpha)$ *is multiplicative.*

Fact II. If $\alpha \in k$*, then*

$$\mathrm{Tr}_{K/k}(\alpha) = [K\colon k]\alpha \quad \textit{and} \quad \mathcal{N}_{K/k}(\alpha) = \alpha^{[K\colon k]}.$$

Fact III. If $L \supseteq K \supseteq k$*, then*

$$\mathrm{Tr}_{L/k}(\alpha) = \mathrm{Tr}_{K/k}(\mathrm{Tr}_{L/K}(\alpha)) \quad \textit{and} \quad \mathcal{N}_{L/k}(\alpha) = \mathcal{N}_{K/k}(\mathcal{N}_{L/K}(\alpha)).$$

Of course, from Facts II and III , we find

$$\mathrm{Tr}_{K/k}(\alpha) = [K\colon k(\alpha)]\mathrm{Tr}_{k(\alpha)/k}(\alpha) \quad \text{and} \quad \mathcal{N}_{K/k}(\alpha) = (\mathcal{N}_{k(\alpha)/k}(\alpha))^{[K\colon k(\alpha)]}.$$

When K/k is normal, more can be said. First, assume K/k is both normal and separable, then

$$\mathrm{Tr}_{K/k}(\alpha) = \sum_{\alpha\in\mathcal{G}(K/k)} (\sigma\alpha) \quad \text{and} \quad \mathcal{N}_{K/k}(\alpha) = \prod_{\alpha\in\mathcal{G}(K/k)} (\sigma\alpha).$$

Both of these statements are very easy corresponding to the fact that the roots of the characteristic polynomial of T_α are exactly the various $\sigma\alpha$ as σ ranges over $\mathcal{G}(K/k)$.

Now allow inseparability. We have

$$\mathcal{N}_{K/k}(\alpha) = \mathcal{N}_{K_{(*)}/k}(\mathcal{N}_{K/K_{(*)}}(\alpha)) = \mathcal{N}_{k^{(*)}/k}(\mathcal{N}_{K/k^{(*)}}(\alpha)).$$

Hence, we must first investigate $\mathcal{N}_{K/k}(\alpha)$ when K/k is purely inseparable. I claim the value of this norm is $\alpha^{[K\colon k]}$. To see this, observe that

$$\mathcal{N}_{K/k}(\alpha) = \mathcal{N}_{k(\alpha)/k}(\mathcal{N}_{K/k(\alpha)}(\alpha)) = \mathcal{N}_{k(\alpha)/k}(\alpha)^{[K\colon k(\alpha)]}. \tag{$\dagger$}$$

Now, the minimal and characteristic polynomials for T_α on the vector space $k(\alpha)$ are $X^q - c$, where $q = [k(\alpha)\colon k] = p^r$, and $c = \alpha^q$. Here, $p = \mathrm{char}(k)$. Therefore, the norm of α is $\det(T_\alpha) = c$ if p is odd and $-c = c$ if p is 2. Hence, $\mathcal{N}_{k(\alpha)/k}(\alpha) = \alpha^q = \alpha^{[k(\alpha)\colon k]}$. Put this together with ($\dagger$) above and obtain our claim. The general case now is

$$\mathcal{N}_{K/k}(\alpha) = \mathcal{N}_{K_{(*)}/k}(\alpha^{[K\colon k]_i}) = (\mathcal{N}_{K/k^{(*)}}(\alpha))^{[K\colon k]_i}.$$

Proposition 4.58 *(Original Form of Hilbert Theorem 90[5].) Suppose that* K/k *is normal and that* $K_{(*)}/k$ *is a cyclic extension. Then, a necessary and sufficient condition that* $\mathcal{N}_{K/k}(\alpha) = 1$ *is that there exists a* $\beta \in K_{(*)}$ *so that*

$$\alpha^{[K_{(*)}(\alpha)\colon K_{(*)}]} = \frac{\sigma\beta}{\beta}.$$

Here, σ *is an a priori chosen generator of* $\mathcal{G}(K_{(*)}/k)$*.*

Proof. This is merely the confluence of Propositions 4.56 and 4.57. If $\alpha \in K_{(*)}$, statements (b) and (c) of Proposition 4.56 and (2) of Proposition 4.57 give the statement that $\mathcal{N}_{K_{(*)}/k}(\alpha) = 1$ iff $\alpha = \sigma\beta/\beta$ for some $\beta \in K_{(*)}$. But, $\mathcal{N}_{K/k}(\alpha) = (\mathcal{N}_{K_{(*)}/k}(\alpha))^{[K\colon K_{(*)}]}$ in this case, and $[K\colon K_{(*)}]$ is a p-power. Therefore, $\mathcal{N}_{K/k}(\alpha) = 1$ iff $\mathcal{N}_{K_{(*)}/k}(\alpha) = 1$.

[5]Of course, Hilbert dealt only with the separable case.

Suppose now that $\alpha \in K$ yet $\alpha \notin K_{(*)}$. Then, $\alpha^{[K_{(*)}(\alpha)\colon K_{(*)}]}$ is in $K_{(*)}$. But,

$$\mathcal{N}_{K/k}(\alpha) = \mathcal{N}_{K_{(*)}/k}(\mathcal{N}_{K_{(*)}(\alpha)/K_{(*)}}(\alpha))^{[K\colon K_{(*)}]}.$$

As $[K\colon K_{(*)}]$ is a p-power, the left hand side is 1 iff $\mathcal{N}_{K_{(*)}/k}(\mathcal{N}_{K_{(*)}(\alpha)/K_{(*)}}(\alpha))$ is 1. By our remarks above, this last quantity is exactly $\mathcal{N}_{K_{(*)}/k}(\alpha^{[K_{(*)}(\alpha)\colon K_{(*)}]})$; so, we can apply the first part of the proof to the element $\alpha^{[K_{(*)}(\alpha)\colon K_{(*)}]}$, and we are done. □

It is not clear that β in Proposition 4.58 is of the form γ^q (where $q = [K_{(*)}(\alpha)\colon K_{(*)}]$), because in the proof of Proposition 4.57 part (2), the element λ may not be a qth power. If it proves to be so, then α would be $\sigma\gamma/\gamma$.

4.8 Krull's Galois Theory

In our treatment of Galois theory, the extensions were assumed finite. W. Krull discovered a natural way to treat (possibly) infinite algebraic extensions, His method leads to a non-trivial topology on the Galois group. We begin with the generalization of the extension lemma.

Theorem 4.59 *(General Extension Lemma) Suppose K/k is an algebraic extension and $\widetilde{k}$ is another field isomorphic to k via $\theta\colon k \to \widetilde{k}$. Let Γ be a field related to $\widetilde{k}$, but otherwise arbitrary. Then, there exists an algebraic extension, $\widetilde{K}/\widetilde{k}$, with $\widetilde{K} \underset{\text{rel}}{\sim} \Gamma$ and an extension of θ to an isomorphism $\widetilde{\theta}\colon K \to \widetilde{K}$.*

$$\begin{array}{ccccc} K & \xrightarrow{\widetilde{\theta}} & \widetilde{K} & \underset{\text{rel}}{\sim} & \Gamma \\ {\scriptstyle\text{alg}}\uparrow & & {\scriptstyle\text{alg}}\uparrow & & \| \\ k & \xrightarrow[\theta]{} & \widetilde{k} & \underset{\text{rel}}{\sim} & \Gamma \end{array}$$

Proof. This is a standard use of Zorn's lemma. We let

$$\mathcal{S} = \{(L, \varphi, \widetilde{L}) \mid L/k \text{ is algebraic, } \varphi \text{ extends } \theta \text{ and is an isomorphism } L \longrightarrow \widetilde{L} \text{ and } \widetilde{L} \underset{\text{rel}}{\sim} \Gamma\}.$$

Notice that the $\widetilde{L}$ in $\mathcal{S}$ are automatically algebraic over $\widetilde{k}$. We partially order $\mathcal{S}$ *via* the usual:

$$(L, \varphi, \widetilde{L}) \leq (M, \psi, \widetilde{M}) \quad \text{iff} \quad L \subseteq M;\ \widetilde{L} \subseteq \widetilde{M};\ \psi \restriction L = \varphi.$$

Of course, $\mathcal{S}$ is inductive; so, let $(L_0, \varphi_0, \widetilde{L}_0)$ be a maximal element of $\mathcal{S}$. Were $L_0 \neq K$, there would be some $\alpha \in K$ with $\alpha \notin L_0$. Then, the extension lemma for the finite extension $L_0(\alpha)/L_0$ would yield $(L_0(\alpha), \widetilde{\varphi}_0, \widetilde{L}_0)$ an element in $\mathcal{S}$ bigger that our maximal element—a contradiction. Therefore, $L_0 = K$. □

The material on splitting fields, etc. of Section 4.4 carries over provided no statement involving finiteness is used (e.g., statement (3) of Proposition 4.25 would be omitted in the general case that M/k was algebraic, not necessarily finite). The corollaries SMA, I and SMA II (Corollary 4.27 and Corollary 4.28) go over as does the existence of a normal closure.

Proposition 4.60 *Suppose K/k is an algebraic extension and write $\{K_\alpha/k \mid \alpha \in \Lambda\}$ for the family of sub-extensions of K/k of finite degree. Then, our family is a right mapping family in a natural way and we have*

$$K = \varinjlim_{\alpha} K_\alpha.$$

If K/k is normal, we may restrict the K_α/k to the finite normal extensions. Conversely, if $K = \varinjlim_{\alpha} K_\alpha$ and each K_α is normal over k, then so is K.

Proof. Of course, we define $\alpha \leq \beta$ (in Λ) when and only when $K_\alpha \subseteq K_\beta$ (everything takes place inside K). The map $K_\alpha \longrightarrow K_\beta$ is the inclusion. Since we have the inclusions $K_\alpha \hookrightarrow K$, consistent with the $K_\alpha \longrightarrow K_\beta$, we get the canonical homomorphism

$$\varinjlim_{\alpha} K_\alpha \longrightarrow K.$$

Choose $\xi \in K$. Then $k(\xi)$ is some K_α, and it is clear that $\xi \mapsto \text{can}_\alpha(\xi) \in \varinjlim_{\alpha} K_\alpha$ is well-defined and provides an inverse map to that above.

Of course, the family of finite normal extensions M_α/k is final in the family of all finite extensions provided K/k is itself normal. So, all we need prove is the last statement. We have $K = \varinjlim_{\alpha} K_\alpha$ and each

K_α is normal over k. If $\xi \in K$, there is an α so that $\xi \in K_\alpha$. Then all the k-conjugates of ξ lie in K_α; hence, they are in K. □

If Ω is an algebraic normal extension of K, then we consider the group $\mathrm{Aut}_k(\Omega)$. We topologize $\mathrm{Aut}_k(\Omega)$ by taking as a fundamental set of neighborhoods about 1 the subgroups of finite index in $\mathrm{Aut}_k(\Omega)$. Of course, it is the same to take the *normal* subgroups of finite index as our basic neighborhoods of $\{1\}$ in $\mathrm{Aut}_k(\Omega)$. (Remember: To get the neighborhoods about $\sigma \in \mathrm{Aut}_k(\Omega)$, we take the cosets σH, where the H are our neighborhoods about 1.) This renders $\mathrm{Aut}_k(\Omega)$ a Hausdorff topological group (use ordinary Galois Theory to see this) and it is this group *together with its topology* that we call the *Galois group of* Ω *over* k and denote by $\mathcal{G}(\Omega/k)$. The topology itself is the *Krull topology*.

Theorem 4.61 *The group $\mathcal{G} = \mathcal{G}(\Omega/k)$ is compact and totally disconnected in its Krull topology. In fact, we have $\mathcal{G}(\Omega/k) = \varprojlim_{\mathfrak{H}} \mathcal{G}/\mathfrak{H}$, where the left limit is taken over all open subgroups, $\mathfrak{H}$, of $\mathcal{G}$. Thus, $\mathcal{G}(\Omega/k)$ is a profinite group. Moreover, if we write $\Omega = \varinjlim_{\alpha} \Omega_\alpha$, where each Ω_α is a finite normal extension of k, then $\mathcal{G}(\Omega/k) = \varprojlim_{\alpha} \mathcal{G}(\Omega_\alpha/k)$.*

Proof. If $\sigma \in \mathcal{G}(\Omega/k)$ and Ω_α is one of the finite normal subextensions of Ω/k, then $\sigma \restriction \Omega_\alpha$ is in $\mathcal{G}(\Omega_\alpha/k)$. The maps $\pi_\alpha \colon \mathcal{G}(\Omega/k) \to \mathcal{G}(\Omega_\alpha/k)$ are consistent and hence we obtain the commutative diagram

$$\begin{array}{ccc} \mathcal{G}(\Omega/k) & \xrightarrow{\quad\varphi\quad} & \varprojlim_{\beta} \mathcal{G}(\Omega_\beta/k) \\ & {\scriptstyle \pi_\alpha} \searrow \quad \swarrow {\scriptstyle \mathrm{can}_\alpha} & \\ & \mathcal{G}(\Omega_\alpha/k) & \end{array}$$

If $\xi \in \varprojlim_{\beta} \mathcal{G}(\Omega_\beta/k)$, then ξ consists in a collection (ξ_β) where $\xi_\beta \in \mathcal{G}(\Omega_\beta/k)$ and when $k \subseteq \Omega_\beta \subseteq \Omega_\gamma$, we have $\xi_\gamma \restriction \Omega_\beta = \xi_\beta$. Since each $x \in \Omega$ lies in some finite normal extension of k, we have $x \in \Omega_\beta$ for various β. Then $\xi_\beta(x)$ is well-defined and our collection $(\xi_\beta) = \xi$ gives rise to an element of $\mathcal{G}(\Omega/k)$. Therefore we have a map

$$\varprojlim_{\beta} \mathcal{G}(\Omega_\beta/k) \xrightarrow{\psi} \mathcal{G}(\Omega/k)$$

plainly inverse to φ. Now, a neighborhood of 1 in $\varprojlim_{\beta} \mathcal{G}(\Omega_\beta/k)$ consists of those tuples (ξ_β) for which finitely many β are the identity and otherwise arbitrary (though consistent). Such tuples when restricted to the compositum of the Ω_β for which $\xi_\beta = 1$, are the identity on the compositum which is a field of finite degree over k, call it L. I claim $\mathcal{G}(\Omega/L)$ has finite index in $\mathcal{G}(\Omega/k)$. For L is normal and the usual argument shows $\mathcal{G}(\Omega/L) \lhd \mathcal{G}(\Omega/k)$. Moreover, SMA II (in its extended form) implies that $\mathcal{G}(\Omega/k) \longrightarrow \mathcal{G}(\Omega/L)$ is surjective. Hence, the exact sequence

$$0 \longrightarrow \mathcal{G}(\Omega/L) \longrightarrow \mathcal{G}(\Omega/k) \longrightarrow \mathcal{G}(L/k) \longrightarrow 0$$

gives the finite index assertion immediately. But then, we see that open neighborhoods of 1 in the Krull topology on $\mathcal{G}(\Omega/k)$ correspond to open neighnorhoods of 1 in the natural (product) topology on $\varprojlim_{\beta} \mathcal{G}(\Omega_\beta/k)$. Consequently, our maps φ and ψ are homeomorphisms.

Since $\mathcal{G}(\Omega_\beta/k)$ is compact, so is $\mathcal{G}(\Omega/k)$ in the Krull topology, and of course $\mathcal{G}(\Omega/k)$ is a profinite group. Every profinite group is totally disconnected (DX); so, $\mathcal{G}(\Omega/k)$ is totally disconnected.

That $\mathcal{G}$ is $\varprojlim_{\mathfrak{H}} \mathcal{G}/\mathfrak{H}$ as $\mathfrak{H}$ ranges over all open normal subgroups of $\mathcal{G}$ is the same kind of argument (remember that $\mathfrak{H}$ will be closed and of finite index). Or, it follows immediately from the next lemma whose proof is easy. □

Proposition 4.62 *Suppose $\mathcal{G}$ is a compact (Hausdorff) group and $\mathcal{G}_\alpha, \mathfrak{H}_\alpha$ are two families of closed subgroups with $\mathfrak{H}_\alpha \lhd \mathcal{G}_\alpha$ for every α. Assume that the indices $\alpha, \beta, \ldots$ form a directed set and that for every $\beta \geq \alpha$ we have $\mathcal{G}_\beta \subseteq \mathcal{G}_\alpha$ and $\mathfrak{H}_\beta \subseteq \mathfrak{H}_\alpha$. Then, the groups $\mathcal{G}_\alpha/\mathfrak{H}_\alpha$ form an inverse mapping family in a natural way and*

$$\varprojlim_\alpha \mathcal{G}_\alpha/\mathfrak{H}_\alpha = \bigcap_\alpha \mathcal{G}_\alpha \Big/ \bigcap_\alpha \mathfrak{H}_\alpha.$$

Using the same notations as in our treatment of standard Galois Theory, we can now extend the fundamental theorem to the general case. First of all, Lemma 4.33 and the material on Galois equivalence (between Lemma 4.33 and Theorem 4.38) go over word for word (together with no change in their proofs). So, here is the theorem.

Theorem 4.63 *(Fundamental Theorem of Galois Theory, General Case) If Ω/k is a normal (not necessarily finite) algebraic extension, then the mappings*

$$\begin{aligned} [L] &\mapsto \mathcal{G}(\Omega/L) \\ \mathcal{H} &\mapsto [\mathrm{Fix}(\mathcal{H})] \end{aligned}$$

establish a one-to-one order-inverting correspondence between Galois classes of extension fields of k and **closed** *subgroups of $\mathcal{G}(\Omega/k)$. In this correspondence:*

(a) $L^{(*)}$ is normal over k iff $L_{(*)}$ is normal over k iff $\mathcal{G}(\Omega/L)$ is a normal subgroup of $\mathcal{G}(\Omega/k)$.

(b) Under the conditions of (a), we have a natural exact sequence

$$0 \longrightarrow \mathcal{G}(\Omega/L) \longrightarrow \mathcal{G}(\Omega/k) \longrightarrow \mathcal{G}(L_{(*)}/k) \longrightarrow 0$$

of compact topological groups.

(c) A necessary and sufficient condition that $L_{(*)}$ be a finite extension of k is that $\mathcal{G}(\Omega/L)$ be an open subgroup of $\mathcal{G}(\Omega/k)$. In this case,

$$(\mathcal{G}(\Omega/k)\colon \mathcal{G}(\Omega/L)) = [L_{(*)}\colon k].$$

Proof. If $\alpha \in \Omega$, I claim $\{\sigma \mid \sigma(\alpha) = \alpha\}$ is an open (hence closed) subgroup of $\mathcal{G}(\Omega/k)$. Notice that if this claim is proved, then

$$\mathcal{G}(\Omega/L) = \{\sigma \mid (\forall \alpha \in L)(\sigma(\alpha) = \alpha)\} = \bigcap_{\alpha \in L} \{\sigma \mid \sigma(\alpha) = \alpha\}$$

is a closed subgroup. Now, $k(\alpha)$ has finite degree over k, so its normal closure, L, also has finite degree. In the proof of Theorem 4.61, we showed $\mathcal{G}(\Omega/L)$ has finite index in $\mathcal{G}(\Omega/k)$. But,

$$\mathcal{G}(\Omega/L) \subseteq \mathcal{G}(\Omega/k(\alpha)) \subseteq \mathcal{G}(\Omega/k)$$

and therefore $(\mathcal{G}(\Omega/k)\colon \mathcal{G}(\Omega/k(\alpha))) < \infty$. By definition of the Krull topology, the subgroup $\mathcal{G}(\Omega/k(\alpha))$ is open, as contended.

Next, just as in the usual (finite) case we see that $\mathcal{G}(\Omega/L^{(*)}) = \mathcal{G}(\Omega/L)$ and if $L = \mathrm{Fix}(\mathcal{G})$, then $L = L^{(*)}$. So, if we start with $[L]$, then we get $\mathcal{G}(\Omega/L)$ which is $\mathcal{G}(\Omega/L^{(*)})$. However, as mentioned, $\mathrm{Fix}(\mathcal{G}(\Omega/L^{(*)}))$ is $(L^{(*)})^{(*)} = L^{(*)}$ and so the correspondence inverts if we start from the field side.

Now take a *closed* subgroup $\mathfrak{H}$ and form $[\mathrm{Fix}(\mathfrak{H})]$. If $L = \mathrm{Fix}(\mathfrak{H})$, consider $\mathcal{G}(\Omega/L)$. Now $L = L^{(*)}$, so in what follows we consider only those subfields, M, of Ω/k with $M = M^{(*)}$. The Galois group don't change and all fields are now separable over the base field, $k^{(*)}$. For notation, drop all mention of "upper stars."'

We must show $\mathfrak{H} = \mathcal{G}(\Omega/L)$. We know $\mathfrak{H} \subseteq \mathcal{G}(\Omega/L)$ by definition of L. Observe that $\Omega = \varinjlim_{\alpha} K_\alpha$ for fields, K_α, finite and normal over k. We find as well that $L = \varinjlim_{\alpha} K_\alpha \cap L$. The Galois group $\mathcal{G}(\Omega/K_\alpha)$ is then an open, normal subgroup of $\mathcal{G}(\Omega/k)$ by definition of the Krull topology. Consider the subgroups $\mathfrak{H}\mathcal{G}(\Omega/K_\alpha)$, which contains $\mathfrak{H}$. I claim: $\mathrm{Fix}(\mathfrak{H}\mathcal{G}(\Omega/K_\alpha))$ is just $L\mathcal{K}_\alpha$. For, the elements of $\mathfrak{H}\mathcal{G}(\Omega/K_\alpha)$ are products $\sigma\tau$, where $\sigma \in \mathfrak{H}$ and $\tau \in \mathcal{G}(\Omega/K_\alpha)$. A ξ in $\mathrm{Fix}(\mathfrak{H}\mathcal{G}(\Omega/K_\alpha))$ satisfies $\sigma\tau(\xi) = \xi$, for all such σ and τ. In particular, when $\sigma = 1$, we find $\xi \in \mathrm{Fix}(\mathcal{G}(\Omega/K_\alpha) = K_\alpha$ (remember: $K_\alpha = K_\alpha^{(*)}$), and when $\tau = 1$, we find $\xi \in \mathrm{Fix}(\mathfrak{H}) = L$; hence, $\xi \in K_\alpha \cap L$. Conversely, if $\xi \in K_\alpha \cap L$ it is fixed by both $\mathfrak{H}$ and $\mathcal{G}(\Omega/K_\alpha)$; therefore, our cliam is proved. Then, we have the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{G}(\Omega/K_\alpha) & \longrightarrow & \mathcal{G}(\Omega/k) & \longrightarrow & \mathcal{G}(K_\alpha/k) & \longrightarrow & 0 \\
 & & \| & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathcal{G}(\Omega/K_\alpha) & \longrightarrow & \mathcal{G}(\Omega/K_\alpha \cap L) & \longrightarrow & \mathcal{G}(K_\alpha/K_\alpha \cap L) & \longrightarrow & 0,
\end{array}$$

and from it we see that $\mathfrak{H}\mathcal{G}(\Omega/K_\alpha)$ corresponds to a subgroup of $\mathcal{G}(K_\alpha/k)$, *via* $\mathfrak{H}\mathcal{G}(\Omega/K_\alpha) \mapsto \mathfrak{H}\mathcal{G}(\Omega/K_\alpha)/\mathcal{G}(\Omega/K_\alpha)$. But then, the lower line of our diagram and the finite case of ordinary Galois theory show that

$$\mathfrak{H}\mathcal{G}(\Omega/K_\alpha)/\mathcal{G}(\Omega/K_\alpha) \cong \mathcal{G}(K_\alpha/K_\alpha \cap L).$$

We pass these isomorphisms to the projective limit over α; on the left hand side, Lemma 4.62 implies that we get

$$\bigcap_\alpha \mathfrak{H}\mathcal{G}(\Omega/K_\alpha)/\bigcap_\alpha \mathcal{G}(\Omega/K_\alpha) = \bigcap_\alpha \mathfrak{H}\mathcal{G}(\Omega/K_\alpha)$$

while on the right hand side we get $\mathcal{G}(\Omega/L)$. But, $\bigcap_\alpha \mathfrak{H}\mathcal{G}(\Omega/K_\alpha)$ is the closure of $\mathfrak{H}$ and $\mathfrak{H}$ is already closed. Therefore, $\mathfrak{H} = \mathcal{G}(\Omega/L)$.

The proofs of assertions (a) and (b) are now just as they were in the finite case. As for (c), we know that $\mathcal{G}(\Omega/L_{(*)}) = \mathcal{G}(\Omega/L)$ and that this subgroup is of finite index in $\mathcal{G}(\Omega_{(*)}/k)$. We take, as in the proof above, a family of fields, K_α, of finite degree and normal over k so that $\varinjlim_{\alpha} K_\alpha = \Omega$. Then

$$(\mathcal{G}(K_\alpha/k)\colon \mathcal{G}(K_\alpha/K_\alpha \cap L_{(*)})) = [K_\alpha \cap L_{(*)}\colon k]$$

by usual Galois theory. Pass to the limit over α, observe that the left side tends to $(\mathcal{G}(\Omega/k)\colon \mathcal{G}(\Omega/L))$ and in fact is constant as soon as $K_\alpha \supseteq L_{(*)}$, and we get (c). □

We can now extend the notions and results of the previous section on Galois cohomology to the general (not necessarily finite) case. All that is necessary is to sprinkle the word "continuous" in the appropriate places and use some case. The group G will be a profinite group, for example $G = \mathcal{G}(\Omega/k)$. All modules will be given the discrete topology unless otherwise noted and our action $G \times M \longrightarrow M$ will be assumed continuous. This means that for $m \in M$, there is an *open* subgroup, U, of G so that $Um = m$. We define

$$C^n(G, M) = \{f\colon G^r \to M \mid f \quad \text{is continuous}\},$$

and use the usual formula for δ, thus δ is a continuous function ($C^r(G, M)$ inherits the discrete topology from M as G is compact). The continuity of the cochains shows up as follows: If $N \lhd G$ (N is, of course, closed), then M^N is a G/N-module. If $\widetilde{N} \subseteq N$ and $\widetilde{N} \lhd N$, then there are maps $G/\widetilde{N} \longrightarrow G/N$ and $M^N \longrightarrow N^{\widetilde{N}}$. The latter two combine to give a map

$$C^r(G/N, M^N) \longrightarrow C^r(G/\widetilde{N}, M^{\widetilde{N}})$$

called *inflation from G/N to $G/\widetilde{N}$*; it is injective. We have

Proposition 4.64 *For a continuous G-module, M, for the profinite group, G, the modules $C^r(G/U, M^U)$ form a right mapping system as U runs over the open normal subgroups of G—the map being inflation. We have*

$$C^r(G, M) = \varinjlim_U C^r(G/U, M^U),$$

and passing to cohomology, we also have

$$H^r(G, M) = \varinjlim_U H^r(G/U, M^U).$$

The proof of this is now routine and may be safely left to the reader (DX). The cohomological triviality of $\mathrm{Map}(G, B)$ (continuous functions, of course) expressed by Proposition 4.54 carries over and so does Proposition 4.57 (Hilbert Theorem 90).

4.9 Kummer Theory

In this section we consider base fields containing prescribed roots of unity. At first, we assume our base field contains a primitive mth root of unity. Notice that something mildly subtle is happening. We are not merely assuming all mth roots of 1 lie in k, for that would be true is $m = \text{char}(k) > 0$, yet there is *no* primitive mth root of unity in this case because 1 is the only mth root of unity when $m = \text{char}(k) > 0$. When a primitive mth root of 1 lies in k, then necessarily $(\text{char}(k), m) = 1$. (Else, $p = \text{char}(k) \mid m$ and $X^m - 1 = (X^q - 1)^p$, when $m = pq$. So each mth root of 1 is already a qth root of 1 with $q < m$, contradicting primitivity.)

Proposition 4.65 *Suppose the field k contains a primitive mth root of 1. A necessary and sufficient condition that K/k be a normal, separable extension whose Galois group is cyclic of order m is that $K = k(\beta)$ where the minimal k-polynomial for β is $X^m - b$.*

Proof. ($\Leftarrow$). We assume $K = k(\beta)$ and β is a root of the irreducible k-polynomial $X^m - b$. Write μ for a primitive mth root of 1 in k, then $1, \mu, \ldots, \mu^{m-1}$ are all the mth roots of 1, they are all distinct and lie in k. Of course, $(m, \text{char}(k)) = 1$ shows K/k is separable and $[K\colon k] = m$. Now, the elements

$$\beta, \mu\beta, \mu^2\beta, \ldots, \mu^{m-1}\beta$$

are all distinct and all are roots of $X^m - b$, therefore K is a splitting field of $X^m - b$; so, K/k is indeed normal. If we consider the k-isomorphism $k(\beta) \longrightarrow k(\mu\beta)$, we see (even without SMA, I) that it gives an element, σ, of $\mathcal{G}(K/k)$. The powers of σ operate on β *via*

$$\sigma^r(\beta) = \mu^r\beta$$

and so $1, \sigma, \ldots, \sigma^{m-1}$ are m distinct elements of $\mathcal{G}(K/k)$. They thereby exhaust $\mathcal{G}(K/k)$ and ($\Leftarrow$) is proved.

($\Rightarrow$). We suppose here that K/k is normal, separable and $\mathcal{G}(K/k)$ is cyclic of order $m = [K\colon k]$. Now we know $\mathcal{N}_{K/k}(\mu) = \mu^m = 1$, so we can apply the original form of Hilbert Theorem 90. We find there exists a $\beta \in K$ so that $\sigma\beta = \mu\beta$, where σ is a generator of $\mathcal{G}(K/k)$. Then, of course, $\sigma^r\beta = \mu^r\beta$, and so β is left fixed only by the trivial subgroup of $\mathcal{G}(K/k)$. By the fundamental theorem of Galois Theory, $k(\beta) = K$. The minimal k-polynomial of β is then

$$\prod_{r=0}^{m-1}(X - \sigma^r\beta) = \prod_{r=0}^{m-1}(X - \mu^r\beta).$$

On the other hand, if $b = \beta^m$, then each σ^r fixes b and each $\mu^r\beta$ is a root of $X^m - b$. The minimal polynomial for β and $X^m - b$ both have degree m; so it is clear the latter polynomial *is* the minimal polynomial for β. □

Corollary 4.66 *Suppose the field k contains a primitive mth root of 1. If n is any divisor of m, then*

(1) A n.a.s.c. that an extension K/k of degree n be normal with cyclic Galois group is that $K = k(\alpha)$ where the minimal polynomial of α is $X^n - a$.

(2) The k-polynomial $X^m - a$ is irreducible in $k[X]$ if and only if for all divisors, d, of m with $d > 1$, we have $a \notin k^{*d}$.

Proof. First, as $n \mid m$, we can write $m = nd$. Then for our primitive mth root of 1 in k, μ, the element μ^d is a primitive nth root of 1 in k and (1) is simply a restatement of Proposition 4.65 with n replacing m.

For statement (2), first consider $X^m - a$ and let α be a root in an overfield, Ω, of k. Write d for the smallest power of α lying in k. Then, the usual division algorithm argument shows that if $\alpha^q \in k$, we have $d \mid q$; in particular, $d \mid m$. I claim the polynomial $X^d - b$ is the minimal k-polynomial for α (here, $b = \alpha^d \in k$), in particular it is irreducible. To see this, let $f(X)$ be the minimal k-polynomial for α and have degree t.

Thus, $f(X) \mid (X^d - b)$ and $t \leq d$. Yet, the roots of $X^d - b$ are $\alpha, \zeta\alpha, \ldots, \zeta^{d-1}\alpha$, where $\zeta = \mu^n$ is a primitive dth root of 1. Thus,

$$f(X) = (X - \zeta^{i_1}\alpha) \cdots (X - \zeta^{i_t}\alpha)$$

and its constant term is therefore $\pm\Big(\prod_{l=1}^{t} \eta^{i_l}\Big)\alpha^t$. But then, $\alpha^t \in k$; so, $d \mid t$ and $t \leq d$. We find $t = d$ and $f(X) = X^d - b$.

Now if $a \notin k^{*q}$ for any $q \mid m$ with $q > 1$, then the smallest power of α to lies in k is the mth. Else, $\alpha^d \in k$ implies $dq = m$ (as above) and $a = \alpha^m = (\alpha^d)^q \in k^{*q}$ and $q > 1$ if $d < m$. By our claim, $X^m - a$ is irreducible in $k[X]$.

Finally, assume $X^m - a$ is irreducible. Were $a \in k^{*d}$ where $d \mid m$ and $d > 1$, then as $\alpha^m = a$, we have $(\alpha^q)^d = \beta^d$ for some $\beta \in k^*$. Therefore, $\alpha^q = z\beta$ for some z a dth root of 1 (hence, in k). It follows that the smallest power of α in k is, say, δ where $\delta \leq q < m$. Just as before, $\delta \mid m$ and $X^\delta - b$ is k-irreducible, where $b = \alpha^\delta$. Write $\delta r = m$ and look at $\alpha, \mu\alpha, \ldots, \mu^{r-1}\alpha$ (as usual μ is our primitive mth root of 1). Each of these elements has δth power in k and δ is minimal. Set $\zeta = \mu^\delta$, then $X^\delta - \zeta^i b$ is the minimal k-polynomial for $\mu^i\alpha$ by our claim above. But,

$$X^m - a = (X^\delta - b)(X^\delta - \zeta b) \cdots (X^\delta - \zeta^{r-1} b),$$

contradicting the irreducibility of $X^m - a$. □

An important part of the proof above should be isolated and recorded:

Corollary 4.67 *If k contains a primitive mth root of 1 and K is an overfield of k, then given $\alpha \in K$ with $\alpha^m \in k^*$, the minimal k-polynomial for α is $X^d - \alpha^d$, where d is the smallest positive integer so that $\alpha^d \in k$. In fact, $d \mid m$.*

Now, we can make an obvious attempt to "classify" the cyclic overfields of degree n ($n \mid m$) of k when k possesses a primitive mth root of 1. Namely, such a K is $k(\alpha)$ and we could send α to $\overline{\alpha^n}$ where $\overline{\alpha^n}$ is the image of α^n in k^*/k^{*n}. But, α is not unique and its choice depends on μ and σ (a generator of $\mathcal{G}(K/k)$). There is a better way:

Theorem 4.68 *(Kummer) Suppose k is a field possessing a primitive mth root of 1. Write Ω for the maximal, abelian, m-torsion extension of k and denote by $\mathcal{G}$ its (Krull topologized) Galois group. Then there is a natural continuous pairing*

$$\mathcal{G} \prod k^*/k^{*m} \longrightarrow \mu_m \,(=\ m\text{th root of } 1),$$

and it makes $\mathcal{G}$ the Pontrjagin dual of k^*/k^{*m}.

Proof. Choose $\sigma \in \mathcal{G}$ and $\overline{a} \in k^*/k^{*m}$. Lift $\overline{a}$ to some $a \in k^*$ and take an mth root of a in an overfield, call it α. We know that $K = k(\alpha)$ is cyclic of degree d and $d \mid m$ by our above propositions. So, $K \subseteq \Omega$ (we fix an algebraic closure of k and work inside it) and $\sigma\alpha$ makes sense. We set

$$(\sigma, \overline{a}) = \frac{\sigma\alpha}{\alpha}.$$

Note that

$$\Big(\frac{\sigma\alpha}{\alpha}\Big)^m = \frac{\sigma(\alpha^m)}{\alpha^m} = \frac{\alpha^m}{\alpha^m} = 1,$$

therefore $(\sigma, \overline{a}) \in \mu_m$. Let's check that $(\sigma, \overline{a})$ is well-defined. First, if we change the mth root of a we get $\zeta\alpha$ where ζ is some mth root of 1 (hence, $\zeta \in k^*$). Then

$$\frac{\sigma(\zeta\alpha)}{\zeta\alpha} = \frac{\sigma\alpha}{\alpha},$$

so there is no problem with the choice of α. If we lift $\overline{a}$ to some $b \in k^*$, then $b = \lambda^m a$ for some $\lambda \in k^*$. Thus, β, an mth root of b is $\zeta\lambda\alpha$ for some ζ as above. Once again,

$$\frac{\sigma\beta}{\beta} = \frac{\sigma(\zeta\lambda\alpha)}{\zeta\lambda\alpha} = \frac{\sigma\alpha}{\alpha},$$

and so $(\sigma, \overline{a})$ is a well -defined mth root of 1.

It is easy to see that $(\sigma, \overline{a})$ is bi-multiplicative (DX), so assume $(\sigma, \overline{a}) = 1$ for all $\sigma \in \mathcal{G}$. If a lifts $\overline{a}$ and $a \notin k^{*m}$ (i.e., $\overline{a} \neq 1$) then $K = k(\alpha)$ is a non-trivial cyclic degree d extension of k and $d \mid m$. But then, a generator, τ, of $\mathcal{G}(K/k)$ comes from some $\sigma \in \mathcal{G}$ and $\sigma\alpha = \tau\alpha = \zeta\alpha$ (some dth root of 1, say $\zeta \neq 1$). Hence, $(\sigma, \overline{a}) = \zeta \neq 1$, a contradiction. Therefore, $(\sigma, \overline{a})$ is non-degenerate on the right.

If $(\sigma, \overline{a}) = 1$ for all $\overline{a} \in k^*/k^{*m}$, then I claim σ must be 1. For, notice that when K/k is finite normal ($K \subseteq \Omega$), then $\mathcal{G}(K/k)$ is an abelian m-torsion group. Hence, $\mathcal{G}(K/k)$ is a product of various $\mathbb{Z}/d\mathbb{Z}$, where each $d \mid m$. This means that K is generated as a field by elements, α, for which $k(\alpha)$ is a cyclic extension of k. As K is arbitrary, it follows immediately that Ω is a field generated by such elements α. However, Proposition 4.65 and our assumption $(\sigma, \overline{a}) = 1$ (all $\overline{a}$), now yield $\sigma\alpha = \alpha$ for all the α's generating Ω. Thus, $\sigma = 1$, as claimed.

Lastly continuity of $\langle \sigma, \overline{a} \rangle \mapsto (\sigma, \overline{a})$ follows because on the entire open subgroup $\mathcal{G}(\Omega/k(\alpha))$ the pairing $\langle -, \overline{a} \rangle \mapsto (-, \overline{a})$ is identically 1. Here, α is, of course, an mth root of a. The product $\mathcal{G}(\Omega/k(\sigma)) \prod \{\overline{a}\}$ is an open neighborhood of 1 in $\mathcal{G}(\Omega/k) \prod k^*/k^{*m}$. □

Corollary 4.69 *Under the assumptions and notations of Theorem 4.68, there is a one-to-one correspondence between subgroups, S, of k^*/k^{*m} and sub-extensions K/k of Ω/k. It is given by*

$$S \longleftrightarrow K = k(S^{1/m}).$$

In all the foregoing, m was relatively prime to $\mathrm{char}(k) = p > 0$. What happens if $p \mid m$? Of course, we can factor m as $p^r\widetilde{m}$ with $(\widetilde{m}, p) = 1$. It's not hard to see that the case for this breaks up into the p^r case and the previous case. So, we'll assume $m = p^r$. Here, we will use the additive part of Hilbert 90 and the isomorphism $(\mathrm{Ker}\ \mathrm{Tr}_{K/k})/I_{K/k}K^+ \cong H^1(K/k, K^+)$ in case $\mathcal{G}(K/k)$ is cyclic.

So, assume K/k is a cyclic extension of degree p^r; choose a generator, σ, of $\mathcal{G}(K/k)$. For the element $1 \in k^+$, we have $\mathrm{Tr}_{K/k}(1) = [K\colon k] \cdot 1 = 0$, so there exists $\theta \in K^+$ with

$$\sigma(\theta) - \theta = 1, \quad \text{i.e.,} \quad \sigma(\theta) = \theta + 1.$$

The action of the Galois group on θ is given by

$$\sigma^i(\theta) = \theta + 1 \qquad 0 \leq i \leq p^r - 1.$$

Observe that only $\theta, \theta + 1, \ldots, \theta + (p-1)$ are distinct, after that we repeat these in order. Thus, the polynomial

$$g(X) = (X - \theta)(X - (\theta + 1)) \cdots (X - (\theta + (p-1)))$$

is the minimal k-polynomial for θ and $L = k(\theta)$ is a cyclic p-extension. The only case when $K = L$ is when $r = 1$; so, *from now on we'll assume K/k is cyclic of degree p.* Hence, $K = k(\theta)$ and $\sigma(\theta) = \theta + 1$. We can compute the minimal polynomial $g(X)$ as follows: Write $Y = X - \theta$, then $g(X) = Y(Y-1)(Y-2)\cdots(Y-(p-1))$. But, the elements $1, 2, \ldots, p-1$ are the $(p-1)$st roots of unity (and lie in $\mathbb{F}_p$, the prime field), therefore

$$g(X) = Y(Y^{p-1} - 1) = Y^p - Y = X^p - X - (\theta^p - \theta).$$

If we write $\wp(\theta) = \theta^p - \theta$, then we've proved the first part of

Theorem 4.70 *(E. Artin & O. Schreier, 1929) If k is a field of characteristic $p > 0$, then every cyclic p-extension, K/k, has the form $K = k(\theta)$ where $\wp(\theta) = \theta^p - \theta$ lies in k and the Galois group, $\mathcal{G}$, acts by a (prechosen) generator, σ, taking θ to $\theta + 1$. The minimal k-polynomial for θ is $X^p - X - \wp(\theta)$. Conversely, the polynomial $X^p - X - a$ is k-irreducible when and only when $a \notin \wp(k^+)$. If it is irreducible and θ is a root, then $k(\theta)$ is a normal, separable, cyclic p-extension of k.*

Proof. If $a \in \wp(k)$ so that $a = b^p - b$ for some $b \in k$, then

$$(X - b)(X - (b + 1)) \cdots (X - (b + (p - 1))$$

is exactly $X^p - X - \wp(b) = X^p - X - a$; so, our polynomial splits in $k[X]$.

If $a \notin \wp(k^+)$, the polynomial $X^p - X - a$ has no root in k. Adjoin a root to k, we get an extension $K = k(\theta)$. Now, $\theta^p - \theta = a$, so $(\theta + i)^p - (\theta + i) = a$, too, where $0 \leq i \leq p - 1$. Therefore, all the roots of $X^p - X - a$ lie in K and K is a normal extension. But the roots of $X^p - X - a$ are all distinct, therefore $X^p - X - a$ is separable and we find that K/k is a normal, separable extension.

If d is the degree of θ over k, then $\theta, \theta + i_2, \ldots, \theta + i_d$ are the roots of its minimal k-polynomial. Were $d \neq p$, there would be an integer, j, so that $\theta + j$ is not a root of the minimal k-polynomial for θ. Yet, $k(\theta + j) = k(\theta)$, so $\theta + j$ also has degree d over k and $\theta + j, \theta + j_2, \ldots, \theta + j_d$ are all the conjugates of $\theta + j$ and all distinct from each $\theta + i_l$. Continue in this way, we find the p roots $\theta, \theta + 1, \ldots, \theta + (p - 1)$ partition themselves into t blocks of d elements each. But then, $dt = p$ and p is prime. As $\theta \notin k$, we have $d > 1$ therefore $d = p$ and so $X^p - X - a$ is indeed irreducible. □

The analog of Kummer's theorem is

Theorem 4.71 *(E. Artin & O. Schreier) Suppose k is a field of characteristic $p > 0$ and write Ω for the maximal, abelian, p-torsion extension of k. If $\mathcal{G} = \mathcal{G}(\Omega/k)$ is the Galois group of Ω/k (with Krull topology), then there is a natural continuous pairing*

$$\mathcal{G} \prod k^+/\wp(k^+) \longrightarrow \mathbb{Z}/p\mathbb{Z} \ (\subseteq \mathbb{R}/\mathbb{Z})$$

and it makes $\mathcal{G}$ the Pontrjagin dual of $k^+/\wp(k^+)$.

Proof. Pick $\sigma \in \mathcal{G}$ and $\overline{a} \in k^+/\wp(k^+)$. Lift $\overline{a}$ to some $a \in k^+$ and let $\theta \in \overline{k}$ be a root of $X^p - X - a$. Define

$$(\sigma, \overline{a}) = \sigma\theta - \theta.$$

Note that unless $\overline{a} = 0$, the field $k(\theta)$ has degree p over k and is normal, separable cyclic. If $\overline{a} = 0$, then $\theta \in k$. Therfore, $k(\theta)$ is contained in Ω and $\sigma\theta$ makes sense. Now $\sigma\theta$ is a root of $X^p - X - a$ and so $\sigma\theta = \theta + j$ for some $j \in \mathbb{Z}/p\mathbb{Z}$; therefore, $(\sigma, \overline{a})$ is indeed in $\mathbb{Z}/p\mathbb{Z}$.

As in the proof of Kummer's theorem, $\langle \sigma, \overline{a} \rangle \mapsto (\sigma, \overline{a})$ is a pairing of the groups $\mathcal{G}(\Omega/k)$ and $k^+/\wp(k^+)$. Just as in the proof of that theorem, the field Ω is generated by the various θ's as above; so, if $(\sigma, \overline{a}) = 0$ for all $\overline{a}$, we find σ fixes all the θ's and thereby $\sigma = 1$. If $(\sigma, \overline{a}) = 0$ for all $\sigma \in \mathcal{G}(\Omega/k)$, then $\overline{a}$ must be 0 else the polynomial $X^p - X - a$ would be irreducible (Theorem 4.70) and $k(\theta)$, where θ is one of its roots, would be a cyclic p-extension. Then, $\sigma\theta = \theta + 1$ for some $\sigma \in \mathcal{G}(k(\theta)/k)$ and upon lifting σ to $\mathcal{G}(\Omega/k)$ we'd get $(\sigma, \overline{a}) \neq 0$, a contradiction.

Continuity is proved exactly as in Kummer's theorem, the open neighborhood on which $(\sigma, \overline{a})$ vanishes being $\mathcal{G}(\Omega/k(\theta)) \prod \{\overline{a}\}$. □

Corollary 4.72 *If* $\mathrm{char}(k) = p > 0$ *there is a one-to-one correspondence between subgroups, T, of $k^+/\wp(k^+)$ and p-torsion, abelian overfields of k. It is given by*

$$T \longleftrightarrow K = k(\wp^{-1}(T)).$$

What happens for p^r, $r > 1$? Here, the situation is sufficiently complicated that the solution had to wait until 1937. Then E. Witt introduced a ring, $W(k)$, called the ring of *Witt vectors over* k and he proved that even if $\mathrm{char}(k) = p > 0$, the ring $W(k)$ is an integral domain of characteristic 0. Now, it turns out that

$$W(k) = \varprojlim_n W_n(k),$$

where the $W_n(k)$ are "truncated" Witt vector rings. There is a map $F\colon W_n^n(k) \to W_n(k)$ playing the role of $\xi \mapsto \xi^p$ and one gets $\wp = F - \mathrm{id}$. When $n = 1$, the ring $W_1(k)$ is just k, and the exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow k^+ \xrightarrow{\wp} \wp(k^+) \longrightarrow 0$$

becomes an exact sequence

$$0 \longrightarrow \mathbb{Z}/p^r\mathbb{Z} \longrightarrow W_r(k)^+ \xrightarrow{\wp} \wp(W_r(k)^+) \longrightarrow 0,$$

in the general case. It then turns out that if Ω is the maximal, abelian p^r-torsion extension of k, the Galois group, $\mathcal{G}(\Omega/k)$, is naturally Pontrjagin dual to $W_n(k)/\wp(W_n(k))$ by a pairing similar to the Artin-Schreier pairing. See Witt [49] for the details.

4.10 An Amazing Theorem of Galois Theory

Question: If k is a field with $k \neq \overline{k}$, when is $[\overline{k}\colon k]$ finite?

An example: $k = \mathbb{R}$; $K = \mathbb{C} = \mathbb{R}(i)$.

The answer of our question depends on an irreducibility criterion:

Theorem 4.73 *(Artin's Irreducibility Criterion) Given a field, k, consider the polynomial $X^n - a$, where $a \in k^*$. If p is prime and p divides n, assume $a \notin (k^*)^p$. If $4 \mid n$, then assume as well that $a \notin (-4(k^*)^4)$. Under these conditions, $X^n - a$ is irreducible in $k[X]$.*

We will assume this theorem for the moment, and based on it we can prove

Theorem 4.74 *(Artin) Say k is a field, $\overline{k}$ is an algebraic closure of k and $1 < [\overline{k}\colon k] < \infty$. Then we have:*

(1) $\overline{k} = k(i) \quad (i^2 = -1)$.

(2) $\mathrm{char}(k) = 0$.

Proof. We claim that $\overline{k}/k$ is separable.

If not, let $\overline{k}_{(*)} = L$, then $\overline{L}/L$ is purely inseparable and $\overline{k} \neq L$. So, $L \neq L^p$ implies that there is $a \notin L^p$ (where $p = \mathrm{char}(k)$). We know $X^{p^n} - a$ is irreducible in $L[X]$ implies that L has extensions of degree p^n, for all n; yet, all these extensions are contained in $\overline{k}$, a contradiction.

Look at $k(i) \subseteq \overline{k}$; as $\overline{k}/k$ is separable, $\overline{k}/k(i)$ is normal, separable. Let $\mathcal{G} = \mathcal{G}(\overline{k}/k(i))$. We need to show that $\#(\mathcal{G}) = 1$.

Pick a prime, p, with $p \mid \#(\mathcal{G})$; let $\mathcal{H}$ be the subgroup of $\mathcal{G}$ of order p and write $L = \mathrm{Fix}(\mathcal{H})$.

Step 1. $p \neq \mathrm{char}(k)$.

If $p = \mathrm{char}(k)$, then, by separability, there is some $\beta \in \overline{k}$ so that $\mathrm{tr}_{\overline{k}/L}(\beta) = 1$. We know that M/L is separable iff the bilinear form

$$(u, v) \mapsto \mathrm{tr}_{M/L}(uv)$$

is non-degenerate on the vector space M over the field L. Now, there is $\widetilde{\beta}$ so that $\mathrm{tr}_{\overline{k}/L}(1 \cdot \widetilde{\beta}) \neq 0$. Let $\lambda = \mathrm{tr}(\widetilde{\beta}) \in L$ and form $\beta = (1/\lambda)\widetilde{\beta}$. Then, we have

$$\mathrm{tr}_{\overline{k}/L}(\beta) = (1/\lambda)\mathrm{tr}_{\overline{k}/L}(\widetilde{\beta}) = \lambda/\lambda = 1.$$

As the trace is a sum and

$$\mathrm{tr}(\beta^p) = \mathrm{tr}(\beta)^p \quad (p = \mathrm{char}(k)),$$

we get $\mathrm{tr}_{\overline{k}/L}(\beta^p - \beta) = 0$. Our extension $\overline{k}/L$ is cyclic of degree p, say σ is a generator of $\mathcal{H}$. Note that for every $\xi \in \overline{k}$, we have

$$\mathrm{tr}_{\overline{k}/L}(\xi) = \mathrm{tr}_{\overline{k}/L}(\sigma\xi),$$

so $\mathrm{tr}_{\overline{k}/L}(\sigma\xi - \xi) = 0$. By "Additive Hilbert 90", every element of zero trace in $\overline{k}$ has the form $(\sigma\gamma - \gamma)$, for some $\gamma \in \overline{k}$. As $\mathrm{tr}_{\overline{k}/L}(\sigma\xi - \xi) = 0$, there is some $\gamma \in \overline{k}$ so that $\beta^p - \beta = \sigma\gamma - \gamma$. Now, the polynomial $X^p - X - \gamma \in \overline{k}[X]$ has a root in $\overline{k}$, as $\overline{k}$ is algebraically closed. Say $\alpha \in \overline{k}$ is such a root, then $\gamma = \alpha^p - \alpha$. We have

$$\beta^p - \beta = \sigma(\alpha^p - \alpha) - (\alpha^p - \alpha) = \sigma(\alpha)^p - \alpha^p - (\sigma(\alpha) - \alpha),$$

and so

$$\sigma(\alpha) - \alpha - \beta = \sigma(\alpha)^p - \alpha^p - \beta^p = (\sigma(\alpha) - \alpha - \beta)^p.$$

Consequently, $\sigma(\alpha) - \alpha - \beta \in \mathbb{F}_p$, call it ν. It follows that $\sigma(\alpha) - \alpha = \beta + \nu$. Taking $\mathrm{tr}_{\overline{k}/L}$ on both sides, we get

$$0 = \mathrm{tr}_{\overline{k}/L}(\beta) + \mathrm{tr}_{\overline{k}/L}(\nu) = 1 + \mathrm{tr}_{\overline{k}/L}(\nu).$$

As $\nu \in \mathbb{F}_p \subseteq L$, we have

$$\mathrm{tr}_{\overline{k}/L}(\nu) = [\overline{k}\colon L]\nu = p\nu = 0,$$

which implies that $0 = 1 + 0 = 1$, a contradiction. Therefore, $\mathrm{char}(k) \neq p$, as claimed.

Step 2. L does not exist, i.e., as no p divides $\#(\mathcal{G})$, we have $\#(\mathcal{G}) = 1$; thus, $\overline{k} = k(i)$.

We claim that $[\overline{k}\colon L] = p$. Adjoin to L a p-th root of unity, say ζ is such a primitive root. Then, $[\overline{k}\colon L(\zeta)] \mid p$; so, $[L(\zeta)\colon L]$ also divides p. But, $L(\zeta)/L$ has degree at most $p-1$. Indeed,

$$X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1),$$

so $L(\zeta) = L$ already, i.e., $\zeta \in L$ and it follows that $[\overline{k}\colon L] = p$. As L has the p-th roots of unity, by Kummer's theorem (Theorem 4.65), we know $\overline{k} = l(\alpha)$, where α is a root of $X^p - a$, with $a \notin (L^*)^p$. But, if p is odd, the Artin irreducibility criterion implies that $X^{p^l} - a$ is also irreducible for all $l \geq 1$, so $[\overline{k}\colon L] \geq p^l$, for all $l \geq 1$, a contradiction. Therefore, we must have $p = 2$. Now, our situation is

(a) $\overline{k} = L(\alpha)$, where α is a root of $X^2 - a$, with $a \notin (L^*)^2$.

(b) $i \in k \subseteq L$.

Since $X^{2^r} - a$ cannot be irreducible for all $r \geq 0$, since otherwise we would have $[\overline{k}\colon K] \geq 2^r$ for all $r \geq 0$, it must be that $a \in (-4(L^*)^4)$ (by Artin's irreducibility). Thus, $a = -4b^4$, for some $b \in L^*$; it follows that $\alpha = \sqrt{a} = \pm 2ib^2$. As $2, i, b \in L$, we deduce that $\alpha \in L$, a contradiction. Therefore, $\#(\mathcal{G}) = 1$.

Step 3. $\mathrm{char}(k) = 0$.

If not, then say $q = \mathrm{char}(k)$ and write $\mathbb{F}_q$ for the prime field of k. Pick $r >> 0$, adjoin to $\mathbb{F}_q$ a primitive 2^r-th root of unity, call it ζ. Apply natural irrationalities to the picture show in Figure 4.2:

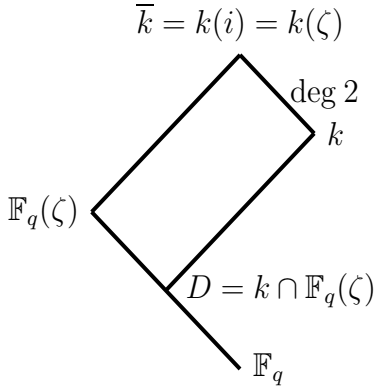


Figure 4.2: The Extension $\overline{k}/\mathbb{F}_q$

If σ is the generator of $\mathcal{G}(\overline{k}/k) = \mathbb{Z}/2\mathbb{Z}$, then $\sigma \restriction \mathbb{F}_q(\zeta)$ yields an automorphism and we know

$$\mathcal{G}(\overline{k}/k) \cong \mathcal{G}(\mathbb{F}_q(\zeta)/D) \hookrightarrow \mathcal{G}(\mathbb{F}_q(\zeta)/\mathbb{F}_q).$$

The extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$ is *cyclic* of degree 2^s, where s is the order of the image of q in $(\mathbb{Z}/2^r\mathbb{Z})^*$. As a cyclic group has a unique subgroup of every possible order, there is a unique subfield of degree 2 in the extension $\mathbb{F}_q(\zeta)/\mathbb{F}_q$. If $\mathbb{F}_q < D$, then D contains this unique extension. But, $\mathbb{F}_q(i)$ has degree 1 or 2 over $\mathbb{F}_q$, so $\mathbb{F}_q(i) \subseteq D$, which yields $i \in D$, and finally, $i \in k$ ($D = k \cap \mathbb{F}_q(\zeta)$). Thus, $\overline{k} = k$, a contradiction. (Note: i is a fourth root of unity; so, as $\overline{k} \neq k$, we have $\text{char}(k) = q \neq 2$). Therefore, $D = \mathbb{F}_q$.

Now,

$$\mathbb{Z}/2\mathbb{Z} = \mathcal{G}(\overline{k}/k) = \mathcal{G}(\mathbb{F}_q(\zeta)/\mathbb{F}_q),$$

a group of order 2^s. If we let r tend to ∞, then s tends to ∞, a contradiction. Therefore, $\text{char}(k) = 0$. □

Finally, here the proof of Theorem 4.73:

Proof of Artin's Irreducibility Criterion. Assume at first that we know the result for n a prime power–here is how to prove the general case: Use induction on the number of primes dividing n. If $n = p^r m$ with $(p, m) = 1$, we may assume p is odd. Now, $X^m - a$ is irreducible by our induction hypothesis; let $\alpha_1, \ldots, \alpha_m$ be its roots. Then,

$$X^m - a = \prod_{j=1}^{m} (X - \alpha_j)$$

and

$$X^n - a = (X^{p^r})^m - a = \prod_{j=1}^{m} (X^{p^r} - \alpha_j).$$

Suppose for some j that α_j is a pth power in $k(\alpha_j)$. Now $X^m - a$ is irreducible so its Galois group acts transitively on its roots. Therefore, each α_i is $\sigma(\alpha_j)$ for some σ and so each of the α_i is a pth power in $k(\alpha_i)$. There exist $\beta_i \in k(\alpha_i)$ with $\beta_i^p = \alpha_i$ for $i = 1, \ldots, m$. We find that

$$\mathcal{N}_{k(\alpha_i)/k}(\alpha_i) = \mathcal{N}_{k(\alpha_i)/k}(\beta_i)^p.$$

But,

$$\prod_{j=1}^{m} \alpha_j = (-1)^{m+1} a = \mathcal{N}_{k(\alpha_i)/k}(\alpha_i) = \mathcal{N}_{k(\alpha_i)/k}(\beta_i)^p.$$

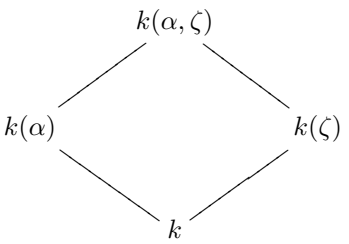
If m is odd, this gives $a \in k^{*p}$, contrary our assumptions. If m is even, then $a = -(\mathcal{N}_{k(\alpha_i)/k}(\beta_i)^p)$. But, p is odd so

$$a = (-\mathcal{N}_{k(\alpha_i)/k}(\beta_i))^p,$$

again contrary to hypothesis. We conclude that none of the α_i are pth powers in the field $k(\alpha_i)$. By the one prime case, the polynomials $X^{p^r} - \alpha_i$ are irreducible for $i = 1, \ldots, m$ and all r.

Let ξ be a root of $X^n - a$. Then, ξ satisfies $X^{p^r} - \alpha_j = 0$ for at least one j. According to the irreducibility of $X^{p^r} - \alpha_j$, we find that $[k(\xi)\colon k(\alpha_j)] = p^r$ (of course $k(\alpha_j) \subseteq k(\xi)$). However, $[k(\alpha_j)\colon k] = m$ by the induction hypothesis and so $[k(\xi)\colon k] = n$. But this means the minimal polynomial for ξ has degree n and ξ *is* a root of $X^n - a$; so, $X^n - a$ is irreducible.

We've achieved a reduction to the heart of the matter, the one prime case. Here, $n = p^r$ and when $p = \text{char}(k)$ we already know the result. Therefore, we may and do assume $p \neq \text{char}(k)$. Now use induction on r. Say $r = 1$, adjoin the pth roots of 1 to k—call ζ a primitive pth root of 1:



Here, α is a root of $X^p - a$. Were $[k(\alpha)\colon k] \neq p$, i.e., were $X^p - a$ reducible, we would have $[k(\alpha,\zeta)\colon k(\zeta)] < p$. Now over $k(\zeta)$, the Galois group of $X^p - a$ is cyclic of order p or trivial according as $a \notin k(\zeta)^p$ or $a \in k(\zeta)^p$. We then would have $a \in k(\zeta)^p$; hence $\alpha \in k(\zeta)$. We know that $[k(\zeta)\colon k] = r \leq p-1$ and so, $(r,p) = 1$. Write $1 = sr + tp$, for some s, t. Now,

$$a^r = \mathcal{N}_{k(\zeta)/k}(a) = \mathcal{N}_{k(\zeta)/k}(\alpha)^p.$$

But,

$$a = a^{sr+tp} = \mathcal{N}_{k(\zeta)/k}(\alpha)^{ps} a^{pt} = (\mathcal{N}_{k(\zeta)/k}(\alpha)^p \cdot a^t)^p \in k^{*p},$$

a contradiction. We conclude $X^p - a$ is irreducible.

Induction Step. Consider $X^{p^r} - a$ and assume p is *odd*. Write α for a root of $X^p - a$, and further write $\prod_{j=1}^{p}(X - \alpha_j) = X^p - a$, with $\alpha = \alpha_1$. Now α is not a pth power in $k(\alpha)$. For, if it were β^p, then

$$a = (-1)^{p+1}a = \mathcal{N}_{k(\zeta)/k}(\alpha) = \mathcal{N}_{k(\zeta)/k}(\beta)^p \qquad (p \text{ is odd})$$

contrary to the hypothesis that a is not a pth power. Again by transitivity of the Galois group on the α_j, no α_j is a pth power in $k(\alpha_j)$, and therefore, by induction all the polynomials

$$X^{p^{r-1}} - \alpha_j, \quad j = 1, 2, \ldots, p$$

are irreducible (over $k(\alpha_j)$). If ξ is a root of $X^{p^r} - a$, then ξ is a root of $X^{p^{r-1}} - \alpha_j$ for some j, and as before

$$[k(\xi)\colon k(\alpha_j)] = p^{r-1} \quad \text{and} \quad [k(\alpha_j)\colon k] = p;$$

so, $[k(\xi)\colon k] = p^r$. We conclude $X^{p^r} - a$ is indeed irreducible.

Finally, we have the case $p = 2$. We know $X^2 - a$ is irreducible, we must prove $X^{2^r} - a$ is irreducible. As usual and with familiar notation, we have

$$X^{2^r} - a = \prod_{j=1}^{2}(X^{2^{r-1}} - \alpha_j); \quad \alpha = \alpha_1; \quad \alpha^2 = a.$$

So, if $X^{2^{r-1}} - \alpha_j$ is irreducible for $j = 1, 2$, the usual degree argument will show $X^{2^r} - a$ is irreducible. The only way $X^{2^{r-1}} - \alpha_j$ will be reducible, by the induction hypothesis, is if $\alpha_j \in k(\alpha_j)^{*2}$ or $\alpha_j \in -4k(\alpha_j)^{*4}$. We will show each of these is untenable.

(1) Say $\alpha = \alpha_1 = \beta^2$ with $\beta \in k(\alpha)^*$; so, the same is true of α_2. Now,

$$-a = \mathcal{N}_{k(\alpha)/k}(\alpha) = \mathcal{N}_{k(\alpha)/k}(\beta)^2 = b^2$$

yet $a \notin k^{*2}$, so $(-1) \notin k^{*2}$. Hence, $i \notin k$ and we factor $X^{2^r} - a$ over $k(i)$:

$$X^{2^r} - a = X^{2^r} + b^2 = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib).$$

If, on the right hand side, one of the factors is reducible, the induction hypothesis shows ib (or $-ib$) $\in k(i)^{*2}$ or ib (or $-ib$) $\in -4k(i)^{*4}$. Since -4 is square in $k(i)$, the cases $ib \in -4k(i)^{*4}$ or $-ib \in -4k(i)^{*4}$ reduce respectively to $ib \in k(i)^{*2}$ or -$ib \in k(i)^{*2}$. But -1 is also a square, so these two cases are just the one case: $ib \in k(i)^{*2}$.

Write $ib = (\gamma + i\delta)^2$, with $\gamma, \delta \in k$. Then $\gamma^2 = \delta^2$ and $b = 2\gamma\delta$. However, $\gamma\delta = \pm\gamma^2$, and so $b^2 = 4\gamma^4$. But then, $a = -b^2 \in -4k^{*4}$, a contradiction. We are left with

(2) $\alpha = -4\beta^4$ with $\beta \in k(\alpha)^*$. Again,

$$-a = \mathcal{N}_{k(\alpha)/k}(\alpha) = \mathcal{N}_{k(\alpha)/k}(-4)\mathcal{N}_{k(\alpha)/k}(\beta)^4.$$

Since $\mathcal{N}_{k(\alpha)/k}(-4) = (-4)^2 = 16$, we deduce $-a$ is a square and we've assumed a is not a square. As above, $i \notin k$ and we now repeat the argument of (1) to finish the proof. □

4.11 Algebraic Closures; Steinitz's Theory of Fields

In the twentieth century, E. Steinitz examined the theory of fields, especially transcendental extensions. He had at his disposal the then new technique of transfinite induction which he used in the form of Zermelo's well-ordering principle. Of course, the latter is equivalent to Zorn's Lemma or the Axiom of Choice. Here, we'll examine Steinitz's results both in the purely algebraic case (existence of an algebraic closure) and in the general case (transcendence bases).

Recall that in Remark (4) at the close of Section 4.2 we made the following definition (but informally):

Definition 4.15 A field, K, is *algebraically closed* (AC) iff for every $f \in K[X]$, there exists a $\theta \in K$, so that $f(\theta) = 0$.

We also defined an *algebraic closure* of the field k as a field, K, which was itself AC and moreover was algebraic over k. Here, we'll prove the existence of an algebraic closure for each field, k, and its (essential) uniqueness. First, for technical agility we'll need equivalent forms of the condition (AC):

Proposition 4.75 *For a field, K, the following conditions are equivalent:*

(1) K has AC

(2) For every $f \in K[X]$, all the roots of f (in any extension of K) are already in K

(3) Every polynomial $f \in K[X]$ factors into linear factors in $K[X]$

(4) The only irreducible K-polynomials are the linear ones

(5) If L/K is algebraic, then $L = K$ (so, K is algebraically closed in any of its overfields)

(6) If k is a subfield of K for which K/k is algebraic, then for any algebraic extension, L, of k, there exists a k-monomorphism $L \longrightarrow K$.

(7) If k is a subfield of K for which K/k is algebraic and if $\widetilde{k}$ is a field isomorphic to k, via an isomorphism, φ, then for any algebraic extension, $\widetilde{L}$ or $\widetilde{k}$, there exists a monomorphism $\Phi\colon \widetilde{L} \to K$ extending φ.

The proofs of the equivalences (1)–(7) are trivial (DX); in (6) and (7) one makes use of the extension lemma.

Remark: An algebraicaly closed field is always infinite. For, were it finite and $\theta_1, \ldots, \theta_n$ a listing of its elements, then $f(T) = 1 + \prod_{j=1}^{n}(T - \theta_j)$ would be a polynomial with no root in our field.

Now for the proof of the existence of algebraic closures, we need a very basic existence theorem.

Theorem 4.76 *(Basic Existence Theorem) Suppose k is a field and K_λ ($\lambda \in \Lambda$) is a family of overfields of k. Then, there exists a field extension K/k so that for every $\lambda \in \Lambda$ we have a k-monomorphism $\varphi_\lambda\colon K_\lambda \to K$. That is, K contains a k-isomorphic copy of each field K_λ. Moreover, we may even choose K so that it is generated by all the subfields $\varphi_\lambda(K_\lambda)$.*

Proof. The proof is very simple using our techniques. We form the commutative ring $A = \bigotimes_{\lambda\in\Lambda} K_\lambda$. Of course,

$$A = \varinjlim_{S\in\mathcal{L}(\Lambda)} \Big(\bigotimes_{\lambda\in\Lambda} K_\lambda\Big),$$

where $\mathcal{L}(\Lambda)$ is the family of *finite* subsets of Λ. The ring A is a k-algebra (the tensor products are taken over k) and we embed k in A as usual *via* $\alpha \mapsto \alpha \cdot (1 \otimes 1 \otimes \cdots \otimes 1 \otimes \cdots)$. Choose any maximal ideal, $\mathfrak{M}$, of A and write $K = A/\mathfrak{M}$. Of course, K is a field extension of k and as each K_λ has a k-algebra homomorphism to K ($K_\alpha \longrightarrow \bigotimes_\mu K_\mu = A \longrightarrow A/\mathfrak{M} = K$) taking 1 to 1, we see that each K_λ is embedded in K *via* this homomorphism. Now the images in A of the K_λ generate A; so, their images in K generate K. $\square$

Theorem 4.77 *(Steinitz) If k is a field, then k possesses an algebraic closure, Ω. If Ω and $\widetilde{\Omega}$ are two algebraic closures of k, then there exists a (non-canonical) k-isomorphism $\Omega \xrightarrow{\sim} \widetilde{\Omega}$. The set $\mathrm{Isom}_k(\Omega, \widetilde{\Omega})$ is in one-to-one correspondence with $\mathcal{G}(\Omega/k)$.*

Proof. We wish to use the Basic Existence Theorem, so the only problem is to find a good way of parametrizing all finite extensions of k. Here, a better idea is to parametrize all the *finitely generated* extensions of k. Take $A = k[X_j]_{j=0}^{\infty}$, the polynomial algebra on $\aleph_0$ independent transcendentals over k. View, for each $n \geq 0$, the finitely generated polynomial rings $k[X_0, \ldots, X_n]$ as a subring of A. In each ring $k[X_0, \ldots, X_n]$ we have the family of its maximal ideals, $\mathfrak{M}$. Write $K(n, \mathfrak{M})$ for the field $k[X_0, \ldots, X_n]/\mathfrak{M}$ and consider the collection of all these $K(n, \mathfrak{M})$.[6] By the Basic Existence Theorem, there is field, L, over k containing a k-isomorphic copy of each $K(n, \mathfrak{M})$. But each finite degree extension, M, of k is k-isomorphic to at least one $K(n, \mathfrak{M})$; and so, each finite degree extension is "contained" in L. Write

$$\begin{aligned} \Omega = L_{\mathrm{alg}} &= \{\xi \in L \mid \xi \text{ is algebraic over } k\} \\ &= \text{ algebraic closure of } k \text{ in } L. \end{aligned}$$

By construction, Ω is algebraic over k; by choice of L, each finite degree extension, M, of k is k-isomorphic to a $K(n, \mathfrak{M})$ so the latter is algebraic over k; hence, in Ω. And now, (the obvious modification of) Proposition 4.75 #(6) shows Ω is algebraically closed.

Having proved existence, we now investigate uniqueness. Say $\widetilde{\Omega}$ is another algebraic closure of k. Now for Ω and $\widetilde{\Omega}$ we have

$$\Omega = \varinjlim_{K/k \text{ finite}, K \subseteq \Omega} K \tag{$\dagger$}$$

$$\widetilde{\Omega} = \varinjlim_{\widetilde{K}/k \text{ finite}, \widetilde{K} \subseteq \widetilde{\Omega}} \widetilde{K}. \tag{$\ddagger$}$$

Since Ω is algebraically closed, for each such $\widetilde{K}/k$ we get a k-injection $\widetilde{K} \longrightarrow \Omega$. We may assume each such $\widetilde{K}$ is normal over k and choose a maximal chain of such $\widetilde{K}$. Then, twisting if necessary by the $\mathcal{G}(\widetilde{K}/k)$, we obtain a consistent family of k-injections of these $\widetilde{K}$ into Ω. By ($\ddagger$), there results the k-injection $\widetilde{\Omega} \longrightarrow \Omega$. But the image of $\widetilde{\Omega}$ is algebraically closed and Ω is algebraic over it. We deduce from Proposition 4.75 (5) that $\Omega =$ image of $\widetilde{\Omega}$.

Lastly, if φ and ψ are two k-isomorphisms from Ω to $\widetilde{\Omega}$, the map $\psi^{-1} \circ \varphi$ is in $\mathcal{G}(\Omega/k)$. Hence, the k-isomorphisms $\varphi \circ \sigma$ run over all k-isomorphisms $\Omega \longrightarrow \widetilde{\Omega}$ whenever φ is one such and σ runs over $\mathcal{G}(\Omega/k)$. □

There remains the general case of a field extension k/k. The important concept here is the notion of *transcendence basis*.

Definition 4.16 A subset, S, of a field extension, K/k, is a *transcendence basis* for K/k iff

(1) S is algebraically independent over k and

(2) K is algebraic over $k(S)$.

We need some technique in handling algebraically independent elements. The most useful technical observation is the following:

[6] For readers with a foundational mind, note: In the first place, the pairs $(n, \mathfrak{M})$ are elements of the set $\mathbb{N} \coprod \mathcal{P}(A)$, where $\mathcal{P}(A)$ is the power set of A; so, our indexing is done by a set. Next, each field, $K(n, \mathfrak{M})$, is itself in $\mathcal{P}(A)$; so, the whole collection is perfectly valid from the point of view of set theory.

Proposition 4.78 *Suppose that K/k is a field extension and A and B are subsets of K. Then the three conditions below are mutually equivalent:*

(1) $A \cap B = \emptyset$ and $A \cup B$ is algebraically independent over k

(2) A is algebraically independent over k and B is algebraically independent over $k(A)$

(3) Same statement as (2) with A and B interchanged.

Proof. By symmetry, (2) $\iff$ (3); all that remains is to prove (1) $\iff$ (2).

(1) $\implies$ (2). As $A \subseteq A \cup B$ and the latter is algebraically independent over k, we find that A is algebraically independent over k. If B is algebraically dependent over $k(A)$, there are elements $b_1, \ldots, b_t$ and a nonzero polynomial $f(T_1, \ldots, T_t) \in k(A)[T_1, \ldots, T_t]$ with $f(b_1, \ldots, b_t) = 0$. But, the coefficients may be chosen from $k[A]$ and involve only finitely many elements $a_1, \ldots, a_s$ from A. Then, $f(T_1, \ldots, T_t)$ is actually a nonzero polynomial of the form $\widetilde{f}(a_1, \ldots, a_s, T_1, \ldots, T_t)$, and $\widetilde{f}$ is a polynomial over k in variables $U_1, \ldots, U_s, T_1, \ldots, T_t$. It is satisfied by $\{a_1, \ldots, a_s, b_1, \ldots, b_t\} \subseteq A \cup B$ contradicting (1).

(2) $\implies$ (1). No element, ξ, can be in $A \cap B$, else the polynomial $T - \xi \in k(A)[T]$ is satisfied by $\xi \in B$ contradicting (2). We need only show each finite subset of $A \cup B$ is algebraically independent and, of course, this is immediate if that finite subset is in A or B. So, we may assume that our subset is $a_1, \ldots, a_s, b_1, \ldots, b_t$. Any polynomial $f(U_1, \ldots, U_s, T_1, \ldots, T_t) \in k[U_1, \ldots, U_s, T_1, \ldots, T_t]$ which vanishes on $a_1, \ldots, a_s, b_1, \ldots, b_t$ gives a polynomial

$$f(a_1, \ldots, a_s, T_1, \ldots, T_t) \in k(A)[T_1, \ldots, T_t]$$

which vanishes on $b_1, \ldots, b_t$. By (2), all the coefficients of $f(a_1, \ldots, a_s, T_1, \ldots, T_t)$ have to vanish. By (2), again, these coefficients which are just different polynomials $g_j(U_1, \ldots, U_s)$ (coeffs in k) must be zero *as polynomials*. Therefore, our original polynomial $f(U_1, \ldots, U_s, T_1, \ldots, T_t)$ is identically zero. This proves (1). □

We derive many corollaries from Proposition 4.78.

Corollary 4.79 *Let K/k be a field extension and A be a subset of K. Then, A is algebraically independent over k iff for all $\xi \in A$, the element ξ is transcendental over $k(A - \{\xi\})$.*

Proof. By taking $A - \{\xi\}$ and $\{\xi\}$ as the two subsets of Proposition 4.78, we see that ($\Longrightarrow$) is proved. To prove ($\Longleftarrow$), take a finite subset of A, say $a_1, \ldots, a_t$, and suppose it is algebraically dependent over k. We may assume no smaller subset of $a_1, \ldots, a_t$ is dependent by passing to that smaller subset. Apply Proposition 4.78 to the sets $\{a_1\}$ and $\{a_2, \ldots, a_t\}$. Since $a_1, \ldots, a_t$ is **not** independent, it follows that a_1 is not independent over $k(a_2, \ldots, a_t)$. Hence, a_1 is not independent over the bigger field $k(A - \{a_1\})$. This contradicts our hypothesis when $\xi = a_1$. □

Corollary 4.80 *If K/k be a field extension and A is an algebraically independent subset (over k) of K, and if $\xi \in K$ has the property that ξ is transcendental over $k(A)$, then $A \cup \{\xi\}$ is again algebraically independent over k.*

Proof. This is immediate either from Proposition 4.78 or Corollary 4.79.

Corollary 4.81 *Suppose K/k is a field extension and A is an algebraically independent subset of K. A necessary and sufficient condition that A be a transcendence basis for K/k is that A be a maximal element (under partial ordering by set inclusion) among the algebraically independent subsets of K.*

Proof. If A is a transcendence basis for L/k yet is not maximal, there is an independent set, B, of K and $B > A$. In Proposition 4.78, let $B - a$ and A be the two sets, the $K \subseteq k(A)(B - A)$ and $K/K(A)$ is algebraic. So, $B - A$ is not algebraically independent over $k(A)$ contradicting Proposition 4.78.

Conversely, if A is maximal among algebraically independent sets and $\xi \in K$ but not in $K(A)$, then ξ cannot be transcendental over $k(A)$ by Proposition 4.78 (set $B = \{\xi\}$, $A = A$). So, ξ is algebraic over $K(A)$; that is, $K/k(A)$ is algebraic. □

Theorem 4.82 *(Steinitz) If K/k is a field extension and if $S \subseteq T$ are two subsets of K so that*

(a) K is algebraic over $k(S)$ and

(b) T is algebraically independent over k, then there exists a transcendence basis, B, for K/k with $T \subseteq B \subseteq S$. In particular, every field extension possesses a transcendence basis.

Proof. We let $\mathcal{S}$ denote the collection of subsets of S which both contain T and are algebraically independent over k. Of course, as $T \in \mathcal{S}$, we have $\mathcal{S} \neq \emptyset$. Partially order $\mathcal{S}$ by set-theoretic inclusion and note that $\mathcal{S}$ is inductive. Let B be a maximal element of $\mathcal{S}$, it exists by Zorn's Lemma. Consider the extension $k(S)/k(B)$. We know if each element of S is algebraic over $k(S)$, then $k(S)$ will be algebraic over $k(B)$. But by the maximality of B and Proposition 4.78 (or Corollary 4.80), we see that every element of S is indeed algebraic over $k(B)$. Thus, from the facts that K is algebraic over $k(S)$ and $k(S)$ is algebraic over $k(B)$, we find K is algebraic over $k(B)$.

Upon taking $S = K$ and $T = \emptyset$, we deduce each field extension has a transcendence basis. □

Doubtless you will have noticed an analogy between the familiar theory of linear dependence and independence for vector spaces and our theory of algebraic independence and indepnedence for field extensions. For example, Proposition 4.78 can be translated into the linear case. Steinitz noticed this explicitly and transformed the analogy into an axiomatic treatment of both cases simulataneously. In the linear case, the notion of Span is a crucial ingredient and Steinitz generalized this by setting

$$\Sigma(A) = \{\xi \in K \mid \xi \text{ is algebraic over } k(A) \qquad (*)$$

for A a subset of K and K/k a field extension. Of course we can then write: A is a transcendence basis for K/k iff A is algebraically independent over k and $K = \Sigma(A)$. The axioms for the Σ operation are the dictated by the linear case:

(1) $A \subseteq \Sigma(A)$,

(2) If $A \subseteq B$, then $\Sigma(A) \subseteq \Sigma(B)$.

(3) $\Sigma(\Sigma(A)) = \Sigma(A)$.

(4) If $\xi \in \Sigma(A)$, then there is a finite subset, $\widetilde{A}$, of A so that $\xi \in \Sigma(\widetilde{A})$.

(5) If $\eta \in \Sigma(A \cup \{\xi\})$ but $\eta \notin \Sigma(A)$, then $\xi \in \Sigma(A \cup \{\eta\})$.

Conditions (1)–(3) are obvious both in the linear case (when $\Sigma(A) = \text{Span}(A)$) and in the algebraic case (when $\Sigma(A)$ is as above). However, (4) and (5) deserve some comment. Property (4) makes the formation of $\Sigma(A)$ a property "of finite character", and allows the application of Zorn's Lemma in proofs of statements about $\Sigma(A)$ or independence. Property (5) is called the *Steinitz Exchange Lemma*—it is well-known in the linear case. Here it is in the algebraic case:

Proposition 4.83 *(Steinitz Exchange Lemma) For a field extension, K/k, a subset $A \subseteq K$ and element ξ, η of K we have*

If $\eta \in \Sigma(A \cup \{\xi\})$ but $\eta \notin \Sigma(A)$, then $\xi \in \Sigma(A \cup \{\eta\})$.

Here, $\Sigma(A)$ is as above in $(*)$.

Proof. In $k(A)$ we can choose a transcendence basis (over k) contained in A by Theorem 4.83. As $k(A)$ is algebraic over $k(B)$, it is algebraic over $k(B \cup \{\xi\})$. Now, ξ is algebraic over $k(B \cup \{\xi\})$; so, $k(A \cup \{\xi\})$ is algebraic over $k(B \cup \{\xi\})$ and therefore $\eta \in k(B \cup \{\xi\})$. If the exchange lemma were valid when A was independent, we would deduce $\xi \in \Sigma(B \cup \{\eta\}) \subseteq \Sigma(A \cup \{\eta\})$.

This achieves a reduction to the case where A is algbraically independent. The silly case $\xi = \eta$ is a tautology and so we have $\xi \neq \eta$ and $A \cup \{\xi, \eta\}$ is algebraically dependent. But then, Proposition 4.78 applied to the sets $A \cup \{\eta\}$, $\{\xi\}|$ shows that $\xi \in \Sigma(A \cup \{\eta\})$, as desired. □

Clearly, the Exchange Lemma is susceptible of generalizations. But one must be careful. "Obvious" generalizations may be false. For example, the statement: If A, B, C are subsets of K (an extension of k) and if $C \subseteq \Sigma(A \cup B)$ but $C \not\subseteq \Sigma(A)$, then $B \subseteq \Sigma(A \cup C)$ is *false*. Indeed, even the weaker statememnt (because the hypotheses are stronger): If $C \subseteq \Sigma(A \cup B)$ but *no element of* C *is in* $\Sigma(A)$, then $B \subseteq \Sigma(A \cup C)$ is *false*. To see why the latter is false, just take $A = \emptyset$ and $K = k(X, Y, \sqrt{X})$, where X and Y are algebraically independent over k. Set $B = \{X, Y\}$ and $C = \{\sqrt{X}\}$.

Proposition 4.84 *(General Steinitz Exchange Lemma) Suppose K/k is a field extension and $A, B, C \subseteq K$. Assume that $C \subseteq \Sigma(A \cup B)$ but $C \not\subseteq \Sigma(A)$. Then, there exists a subset, B', of B with properties*

(1) $B \subseteq \Sigma(A \cup C \cup B')$.

(2) $B \neq B'$.

(3) $B' \cap C = \emptyset$.

Before proving this form of the exchange lemma, we should remark that:

(a) The hypotheses are those of the previous strong (but false) statement—the conclusion is weaker: we need B'. In the example where $A = \emptyset$, $C = \{\sqrt{X}\}$, $B = \{X, Y\}$, it is clear that $B' = \{Y\}$.

(b) The name come from the fact that B'' $(= B - B')$ and C have been exchanged. That is, we conclude $B'' \subseteq \Sigma(A \cup B' \cup C)$ from the hypotheses $C \subseteq \Sigma(A \cup B' \cup B'')$ and $C \not\subseteq \Sigma(A)$.

Proof. Here, the notation Σ refers to algebraic dependence *over* k. Let $\widetilde{A}$ be a maximal algebraically independent subset of A, so that $\Sigma(\widetilde{A}) = \Sigma(A)$. Write $\widetilde{C}$ for a subset of C maximal with respect to algebraic independence *over* $k(\widetilde{A})$. Because $C \not\subseteq \Sigma(\widetilde{A})$, we see that $\widetilde{C} \neq \emptyset$ and that $\widetilde{A} \cup \widetilde{C}$ is algebraically independent over k by Proposition 4.78. Now $C \subseteq \Sigma(\widetilde{A} \cup \widetilde{C})$ and $A \subseteq \Sigma(\widetilde{A}) \subseteq \Sigma(\widetilde{A} \cup \widetilde{C})$. We find that

$$\Sigma(A \cup B) = \Sigma(\widetilde{A} \cup \widetilde{C}).$$

Write $T = \widetilde{A} \cup \widetilde{C} \cup B$. Now, $\Sigma(A \cup B) = \Sigma(\widetilde{A} \cup B)$ and by hypothesis we find that $C \subseteq \Sigma(\widetilde{A} \cup B)$. Therefore, $\Sigma(T) = \Sigma(A \cup B)$; call this field $\widetilde{K}$. In it, we have $T \supseteq \widetilde{A} \cup \widetilde{C}$, the former set generates and the latter is algebraically independent. By the existence of transcendence bases (Theorem 4.83), there is a transcendence basis for $\widetilde{K}/k$, call it S, so that

$$T \supseteq S \supseteq \widetilde{A} \cup \widetilde{C}.$$

We set $B' = S - (\widetilde{A} \cup \widetilde{C}) \subseteq B$. Of course, $B' \cap \widetilde{C} = \emptyset$. We know

$$\Sigma(T) = \Sigma(S) = \Sigma(\widetilde{A} \cup \widetilde{C} \cup B')$$

and $B \subseteq \Sigma(T)$; so, conclusion (1) is proved. Were $B' = B$, we'd have $S = \widetilde{A} \cup \widetilde{C} \cup B$. Now $\widetilde{C} \subseteq C$ and by hypothesis $C \subseteq \Sigma(A \cup B) = \Sigma(\widetilde{A} \cup B)$. As S is algebraically independent, we have a contradiction of Proposition 4.78; this proves (2). Finally, if $\xi \in B' \cap C$, then $\xi \in C \subseteq \Sigma(\widetilde{A} \cup \widetilde{C})$ implies that the subset of $B' \cup \widetilde{A} \cup \widetilde{C} = S$ consisting of $\{\xi\} \cup \widetilde{A} \cup \widetilde{C}$ is dependent; contradiction on how we chose S. □

The main use of the standard exchange lemma is to prove that transcendence bases have the same cardinality. Here's how the finite case goes.

Theorem 4.85 *Suppose K/k is a field and S is a finite subset of K while T is any subset of K. Assume that $\#(T) > \#(S)$ and $T \subseteq \Sigma(S)$. Then T is algebraically dependent. In particular, if K/k has a finite transcendence basis, then all transcendence bases of K/k are finite with the same cardinality.*

Proof. First, replace K by $\Sigma(S)$, second replace S by a transcendence basis (for $K = \Sigma(S)$) which is a subset of S. Therefore, we may assume S is a transcendence basis for K/k. If $\#(T) = \infty$, then then replace T by any finite subset with $\#(T) > \#(S)$; so we may assume T is finite, too. Now suppose the result is false and choose a counter-example pair S, T so that $\#(S)+\#(T)$ is minimal. Of course, in this case $\#(T) = \#(T)+1$, else we could reduce the sum by choosing a subset of T with $\#(T) = \#(S) + 1$.

Our situation is now that

(a) S and T are finite algebraically independent sets

(b) $T \subseteq \Sigma(S)$

(c) $\#(S) = n$, $\#(T) = n + 1$

(d) n is minimal among integers having (a), (b), (c).

Label the elements of S as $s_1, \ldots, s_n$ but refrain from labelling T as yet. Consider $S - \{s_1\}$. There must be some $t \in T$ so that $t \notin \Sigma(S - \{s_1\})$, else $T \subseteq \Sigma(S - \{s_1\})$ and (d) would show T dependent contradicting (a). Call this element t_1. Note that $\{s_2, \ldots, s_n, t_1\}$ is an independent set at $t_1 \notin \Sigma(s_2, \ldots, s_n)$. Since $t_1 \in \Sigma((S-\{s_1\})\cup\{s_1\})$, the standard exchange lemma (Proposition 4.83) shows that $s_1 \in \Sigma(s_2, \ldots, s_n, t_1)$. All the other elements of S lie in $\Sigma(s_2, \ldots, s_n, t_1)$ so $T - \{t_1\}$ is certainly in $\Sigma(s_2, \ldots, s_n, t_1)$. However, $T - \{t_1\}$ cannot be contained in $\Sigma(s_3, \ldots, s_n, t_1)$. For if it were, the sets $\{s_3, \ldots, s_n, t_1\}$, $T - \{t_1\}$ would satisfy (a) and (b), their cardinalities would be $n - 1$ and n respectively and (d) would be contradicted.

Since $T - \{t_1\} \not\subseteq \Sigma(s_3, \ldots, s_n, t_1)$, there is an element $t_2 \in T - \{t_1\}$ with $t_2 \notin \Sigma(s_3, \ldots, s_n, t_1)$. This means $\{s_3, s_4, \ldots, s_n, t_1, t_2\}$ is an independent set and allows the exchange lemma to be applied once more to $\eta = t_2$, $\xi = s_2$, and $\{s_3, \ldots, s_n, t_1\}$. We conclude that $s_2 \in \Sigma(s_3, \ldots, s_n, t_1, t_2)$ and so all of T (thus also $T - \{t_1, t_2\}$) is in $\Sigma(s_3, \ldots, s_n, t_1, t_2)$. It is clear how to continue the process and equally clear what is happening: We are systematically replacing the elements $s_1, s_2, \ldots$ of S by elements $t_1, t_2, \ldots$ from T. In the end, we find $T - \{t_1, \ldots, t_n\} \subseteq \Sigma(t_1, \ldots, t_n)$; but, $\#(T) = n + 1$, so $t_{n+1} \in \Sigma(t_1, \ldots, t_n)$–our final contradiction (on (a)). As (a)–(d) are untenable, no counter-example exists.

To prove if K/k has finite transcendence basis, all transcendence bases have the same cardinality, we choose a transcendence basis, S, of minimal (so, finite) cardinality and any other transcendence basis, T. Of course, $\#(T) \geq \#(S)$. If $\#(T) > \#(S)$, then $T \subseteq \Sigma(S)$ immediately implies from the above that T is dependent, which is not true. Thus, $\#(T) \leq \#(S)$, and we are done. □

If the reader will go through the argument, he will see we have used only Steinitz's rules (1)—(5) on Σ. Thus, the argument works in the linear case—though a direct argument is simpler. In carrying this out, one sees that Corollary 4.79 gives a way of defining algebraic independence solely in terms of the Σ operation. Namely, A is algebraically independent iff for every $\xi \in A$, the element ξ is not in $\Sigma(A - \{\xi\})$.

We can now handle the infinite case.

Theorem 4.86 *For every field extension K/k, any two transcendence bases have the same cardinality.*

Proof. Is S and T are given transcendence bases for K/k, then, by Theorem 4.85, the sets S and T are simultaneously finite or infinite. Of course, the only case of concern is when S and T are infinite.

I claim two statements, which taken together will quickly finish the proof.

(I) *For each $\xi \in K$*, there exists a *unique finite* subset of S, call it $S(\xi)$, characterized by

  (a) $\xi \in \Sigma(S(\xi))$ and

  (b) If $\widetilde{S} \subseteq S$ and $\xi \in \Sigma(\widetilde{S})$, then $S(\xi) \subseteq \widetilde{S}$.

(II) For ξ and η in T, if $\xi \neq \eta$, then $S(\xi) \neq S(\eta)$.

Suppose we assume (I) and (II) and write $\mathcal{FP}(S)$ for the collection of all *finite* subsets of S. Then the map $\xi \mapsto S(\xi)$ is, by (I) and (II), a well defined injection of T to $\mathcal{FP}(S)$. We find that $\#(T) \leq \#(\mathcal{FP}(S))$ and we know $\#(S) = \#(\mathcal{FP}(S))$ because $\#(S)$ is infinite. Thus, $\#(T) \leq \#(S)$; by symmetry, $\#(S) \leq \#(T)$. Then, the Cantor-Schröder-Bernstein Theorem yields $\#(S) = \#(T)$.

Both (I) and (II) are consequences of the exchange lemma. For (I), choose $\xi \in K$. If ξ is algebraic over k, the set $S(\xi) = \emptyset$ satisfies (a) and (b); we may assume ξ is transcendental over k. There is a finite subset, $\{s_1, \ldots, s_n\}$, of S so that $\xi \in \Sigma(s_1, \ldots, s_n)$. We may assume no smaller subset of $\{s_1, \ldots, s_n\}$ has ξ in the Σ formed from it. Suppose $\{\sigma_1, \ldots, \sigma_q\}$ is another subset of S and $\xi \in \Sigma(\sigma_1, \ldots, \sigma_q)$. Choose any s_j, apply the exchange lemma to ξ, s_j and $S - \{s_j\}$. We find that $s_j \in \Sigma(s_1, \ldots \widehat{s}_j, \ldots, s_n, \xi)$. Now, $\xi \in \Sigma(\sigma_1, \ldots, \sigma_q)$, therefore

$$s_j \in \Sigma(s_1, \ldots \widehat{s}_j, \ldots, s_n, \sigma_1, \ldots, \sigma_q).$$

The elements s_j and σ_l are in the independent set S therefore s_j must be one of the $\sigma_1, \ldots, \sigma_q$. Since s_j is arbitrary in $\{s_1, \ldots, s_n\}$ we get $\{s_1, \ldots, s_n\} \subseteq \{\sigma_1, \ldots, \sigma_q\}$ and so $S(\xi) = \{s_1, \ldots, s_n\}$ has (a) and (b).

To prove (II), first note that if $\xi \in S$, then $S = \{\xi\}$. Pick $\xi, \eta \in T$ and assume $S(\xi) = S(\eta)$. Write $\{s_1, \ldots, s_n\}$ for the listing of the elements of $S(\xi)$. A standard application of the exchange lemma shows $s_1 \in \Sigma(s_2, \ldots, s_n, \xi)$. Therefore, $S(\xi) \subseteq \Sigma(s_2, \ldots, s_n, \xi)$. It follows, as $S(\xi) = S(\eta)$, that $\eta \in \Sigma(s_2, \ldots, s_n, \xi)$. By Claim (I) property (b), we find

$$\{s_1, \ldots, s_n\} = S(\eta) \subseteq \{s_2, \ldots, s_n, \xi\}.$$

Hence, $\xi = s_1$. By symmetry, $\eta = s_1$, too; and so, $\xi = \eta$ (or $\xi \in S$ and hence so is η; therefore $\{\xi\} = S(\xi) = S(\eta) = \{\eta\}$). We are done. □

Definition 4.17 The common cardinal number of all the transcendence bases for K/k is the *transcendence degree of* K/k. It is denoted $\text{tr.d.}_k(K)$. The field K is *purely transcendental over* k iff $K = k(S)$ where S is a transcendence base for K/k.

To finish up this section, we have only to discuss the notion of separability for general field extensions (i.e., not necessarily algebraic). For this, we essentially make Mac Lane I into a definition:

Definition 4.18 A field extension, K/k, is *separable* iff either $\text{char}(k) = 0$ or when $\text{char}(k) = p > 0$, then the natural map

$$k^{1/p} \otimes_k K \longrightarrow K^{1/p}$$

is injective.

There is a related (but stronger) concept, namely the notion of *separable generation*:

Definition 4.19 A field extension, K/k, is *separably generated* iff there exists a transcendence base, B, for K/k so that K is separable (algebraic) over $k(B)$. Such a transcendence bases is called a *separating transcendence base for* K/k.

Separable non-algebraic field extensions exist:

Proposition 4.87 *If $K = k(B)$ and B is an algebraically independent set, then K/k is a separable extension.*

Proof. By the argument of Section 4.3, the definition of separability is that when $u_1, u_2, \ldots$ are element of K linearly independent over k, then $u_1^p, \ldots, u_n^p, \ldots$ are again linearly independent over k. If we apply this to all the monomials formed from the elements of B, we see that we must prove: The elements u^p, where u ranges over B, are algebraically independent over k. But, any non-trivial polynomial relation

$$f(u_{i_1}^p, \ldots, u_{i_t}^p) = 0$$

is, *a fortiori*, a polynomial relation for $u_{i_1}, \ldots, u_{i_t}$; hence, cannot be non-trivial. □

We can make two remarks that will be helpful for what follows:

Remarks:

(I) *Separability is transitive*. To see this, say L is separable over K and K is separable over k. Then, the two maps

$$k^{1/p} \otimes_k K \longrightarrow K^{1/p}; \quad K^{1/p} \otimes_K L \longrightarrow L^{1/p} \tag{$*$}$$

are injective. But then, we get the injection

$$(k^{1/p} \otimes_k K) \otimes_K L \longrightarrow K^{1/p} \otimes_K L \tag{$**$}$$

(as L is flat over K). The left hand side of $(**)$ is $k^{1/p} \otimes_k L$ and the right hand side injects into $L^{1/p}$ by $(*)$; so, we are done.

(II) *Any field extension of a perfect field is separable*. For, if k is perfect, then $k = k^p$; that is, $k^{1/p} = k$. But then, $k^{1/p} \otimes_k K \cong K$ and $K \subseteq K^{1/p}$, as required.

(III) *If $K \supseteq L \supseteq k$ and K/k is separable, then L/k is separable*. For consider the map

$$k^{1/p} \otimes_k L \longrightarrow L^{1/p}.$$

Let its kernel be $\mathfrak{A}$. By the flatness of K over L, we see that

$$0 \longrightarrow \mathfrak{A} \otimes_L K \longrightarrow (k^{1/p} \otimes_k L) \otimes_L K = k^{1/p} \otimes_k K \longrightarrow L^{1/p} \otimes_L K$$

is exact. Now, the composed map $k^{1/p} \otimes_k K \longrightarrow L^{1/p} \otimes_L K \longrightarrow K^{1/p}$ is injective by hypothesis; so, $\mathfrak{A} \otimes_L K = (0)$. But, K is faithfully flat over L, therefore $\mathfrak{A} = (0)$.

Corollary 4.88 *If K/k is separably generated, then K/k is separable.*

Proof. Write B for a separating transcendence base for K/k. Then, K is separable over $k(B)$ and the latter is separable over k by Proposition 4.87. Now Remark (I) applies. □

Separable generation is, in general, a strictly stronger concept than separability. Here is a standard example: Let k be a perfect field (i.e., $k = \mathbb{F}_p$) and write $k = k(T, T^{1/p}, T^{1/p^2}, \ldots)$. Thus, $K = \varinjlim_n K_n$, where $K_n = k(T^{1/p^n})$ and each K_n, being pure transcendental over k, is separable over k. Of course, $K^{1/p} = K$ and $k^{1/p} = k$ by choice of k; so K/k is separable. We will now see it is **not** separably generated. Let's write STB for the phrase separating transcendence basis. We know $\mathrm{tr.d}_k K = 1$ as each K_n is algebraic over K_1. Were an element $z \in K$ an STB, we'd have $z \in K_n$ for some n. Now, we may ignore $K_1, \ldots, K_{n-1}$ and still have $K = \varinjlim_m K_m$ $(m \geq n)$, so we may assume $z \in K_1$. i.e., $z \in k(T)$. but then, the diagram of *algebraic* extensions

$$\begin{array}{c} K \\ | \\ k(T) = K_1 \\ | \\ k(Z) \end{array}$$

and the fact that K is separable over $k(Z)$ would show that K/K_1 is a separable algebraic extension and this is nonsense.

Remark. In the general case when K/k is separable and L is a subextension of the layer K/k it does **not** follow that K/L is separable. For example, $L = K_1$ in the above example shows that K/K_1 is **not** separable even though K/k is separable.

This remark indicates that separability is not a good notion in the general case; separable generation is a much better notion. We are going to show now that the two concepts coalesce when the big field is a finitely generated extension; so, the cause of most difficulties is infinite generation in the general case (as should be clear from the counter-example above). Still, even in the finitely generated case, there are problems: K_2/k is separably generated yet it is **not** separably generated over K_1 (or separable–notations as above). The moral is: *be careful with separability (or separable generation) in the non-algebraic case, especially with infinitely generated extensions*.

Theorem 4.89 *If K/k is a finitely generated field extension, then K/k is separable if and only if it is separably generated.*

Proof. One direction is Corollary 4.88; so, assume K/k is separable and finitely generated, say $K = k(T_1, \ldots, T_n)$. We let $r = \mathrm{tr.d}_k K$ and use induction on $n - r$. If the latter is zero, $T_1, \ldots, T_r$ are already an STB; so, assume $n = r + 1$ (this turns out to be the essential case). Now $T_1, \ldots, T_{r+1}$ are algebraically dependent and, by rearranging their order, we may assume $T_1, \ldots, T_r$ are a transcendence base. Then there is a polynomial of smallest degree in X_{n+1} coefficients in $k[X_1, \ldots, X_r]$ having content 1, say $f(X_1, \ldots, X_{r+1})$, so that $f(T_1, \ldots, T_r, T_{r+1}) = 0$. The degree of this polynomial in X^{r+1} must be positive and if its leading coefficient is $a_0(X_1, \ldots, X_r)$, we can localize $k[X_1, \ldots, X_r]$ with respect to a_0 and make f monic in $k[X_1, \ldots, X_r]_{a_0}[X_{r+1}]$. The division algorithm for monic polynomials shows then that if $g \in k[X_1, \ldots, X_{r+1}]$ vanishes on $T_1, \ldots, T_{r+1}$, we have

$$a_0^s g = f \cdot g \quad \text{in} \quad k[X_1, \ldots, X_{r+1}]$$

for some $s \geq 0$. by unique factorization in $k[X_1, \ldots, X_{r+1}]$ it shows further that f is *irreducible*.

Suppose we could show that $f(X_1, \ldots, X_{r+1}) \notin k[X_1^p, \ldots, X_{r+1}^p]$. If so, at least one variable occurs in f with exponent indivisible by p, call this variable X_i. Then T_i is dependent on $T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{r+1}$ and the latter must be algebraically independent by Theorem 4.82. Moreover, as the exponent of T_i is not divisible by p, the element T_i is separable over $k(T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_{r+1})$ and so, $T_1, \ldots, T_{i-1}, T_{i+1}, \ldots$, T_{r+1} form a separating transcendence basis, as required.

We use the separability of K/k to prove that $f(X_1, \ldots, X_{r+1}) \notin k[X_1^p, \ldots, X_{r+1}^p]$. Were the contrary true, there would be a polynomial

$$f(X_1, \ldots, X_{r+1}) = g(X_1^p, \ldots, X_{r+1}^p).$$

The monomials $m_1, \ldots, m_t$ comprising g all have degree less than of f, so the elements $m_1(T_1, \ldots, T_{r+1}), \ldots$, $m_t(T_1, \ldots, T_{r+1})$ are linearly independent over k. By separability, the elements

$$m_1(T_1, \ldots, T_{r+1})^p = m_1(T_1^p, \ldots, T_{r+1}^p), \ldots, m_t(T_1, \ldots, T_{r+1})^p = m_t(T_1^p, \ldots, T_{r+1}^p)$$

are still linearly independent over k. Yet the relation

$$g(T_1^p, \ldots, T_{r+1}^p) = f(T_1, \ldots, T_{r+1}) = 0$$

is a non-trivial linear relation among $m_1^p, \ldots, m_t^p$, a contradiction.

For use below, we record what we have just proved:

If K/k is separable, of transcendence degree r, then any set of $r+1$ elements of K, say $T_1, \ldots, T_{r+1}$, which contains a transcendence basis for K/k, already contains a separating transcendence basis for $k(T_1, \ldots, T_{r+1})$ over k. (All wee need note is that, by Remark III above, the field $k(T_1, \ldots, T_{r+1})$ is separable over k.)

Now, let's continue with our induction and finish the proof. We have $n-r>1$ and we assume separable generation for all separable field extensions, K/k, generated by less than $n-r$ elements ($\mathrm{tr.d}_k K = r$). By Remark III, $k(T_1,\dots,T_{n-1})$ is separably generated; so we can take an STB $U_1,\dots,U_t$ for it. There are only two possibilities for t: either $t=r-1$ or $t=r$. Since K is then separable (algebraic) over $k(U_1,\dots,U_t,T_n)$, we need only show the latter field is separably generated over k. But, the transcendence degree of $k(U_1,\dots,U_t,T_n)$ over k is r and $t+1\leq r+1$ by the above. Again, Remark III shows $k(U_1,\dots,U_t,T_n)$ is separable over k, and so our argument above (summarized in italics above), implies the required separable generation of $k(U_1,\dots,U_t,T_n)$ over k. □

We can augment the reasoning in the proof of Theorem 4.89 to obtain a useful theorem of Mac Lane:

Theorem 4.90 *(Mac Lane) Suppose K/k is a finitely generated, separable field extension. Then, any set of generators for K/k already contains a separating transcendence basis for K/k.*

Proof. Write $r=\mathrm{tr.d}\,K$ and say $K=k(T_1,\dots,T_n)$. We use, as usual, induction on $n-r$, the case $n-r=0$ is trivial and the case $n-r=1$ is covered by the italicized statement in the middle of the proof of Theorem 4.89. For the induction step, use the notation of the last part of Theorem 4.89 and note that, by the induction hypothesis, STB $U_1,\dots,U_t$ may be chosen from among $T_1,\dots,T_{n-1}$. Then the $r+1=t+1$ generators $U_1,\dots,U_t,T_n$ for $k(U_1,\dots,U_t,T_n)$ are among $T_1,\dots,T_{n-1},T_n$ and so the case $n-r=1$ now applies and finishes the proof. □

An important corollary of our theorems is this result:

Corollary 4.91 *(F.K. Schmidt) If k is a perfect field, every finitely generated field extension of k is separably generated over k.*

Proof. We apply Remark II and Theorem 4.89 (or 4.90) to our finitely generated extension of k. □

4.12 Further Readings

Some basics of Galois theory is covered in most algebra texts (see Section 2.9). Emil Artin's classic [1] is a must. Other references include Kaplanski [31], Zariski and Samuel [50], Bourbaki (Algebra, Chapter IV) [6], Lafon [33], Morandi [41], Escofier [14] and Van Der Waerden [47].

Chapter 5

Homological Algebra

5.1 Introduction

Homological Algebra has now reached into almost every corner of modern mathematics. It started with the invasion of algebra into topology at the hands of Emmy Noether. She pointed out that the ranks and "torsion coefficients" computed for various spaces were just the descriptions of finitely generated abelian groups as coproducts of cyclic groups; so, one should instead study these "homology invariants" as homology *groups*. Algebraic topology was born.

In the late 30's through the decade of the 40's, the invasion was reversed and topology invaded algebra. Among the principal names here were Eilenberg, MacLane, Hochschild, Chevalley and Koszul. This created "homological algebra" and the first deeply influential book was in fact called "Homological Algebra" and authored by H. Cartan and S. Eilenberg (1956) [9].

Our study below is necessarily abbreviated, but it will allow the reader access to the major applications as well as forming a good foundation for deeper study in more modern topics and applications.

5.2 Complexes, Resolutions, Derived Functors

From now on, let $\mathcal{A}$ denote an abelian category; think of $\mathcal{M}\text{od}(R)$, where R is a ring, not necessarily commutative. This is not so restrictive an example. The Freyd-Mitchell embedding theorem [15, 40], says that each "reasonable" abelian category admits a full embedding into $\mathcal{M}\text{od}(R)$ for a suitable ring R.

We make a new category, $\text{Kom}(\mathcal{A})$, its objects are sequences of objects and morphisms from $\mathcal{A}$:

$$\cdots \longrightarrow A^{-n} \xrightarrow{d^{-n}} A^{-n+1} \xrightarrow{d^{-n+1}} \cdots \longrightarrow A^{-1} \xrightarrow{d^{-1}} A^0 \xrightarrow{d^0} A^1 \longrightarrow \cdots \longrightarrow A^n \xrightarrow{d^n} A^{n+1} \longrightarrow \cdots,$$

in which $d^{i+1} \circ d^i = 0$, for all i. That is, its objects are complexes from $\mathcal{A}$.

Such a complex is usually denoted by $A^\bullet$ (sometimes, $(A^\bullet, d^\bullet)$). The morphisms of $\text{Kom}(\mathcal{A})$ are more complicated. However, we have the notion of "premorphism": $(A^\bullet, d^\bullet) \xrightarrow{\varphi^\bullet} (B^\bullet, \delta^\bullet)$. This is a sequence, $\varphi^\bullet$, of morphisms from $\mathcal{A}$, where $\varphi^n \colon A^n \to B^n$, and we require that for all n, the diagram

$$\begin{array}{ccc} A^n & \xrightarrow{d^n} & A^{n+1} \\ {\scriptstyle \varphi^n}\downarrow & & \downarrow{\scriptstyle \varphi^{n+1}} \\ B^n & \xrightarrow[\delta^n]{} & B^{n+1} \end{array}$$

commutes. Such φ's are called *chain maps*, or *cochain maps*. The collection of complexes and their chain maps forms the category PreKom($\mathcal{A}$).

Remarks:

(1) Write $A_n = A^{-n}$. This notation is usually used when $A^\bullet$ stops at A^0 (correspondingly, write d_n for d^{-n}).

(2) A complex is *bounded below* (resp. *bounded above*) iff there is some $N \geq 0$ so that $A^k = (0)$ if $k < -N$ (resp. $A^k = (0)$ if $k > N$). It is *bounded* iff it is bounded above and below. The sub (pre)category of the bounded complexes is denoted PreKom$^b(\mathcal{A})$.

(3) If $A^k = (0)$ for all $k < 0$, we have a *cohomological complex* (*right complex or co-complex*).

(4) If $A^k = (0)$ for all $k > 0$, then we use lower indices and get a *homological complex* (*left complex*, or just *complex*).

(5) The category $\mathcal{A}$ has a full embedding in PreKom($\mathcal{A}$) *via* $A \mapsto A^\bullet$, where $A^k = (0)$ if $k \neq 0$ and $A^0 = A$ and all $d^k \equiv 0$.

(6) Given a sequence, $\{A^n\}_{n=-\infty}^{\infty}$ from $\mathcal{A}$, we get an object of PreKom($\mathcal{A}$), namely:

$$\cdots \longrightarrow A^{-n} \xrightarrow{0} A^{-n+1} \xrightarrow{0} \cdots \longrightarrow A^{-1} \xrightarrow{0} A^0 \xrightarrow{0} A^1 \xrightarrow{0} A^2 \longrightarrow \cdots,$$

where all maps are the zero map. Since Kom($\mathcal{A}$) and PreKom($\mathcal{A}$) will have the same objects, we will drop references to PreKom($\mathcal{A}$) when objects only are discussed.

(7) Given $(A^\bullet, d^\bullet)$ in $\mathcal{O}$b(Kom($\mathcal{A}$)), we make a new object of Kom($\mathcal{A}$): $H^\bullet(A^\bullet)$, with

$$H^n(A^\bullet) = \text{Ker } d^n / \text{Im } d^{n-1} \in \mathcal{O}\text{b}(\mathcal{A}),$$

and with all maps equal to the zero map. The object $H^\bullet(A^\bullet)$ is the *homology* of $(A^\bullet, d^\bullet)$.

Nomenclature. A complex $(A^\bullet, d^\bullet) \in \text{Kom}(\mathcal{A})$ is *acylic* iff $H^\bullet(A^\bullet) \equiv (0)$. That is, the complex $(A^\bullet, d^\bullet)$ is an exact sequence.

Given $A \in \mathcal{O}\text{b}(\mathcal{A})$, a *left (acyclic) resolution* of A is a left complex, $P_\bullet = \{P_n\}_{n=0}^{\infty}$, in Kom($\mathcal{A}$) and a map $P_0 \longrightarrow A$ so that the new complex

$$\cdots P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

is acyclic. A *right (acyclic) resolution* of $A \in \mathcal{O}\text{b}(\mathcal{A})$ is the dual of a left acyclic resolution of A considered as an object of $\mathcal{A}^D$.

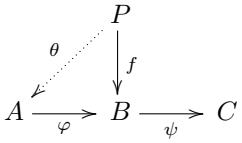
We shall assume of the category $\mathcal{A}$ that:

(I) $\mathcal{A}$ *has enough projectives (or enough injectives, or enough of both).* That is, given any $A \in \mathcal{O}\text{b}(\mathcal{A})$ there exists some projective object, P_0, (resp. injective object Q^0) and a surjection $P_0 \longrightarrow A$ (resp. an injection $A \longrightarrow Q^0$).

Observe that (I) implies that each $A \in \mathcal{O}\text{b}(\mathcal{A})$ has an acyclic resolution $P_\bullet \longrightarrow A \longrightarrow 0$, with all P_n projective, or an acyclic resolution $0 \longrightarrow A \longrightarrow Q^\bullet$, with all Q^n injective. These are called *projective* (resp. *injective*) resolutions. For $\mathcal{M}\text{od}(R)$, both exist. (For $\mathcal{S}h(X)$, the category of sheaves of abelian groups on the topological space, X, injective resolutions exist.)

(II) $\mathcal{A}$ *possesses finite coproducts (resp. finite products, or both).* This holds for $\mathcal{M}\text{od}(R)$ and $\mathcal{S}h(X)$.

Remark: The following simple fact about projectives will be used in several of the subsequent proofs: *If we have a diagram*



in which

(1) P is projective.

(2) The lower sequence is exact (i.e., $\operatorname{Im}\varphi = \operatorname{Ker}\psi$*).*

(3) $\psi \circ f = 0$,

then there is a map $\theta\colon P \to A$ lifting f (as shown by the dotted arrow above). Indeed, $\psi \circ f = 0$ implies that $\operatorname{Im} f \subseteq \operatorname{Ker}\psi$; so, we have $\operatorname{Im} f \subseteq \operatorname{Im}\varphi$, and we are reduced to the usual situation where φ is surjective. Of course, the dual property holds for injectives.

Proposition 5.1 *Suppose we are given an exact sequence*

$$0 \longrightarrow A' \xrightarrow{\psi} A \xrightarrow{\varphi} A'' \longrightarrow 0$$

and both A' and A'' possess projective resolutions $P'_\bullet \longrightarrow A' \longrightarrow 0$ and $P''_\bullet \longrightarrow A'' \longrightarrow 0$. Then, there exists a projective resolution of A, denote it $P_\bullet$, and maps of complexes $P'_\bullet \longrightarrow P_\bullet$ and $P_\bullet \longrightarrow P''_\bullet$, so that the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P'_\bullet & \xrightarrow{\psi_\bullet} & P_\bullet & \xrightarrow{\varphi_\bullet} & P''_\bullet & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A' & \xrightarrow{\psi} & A & \xrightarrow{\varphi} & A'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

commutes and has exact rows and columns. A similar result holds for injective resolutions.

Proof. We have $0 \longrightarrow P'_n \longrightarrow P_n \longrightarrow P''_n \longrightarrow 0$ if P_n exists and P''_n is projective. So, the sequence would split and $P_n = P'_n \amalg P''_n$. Look at

$$0 \longrightarrow P'_n \xrightarrow{\psi_n} \underbrace{P'_n \amalg P''_n}_{P_n} \underset{\varphi_n}{\overset{i''_n}{\rightleftarrows}} P''_n \longrightarrow 0.$$

We have a map $P_n \longrightarrow P_n$ *via* $i''_n \circ \varphi_n$; we also have the map $\mathrm{id} - i''_n \circ \varphi_n$ and

$$\varphi_n \circ (\mathrm{id} - i''_n \circ \varphi_n) = \varphi_n - \varphi_n \circ i''_n \circ \varphi_n = \varphi_n - \mathrm{id}''_n \circ \varphi_n = \varphi_n - \varphi_n \equiv 0.$$

It follows that $\mathrm{id} - i''_n \circ \varphi_n$ factors through ψ_n, i.e.,

$$\mathrm{id} - i''_n \circ \varphi_n\colon P_n \longrightarrow P'_n \xrightarrow{\psi_n} P_n.$$

So, we may speak of "elements of P_n" as pairs $x_n = (x'_n, x''_n)$, where $x''_n = \varphi_n(x_n)$ and $(\mathrm{id} - i''_n \circ \varphi_n)(x_n) = x_n - i''_n(x''_n) = x'_n$. Therefore,

$$x_n = \text{“}x'_n + i''_n(x''_n)\text{”} = (x'_n, x''_n).$$

This shows that for every n, we should define P_n as $P'_n \amalg P''_n$. We need $d_\bullet$ on $P_\bullet$. The map d_n takes P_n to P_{n-1}. These d_n should make the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P'_{n+1} & \longrightarrow & P_{n+1} & \longrightarrow & P''_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{n+1}} & & \downarrow{\scriptstyle d_{n+1}} & & \downarrow{\scriptstyle d''_{n+1}} & & \\
0 & \longrightarrow & P'_n & \xrightarrow{\psi_n} & P_n & \xrightarrow{\varphi_n} & P''_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_n} & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d''_n} & & \\
0 & \longrightarrow & P'_{n-1} & \xrightarrow{\psi_{n-1}} & P_{n-1} & \xrightarrow{\varphi_{n-1}} & P''_{n-1} & \longrightarrow & 0
\end{array}$$

commute and $d_n \circ d_{n+1} = 0$. In terms of pairs, $x_n = (x'_n, x''_n)$, where $\psi_n(x'_n) = (x'_n, 0)$ and $\varphi_n(x_n) = x''_n$, the commutativity of the lower left square requires

$$d_n(x'_n, 0) = (d'_n x'_n, 0).$$

How about $(0, x''_n)$? Observe that we have $\varphi_{n-1} d_n(0, x''_n) = d''_n(x''_n)$. Write $d_n(0, x''_n) = (\alpha_{n-1}, \beta_{n-1})$; we know that $\varphi_{n-1}(\alpha_{n-1}, \beta_{n-1}) = \beta_{n-1}$, thus,

$$d_n(0, x''_n) = (\alpha_{n-1}, d''_n x''_n).$$

So, *we need a map* $\theta_n \colon P''_n \to P'_{n-1}$; namely $\theta_n(x''_n) = \alpha_{n-1}$, the first component of $d_n(0, x''_n)$. If we know θ_n, then

$$\begin{array}{rcl}
d_n(x_n) & = & d_n(x'_n, x''_n) = d_n((x'_n, 0) + (0, x''_n)) \\
 & = & (d'_n(x'_n), 0) + d_n(0, x''_n) \\
 & = & (d'_n(x'_n), 0) + (\theta_n(x''_n), d''_n(x''_n)) \\
 & = & (d'_n(x'_n) + \theta_n(x''_n), d''_n(x''_n)).
\end{array}$$

Everything would be OK in one layer from P_n to P_{n-1}, but we need $d_n \circ d_{n+1} = 0$. Since

$$d_{n+1}(x_{n+1}) = d_{n+1}(x'_{n+1}, x''_{n+1}) = (d'_{n+1}(x'_{n+1}) + \theta_{n+1}(x''_{n+1}), d''_{n+1}(x''_{n+1})),$$

we must have

$$\begin{array}{rcl}
d_n \circ d_{n+1}(x_{n+1}) & = & (d'_n \circ d'_{n+1}(x'_{n+1}) + d'_n \circ \theta_{n+1}(x''_{n+1}) + \theta_n \circ d''_{n+1}(x''_{n+1}), d''_n \circ d''_{n+1}(x''_{n+1})) \\
 & = & (d'_n \circ \theta_{n+1}(x''_{n+1}) + \theta_n \circ d''_{n+1}(x''_{n+1}), 0) = 0.
\end{array}$$

Therefore, *we need*

$$d'_n \circ \theta_{n+1} + \theta_n \circ d''_{n+1} = 0, \quad \text{for all } n \geq 1. \tag{$\dagger_n$}$$

The case $n = 0$ requires commutativity in the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P'_1 & \longrightarrow & P_1 & \longrightarrow & P''_1 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_1} & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d''_1} & & \\
0 & \longrightarrow & P'_0 & \xrightarrow{\psi_0} & P_0 & \xrightarrow{\varphi_0} & P''_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
0 & \longrightarrow & A' & \xrightarrow{\psi} & A & \xrightarrow{\varphi} & A'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Since P_0'' is projective, there is a map $\sigma\colon P_0'' \to A$ so that

$$\varphi \circ \sigma = \epsilon''.$$

We can now define ϵ. We have $\epsilon(x_0) = \epsilon((x_0', x_0'')) = \epsilon((x_0', 0)) + \epsilon((0, x_0''))$ and $\epsilon((x_0', 0)) = \psi\epsilon'(x_0')$, as the lower left square commutes. We also have

$$\varphi(\epsilon(0, x_0'')) = \epsilon''(\varphi_0(0, x_0'')) = \epsilon''(x_0'') = \varphi\sigma(x_0'').$$

Consequently, $\epsilon((0, x_0'')) - \sigma(x_0'')$ is killed by φ and it follows that

$$\epsilon((x_0', x_0'')) = \psi\epsilon'(x_0') + \sigma(x_0'').$$

We construct the map θ_n by induction on n and begin with $n = 1$. Note that

$$0 = \epsilon d_1(x_1', x_1'') = \epsilon(d_1'(x_1') + \theta_1(x_1''), d_1''(x_1'')) = \psi\epsilon'(d_1'(x_1') + \theta_1(x_1'')) + \sigma d_1''(x_1'').$$

Therefore, we need to have

$$\psi\epsilon'\theta_1 + \sigma d_1'' = 0. \tag{††}$$

Construction of θ_1: In the diagram

$$\begin{array}{ccccccc} & & P_1'' & & & & \\ & \overset{\theta_1}{\swarrow} & \downarrow{\scriptstyle -\sigma d_1''} & & & & \\ P_0' & \xrightarrow[\psi\epsilon']{} & A & \longrightarrow & A'' & \longrightarrow & 0 \end{array}$$

as P_1'' is projective, the map $-\sigma d_1''$ lifts to a map $\theta_1\colon P_1'' \to P_0'$; thus (††) holds.

Next, we construct θ_2: Consider the diagram

$$\begin{array}{ccccccc} & & P_2'' & & & & \\ & \overset{\theta_2}{\swarrow} & \downarrow{\scriptstyle -\theta_1 d_2''} & & & & \\ P_1' & \xrightarrow[d_1']{} & P_0' & \xrightarrow[\epsilon']{} & A' & \longrightarrow & 0. \end{array}$$

If we know that $\epsilon'(-\theta_1 d_2'') = 0$, we can lift our map and get θ_2, as shown. But, apply ψ, then by (††), we get

$$\psi\epsilon'\theta_1 d_2'' = \sigma d_1'' d_2'' = 0.$$

Yet, ψ is an injection, so $\epsilon'\theta_1 d_2'' = 0$. Thus, the map θ_2 exists and we have $d_1'\theta_2 = -\theta_1 d_2''$, i.e. $(\dagger_1)$ holds.

Finally, consider the case $n > 1$ and assume the θ_r are constructed for $r \leq n$ and $(\dagger_k)$ holds for all $k \leq n-1$. By the induction hypothesis,

$$-d_{n-1}'\theta_n d_{n+1}'' = \theta_{n-1} d_n'' d_{n+1}'' = 0.$$

We have the diagram

$$\begin{array}{ccccccc} & & P_{n+1}'' & & & & \\ & \overset{\theta_{n+1}}{\swarrow} & \downarrow{\scriptstyle -\theta_n d_{n+1}''} & & & & \\ P_n' & \xrightarrow[d_n']{} & P_{n-1}' & \xrightarrow[d_{n-1}']{} & P_{n-2}' & & \end{array}$$

in which P_{n+1}'' is projective, $-d_{n-1}'\theta_n d_{n+1}'' = 0$ and the lower sequence is exact. Therefore, $-\theta_n d_{n+1}''$ lifts to θ_{n+1} so that

$$d_n'\theta_{n+1} = -\theta_n d_{n+1}'',$$

which is $(\dagger_n)$. The case of injectives follows from the dual category. □

Definition 5.1 Say

$$\cdots \longrightarrow X^{-n} \xrightarrow{d_X^{-n}} X^{-n+1} \xrightarrow{d_X^{-n+1}} \cdots \longrightarrow X^{-1} \xrightarrow{d_X^{-1}} X^0 \xrightarrow{d_X^0} X^1 \longrightarrow \cdots \longrightarrow X^n \xrightarrow{d_X^n} X^{n+1} \longrightarrow \cdots$$

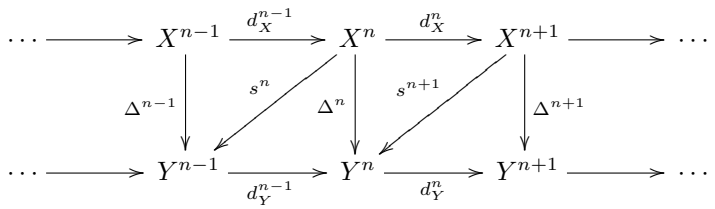
and

$$\cdots \longrightarrow Y^{-n} \xrightarrow{d_Y^{-n}} Y^{-n+1} \xrightarrow{d_Y^{-n+1}} \cdots \longrightarrow Y^{-1} \xrightarrow{d_Y^{-1}} Y^0 \xrightarrow{d_Y^0} Y^1 \longrightarrow \cdots \longrightarrow Y^n \xrightarrow{d_Y^n} Y^{n+1} \longrightarrow \cdots$$

are objects of $\mathrm{Kom}(\mathcal{A})$. A *homotopy* between two maps $f^\bullet, g^\bullet \colon X^\bullet \longrightarrow Y^\bullet$ is a sequence, $\{s^n\}$, of maps $s^n \colon X^n \to Y^{n-1}$ so that

$$f^n - g^n = s^{n+1} \circ d_X^n + d_Y^{n-1} \circ s^n, \quad \text{for all } n,$$

as illustrated in the diagram below:



where $\Delta^n = f^n - g^n$.

Remark: From $f^\bullet$ and $g^\bullet$ we get two maps on homology:

$$\begin{aligned} H^\bullet(f^\bullet) \colon H^\bullet(X^\bullet) &\longrightarrow H^\bullet(Y^\bullet) \\ H^\bullet(g^\bullet) \colon H^\bullet(X^\bullet) &\longrightarrow H^\bullet(Y^\bullet). \end{aligned}$$

But, *when $f^\bullet$ and $g^\bullet$ are homotopic, these maps on homology are* **equal**. Indeed,

$$\begin{aligned} H^\bullet(f^\bullet - g^\bullet) &= H^\bullet(s^{\bullet+1}d^\bullet) + H^\bullet(d^{\bullet-1}s^\bullet) \\ &= H^\bullet(s^{\bullet+1})H^\bullet(d^\bullet) + H^\bullet(d^{\bullet-1})H^\bullet(s^\bullet). \end{aligned}$$

As $H^\bullet(d^\bullet) = 0$ and $H^\bullet(d^{\bullet-1}) = 0$, we get

$$H^\bullet(f^\bullet) - H^\bullet(g^\bullet) = H^\bullet(f^\bullet - g^\bullet) = 0,$$

as claimed.

Now, based on this, we define the category $\mathrm{Kom}(\mathcal{A})$ by changing the morphisms in $\mathrm{PreKom}(\mathcal{A})$.

Definition 5.2 $\mathrm{Kom}(\mathcal{A})$ is *the category whose objects are the chain complexes from $\mathcal{A}$ and whose morphisms are the homotopy classes of chain maps of the complexes.*

Theorem 5.2 *Under the usual assumptions on $\mathcal{A}$, suppose $P^\bullet(A) \longrightarrow A \longrightarrow 0$ is a projective resolution of A and $X^\bullet(A') \longrightarrow A' \longrightarrow 0$ is an acyclic resolution of A'. If $\xi \colon A \to A'$ is a map in $\mathcal{A}$, it lifts uniquely to a morphism $P^\bullet(A) \longrightarrow X^\bullet(A')$ in $\mathrm{Kom}(\mathcal{A})$. [If $0 \longrightarrow A \longrightarrow Q^\bullet(A)$ is an injective resolution of A and $0 \longrightarrow A' \longrightarrow Y^\bullet(A')$ is an acyclic resolution of A', then any map $\xi \colon A' \to A$ lifts uniquely to a morphism $Y^\bullet(A') \longrightarrow Q^\bullet(A)$ in $\mathrm{Kom}(\mathcal{A})$.]*

Proof. We begin by proving the existence of the lift, stepwise, by induction. Since we have morphisms $\epsilon\colon P_0(A) \to A$ and $\xi\colon A \to A'$, we get a morphism $\xi \circ \epsilon\colon P_0(A) \to A'$ and we have the diagram

$$\begin{array}{ccccc} & & P_0(A) & & \\ & \overset{f_0}{\swarrow} & \downarrow{\scriptstyle \xi\circ\epsilon} & & \\ X_0(A') & \longrightarrow & A' & \longrightarrow & 0. \end{array}$$

As $P_0(A)$ is projective, the map $f_0\colon P_0(A) \to X_0(A')$ exists and makes the diagram commute. Assume the lift exists up to level n. We have the diagram

$$\begin{array}{ccccccc} P_{n+1}(A) & \xrightarrow{d^P_{n+1}} & P_n(A) & \xrightarrow{d^P_n} & P_{n-1}(A) & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ X_{n+1}(A') & \xrightarrow[d^X_{n+1}]{} & X_n(A') & \xrightarrow[d^X_n]{} & X_{n-1}(A') & \longrightarrow & \cdots, \end{array} \tag{$\dagger$}$$

so we get a map $f_n \circ d^P_{n+1}\colon P_{n+1}(A) \to X_n(A')$ and a diagram

$$\begin{array}{ccccc} & & P_{n+1}(A) & & \\ & \overset{f_{n+1}}{\swarrow} & \downarrow{\scriptstyle f_n\circ d^P_{n+1}} & & \\ X_{n+1}(A') & \longrightarrow & X_n(A') & \xrightarrow[d^X_n]{} & X_{n-1}(A'). \end{array}$$

But, by commutativity in ($\dagger$), we get

$$d^X_n \circ f_n \circ d^P_{n+1} = f_{n-1} \circ d^P_n \circ d^P_{n+1} = 0.$$

Now, $P_{n+1}(A)$ is projective and the lower row in the above diagram is exact, so there is a lifting $f_{n+1}\colon P_{n+1}(A) \to X_{n+1}(A')$, as required.

Now, we prove uniqueness (in $\mathrm{Kom}(\mathcal{A})$). Say we have two lifts $\{f_n\}$ and $\{g_n\}$. Construct the homotopy $\{s_n\}$, by induction on n.

For the base case, we have the diagram

$$\begin{array}{ccccccc} & & P_0(A) & \xrightarrow{\epsilon} & A & \longrightarrow & 0 \\ & \overset{s_0}{\swarrow} & {\scriptstyle f_0}\downarrow \; \downarrow{\scriptstyle g_0} & & \downarrow{\scriptstyle \xi} & & \\ X_1(A') & \xrightarrow[d^X_1]{} & X_0(A') & \xrightarrow[\epsilon']{} & A' & \longrightarrow & 0. \end{array}$$

As $\epsilon'(f_0 - g_0) = (\xi - \xi)\epsilon = 0$, the lower row is exact and $P_0(A)$ is projective, we get our lifting $s_0\colon P_0(A) \to X_1(A')$ with $f_0 - g_0 = d^X_1 \circ s_0$.

Assume, for the induction step, that we already have $s_0, \ldots, s_{n-1}$. Write $\Delta_n = f_n - g_n$, then we get the diagram

$$\begin{array}{ccccccc} & & P_n(A) & \xrightarrow{d^P_n} & P_{n-1}(A) & \longrightarrow & P_{n-2}(A) \longrightarrow \cdots \\ & & {\scriptstyle \Delta_n}\downarrow & \overset{s_{n-1}}{\swarrow} & \downarrow{\scriptstyle \Delta_{n-1}} & & \downarrow{\scriptstyle \Delta_{n-2}} \\ X_{n+1}(A') & \longrightarrow & X_n(A') & \xrightarrow[d^X_n]{} & X_{n-1}(A') & \longrightarrow & X_{n-2} \longrightarrow \cdots \end{array} \tag{$\ddagger$}$$

There results a map $\Delta_n - s_{n-1} \circ d_n^P \colon P_n(A) \longrightarrow X_n(A')$ and a diagram

$$\begin{array}{ccccc} & & P_n(A) & & \\ & & \downarrow{\scriptstyle \Delta_n - s_{n-1}\circ d_n^P} & & \\ X_{n+1}(A') & \xrightarrow[d_{n+1}^X]{} & X_n(A') & \xrightarrow[d_n^X]{} & X_{n-1}(A'). \end{array}$$

As usual, if we show that $d_n^X \circ (\Delta_n - s_{n-1} \circ d_n^P) = 0$, then there will be a lift $s_n \colon P_n(A) \to X_{n+1}(A')$ making the diagram commute. Now, by the commutativity of (††), we have $d_n^X \circ \Delta_n = \Delta_{n-1} \circ d_n^P$; so

$$d_n^X \circ (\Delta_n - s_{n-1} \circ d_n^P) = \Delta_{n-1} \circ d_n^P - d_n^X \circ s_{n-1} \circ d_n^P.$$

By the induction hypothesis, $\Delta_{n-1} = f_{n-1} - g_{n-1} = s_{n-2} \circ d_{n-1}^P + d_n^X \circ s_{n-1}$, and therefore

$$\Delta_{n-1} \circ d_n^P - d_n^X \circ s_{n-1} \circ d_n^P = s_{n-2} \circ d_{n-1}^P \circ d_n^P + d_n^X \circ s_{n-1} \circ d_n^P - d_n^X \circ s_{n-1} \circ d_n^P = 0.$$

Hence, s_n exists and we are done. The case of injective resolutions follows by duality. □

Corollary 5.3 *Say $\xi \colon A \to A'$ is a morphism in $\mathcal{A}$ and P, P' are respective projective resolutions of A and A'. Then, ξ extends uniquely to a morphism $P \longrightarrow P'$ of* $\mathrm{Kom}(\mathcal{A})$. *(A similar result holds for injective resolutions.)*

Corollary 5.4 *If P and P' are two projective resolutions of the same object, A, of $\mathcal{A}$, then in* $\mathrm{Kom}(\mathcal{A})$, *$P$ is uniquely isomorphic to P'. (Similarly for injective resolutions.)*

Proof. We have the identity morphism, $\mathrm{id} \colon A \to A$, so we get unique lifts, f and g in $\mathrm{Kom}(\mathcal{A})$, where $f \colon P \to P'$ and $g \colon P' \to P$ (each lifting the identity). But then, $f \circ g$ and $g \circ f$ lift the identity to endomorphisms of P' and P respectively. Yet, the identity on each is also a lift; by the theorem we must have $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$ *in* $\mathrm{Kom}(\mathcal{A})$. □

Using the same methods and no new ideas, we can prove the following important proposition. The proof will be omitted–it provides nothing new and has many messy details.

Proposition 5.5 *Suppose we have a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & {\scriptstyle f'}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f''}\downarrow & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0. \end{array}$$

(We call such a diagram a "small commutative diagram.") Given objects, $X'^{\bullet}, X^{\bullet}$, etc. of $\mathrm{Kom}(\mathcal{A})$ *as below, an exact sequence*

$$0 \longrightarrow X'^{\bullet} \longrightarrow X^{\bullet} \longrightarrow X''^{\bullet} \longrightarrow 0$$

over the A-sequence and an exact sequence

$$0 \longrightarrow Y'^{\bullet} \longrightarrow Y^{\bullet} \longrightarrow Y''^{\bullet} \longrightarrow 0$$

over the B-sequence, assume $X''^{\bullet}$ and $Y''^{\bullet}$ are projective resolutions, while $X'^{\bullet}$ and $Y'^{\bullet}$ are acyclic resolutions. Suppose further we have maps $\Phi' \colon X'^{\bullet} \to Y'^{\bullet}$ and $\Phi'' \colon X''^{\bullet} \to Y''^{\bullet}$ over f' and f''. Then, there exists a unique $\Phi \colon X^{\bullet} \to Y^{\bullet}$ (over f) in $\mathrm{Kom}(\mathcal{A})$ *so that the "big diagram" of augmented complexes commutes and $X^{\bullet}$ and $Y^{\bullet}$ are acyclic.*

Definition 5.3 If T is a functor (resp. cofunctor) on $\mathcal{A}$ to another abelian category $\mathcal{B}$, the *left derived functors* of T are the functors, L_nT, given by

$$(L_nT)(A) = H_n(T(P_\bullet(A))),$$

where $P_\bullet(A)$ is any projective resolution of A (resp., when T is a cofunctor, the *right derived functors of* T are the functors, R^nT, given by $(R^nT)(A) = H^n(T(P_\bullet(A)))$).

If T is a functor, its *right derived functors* are the functors, R^nT, given by

$$(R^nT)(A) = H^n(T(Q^\bullet(A))),$$

where $Q^\bullet(A)$ is any injective resolution of A (when T is a cofunctor, the *left derived functors of* T, written $(L_nT)(A)$, are given by $(L_nT)(A) = H_n(T(Q^\bullet(A)))$).

The definition of derived functors is somewhat complicated and certainly unmotivated. Much of the complication disappears when one observes that the values of either right or left derived functors are just the homology objects of a complex; that, no matter whether T is a functor or a cofunctor, *right (resp. left) derived functors are the homology of a right (resp. left) complex* (homology of a right complex is usually called *cohomology*). Thus, for a functor, T, an injective resolution will yield a right complex and so is used to compute right derived functors of T. *Mutatis mutandis* for projective resolutions; for cofunctors, T, simply reverse all arrows. Of course, what we are investigating here is the *effect of* T *on a resolution*. We *always get a complex*, but acyclicity is in general not preserved and *the deviation from acyclicity is measured by the derived functors*.

As for motivation, the concept arose from experience first from algebraic topology later from homological methods applied to pure algebra. Indeed the notion of derived functor took a long time to crystallize from all the gathered examples and results of years of work. Consider, for example, a group G and the abelian category of G-modules. On this category, we have already met the left exact functor $M \rightsquigarrow M^G$ with values in $\mathcal{A}$b. Our notation for this functor was $H^0(G, M)$. Now, in Chapters 1 and 4, we constructed a sequence of functors of M, namely $H^n(G, M)$. An obvious question is: Are the functors $H^n(G, -)$ the right derived functors of $H^0(G, -)$? We will answer this question below by characterizing the derived functors of a given functor, T.

Further remarks:

(1) The definition makes sense, i.e., derived functors are independent of the resolution chosen. Use Corollary 5.4 to see this.

(2) Suppose T is a functor and A is a projective object of $\mathcal{A}$ (resp. an injective object of $\mathcal{A}$), then $(L_nT)(A) = (0)$ for $n > 0$ (resp. $(R^nT)(A) = (0)$ for $n > 0$). If T is a cofunctor, interchange conclusions. (A is its own resolution in either case; so, remark (1) provides the proof.)

(3) If T is exact, then L_nT and R^nT are (0) for $n > 0$ (the homology of an acyclic complex is zero).

Proposition 5.6 *If T is any functor, there are always maps of functors $T \longrightarrow R^0T$ and $L_0T \longrightarrow T$. If Q is injective and P projective, then $T(Q) \longrightarrow (R^0T)(Q)$ and $(L_0T)(P) \longrightarrow T(P)$ are isomorphisms. When T is a cofunctor interchange P and Q. For either a functor or a cofunctor, T, the zeroth derived functor R^0T is always left-exact while L_0T is always right-exact. A necessary and sufficient condition that T be left-exact (resp. right-exact) is that $T \longrightarrow R^0T$ be an isomorphism of functors (resp. $L_0T \longrightarrow T$ be an isomorphism of functors). Finally, the functor map $T \longrightarrow R^0T$ induces an isomorphism of functors $R^nT \longrightarrow R^nR^0T$ for all $n \geq 0$ and similarly there is an isomorphism of functors $L_nL_0T \longrightarrow L_nT$.*

Proof. Most of this is quite trivial. The existence of the maps $T \longrightarrow R^0T$ and $L_0T \longrightarrow T$ follows immediately from the definition (and the strong uniqueness of Corollary 5.4 as applied in Remark (1) above). That R^0T is left exact is clear because it is a kernel and because the exact sequence of resolutions lifting a given exact sequence can always be chosen as split exact at each level. Similarly, L_0T is right exact as a cokernel. Of course, if T is isomorphic to R^0T it must be left exact, while if T is left exact, the terms in the augmented complex outlined by the braces form an exact sequence:

$$\underbrace{0 \longrightarrow T(A) \longrightarrow TQ^0(A) \overset{T(d^0)}{\longrightarrow} TQ^1(A)} \longrightarrow \cdots .$$

Thus, the canonical map $T(A) \longrightarrow (R^0T)(A) = \operatorname{Ker} T(d^0)$ is an isomorphism. Similarly for right exactness and L_0.

Should Q be injective, the sequence

$$0 \longrightarrow Q \overset{\mathrm{id}}{\longrightarrow} Q \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

is an injective resolution of Q and it shows that $T(Q)$ is equal to $(R^0T)(Q)$. Similarly for P and for cofunctors. But now if A is arbitrary and $Q^\bullet(A)$ is an injective resolution of A, the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & T(A) & \longrightarrow & T(Q^0(A)) & \longrightarrow & T(Q^1(A)) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (R^0T)(A) & \longrightarrow & (R^0T)Q^0(A) & \longrightarrow & (R^0T)Q^1(A) & \longrightarrow & \cdots
\end{array}$$

in which the vertical arrows except the leftmost are isomorphisms shows immediately that $R^nT \longrightarrow R^n(R^0T)$ is an isomorphism for all $n \geq 0$. Similarly for $L_n(L_0T) \longrightarrow L_nT$. $\square$

The point of the above is that *right derived functors belong with left exact functors and similarly if we interchange left and right*.

There are two extremely important examples of derived functors—they appear over and over in many applications.

Definition 5.4 If $\mathcal{A}$ is any abelian category and $\mathcal{B} = \mathcal{A}\mathrm{b}$ (abelian groups), write $T_B(A) = \operatorname{Hom}_{\mathcal{A}}(A, B)$, for fixed B. (This is a left-exact cofunctor, so we want its right derived functors R^nT_B). Set

$$\operatorname{Ext}^n_{\mathcal{A}}(A, B) = (R^nT_B)(A). \qquad (*)$$

If $\mathcal{A} = \mathcal{M}\mathrm{od}(R^{\mathrm{op}})$ and $\mathcal{B} = \mathcal{A}\mathrm{b}$, set $S_B(A) = A \otimes_R B$, for fixed B. (This is a right-exact functor, so we want its left-derived functors L_nS_B). Set

$$\operatorname{Tor}^R_n(A, B) = (L_nS_B)(A). \qquad (**)$$

To be more explicit, in order to compute $\operatorname{Ext}^\bullet_{\mathcal{A}}(A, B)$, we take a projective resolution of A

$$P^\bullet \longrightarrow A \longrightarrow 0$$

apply $\operatorname{Hom}_{\mathcal{A}}(-, B)$ and compute the cohomology of the (right) complex $\operatorname{Hom}_{\mathcal{A}}(P^\bullet, B)$. For the tensor product, we similarly take a projective resolution of the R^{op} module, A,

$$P^\bullet \longrightarrow A \longrightarrow 0$$

apply $- \otimes_R B$ and compute the homology of the complex $P^\bullet \otimes_R B$. Because $\mathrm{Hom}_{\mathcal{A}}(-, B)$ is left exact and $- \otimes_R B$ is right exact, we have

$$\begin{aligned} \mathrm{Hom}_{\mathcal{A}}(A, B) &= \mathrm{Ext}^0_{\mathcal{A}}(A, B) \\ A \otimes_R B &= \mathrm{Tor}^R_0(A, B). \end{aligned}$$

The following proposition, which we will call the *basic lemma*, will give us a chief property of derived functors and help us characterize the sequence of derived functors of a given functor.

Proposition 5.7 *(Long (co)homology sequence) Suppose $X^\bullet, Y^\bullet, Z^\bullet$ are complexes and*

$$0 \longrightarrow X^\bullet \longrightarrow Y^\bullet \longrightarrow Z^\bullet \longrightarrow 0$$

is exact in pre-$\mathrm{Kom}(\mathcal{A})$ *(also OK in* $\mathrm{Kom}(\mathcal{A})$*). Then, there exists a long exact sequence of homology (or cohomology)*

$$\begin{array}{l} \cdots \longrightarrow H^{n-1}(Z^\bullet) \longrightarrow \\ H^n(X^\bullet) \longrightarrow H^n(Y^\bullet) \longrightarrow H^n(Z^\bullet) \longrightarrow \\ H^{n+1}(X^\bullet) \longrightarrow H^{n+1}(Y^\bullet) \longrightarrow H^{n+1}(Z^\bullet) \longrightarrow \\ H^{n+2}(X^\bullet) \longrightarrow \cdots \end{array}$$

(for all n). The maps $\delta^n \colon H^n(Z^\bullet) \to H^{n+1}(X^\bullet)$ are called connecting homomorphisms.

Proof. Look at the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X^{n-1} & \longrightarrow & Y^{n-1} & \longrightarrow & Z^{n-1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X^n & \longrightarrow & Y^n & \longrightarrow & Z^n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^n_X} & & \downarrow{\scriptstyle d^n_Y} & & \downarrow{\scriptstyle d^n_Z} & & \\ 0 & \longrightarrow & X^{n+1} & \longrightarrow & Y^{n+1} & \longrightarrow & Z^{n+1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X^{n+2} & \longrightarrow & Y^{n+2} & \longrightarrow & Z^{n+2} & \longrightarrow & 0 \end{array}$$

and apply the snake lemma to the rows n and $n+1$. We get

$$0 \longrightarrow \mathrm{Ker}\, d^n_X \longrightarrow \mathrm{Ker}\, d^n_Y \longrightarrow \mathrm{Ker}\, d^n_Z \xrightarrow{\delta} \mathrm{Coker}\, d^n_X \longrightarrow \mathrm{Coker}\, d^n_Y \longrightarrow \mathrm{Coker}\, d^n_Z \longrightarrow 0.$$

If we look at $\mathrm{Im}\, d^{n-1}_X$ and apply the map $X^\bullet \longrightarrow Y^\bullet$, we land in $\mathrm{Im}\, d^{n-1}_Y$, etc. Thus, at *every* level we get that

$$H^n(X^\bullet) \longrightarrow H^n(Y^\bullet) \longrightarrow H^n(Z^\bullet) \quad \text{is exact.}$$

Now, the connecting map, δ, of the snake lemma maps $\mathrm{Ker}\, d^n_Z$ to $H^{n+1}(X^\bullet)$. But, clearly, $\mathrm{Im}\, d^{n-1}_Z$ goes to zero under δ (because every element of $\mathrm{Im}\, d^{n-1}_Z$ comes from some element in Y^{n-1}). So, we get the connecting homomorphism

$$\delta^n \colon H^n(Z^\bullet) \longrightarrow H^{n+1}(X^\bullet).$$

A diagram chase proves exactness (DX). $\square$

Corollary 5.8 *Given a commutative diagram of complexes*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X^\bullet & \longrightarrow & Y^\bullet & \longrightarrow & Z^\bullet & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \widetilde{X}^\bullet & \longrightarrow & \widetilde{Y}^\bullet & \longrightarrow & \widetilde{Z}^\bullet & \longrightarrow & 0 \end{array}$$

we have the big diagram of long exact sequences

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & H^n(X^\bullet) & \longrightarrow & H^n(Y^\bullet) & \longrightarrow & H^n(Z^\bullet) & \longrightarrow & H^{n+1}(X^\bullet) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & H^n(\widetilde{X}^\bullet) & \longrightarrow & H^n(\widetilde{Y}^\bullet) & \longrightarrow & H^n(\widetilde{Z}^\bullet) & \longrightarrow & H^{n+1}(\widetilde{X}^\bullet) & \longrightarrow & \cdots \end{array} \qquad (**)$$

which commutes.

Proof. Chase the diagram in the usual way. □

Suppose T is a right-exact functor on $\mathcal{A}$ and

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is an exact sequence in $\mathcal{A}$. Resolve this exact sequence (as we have shown is possible, cf. Proposition 5.1) to get

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P^\bullet(A) & \longrightarrow & P^\bullet(B) & \longrightarrow & P^\bullet(C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \epsilon_A} & & \downarrow{\scriptstyle \epsilon_B} & & \downarrow{\scriptstyle \epsilon_C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Then, as L_nT is the homology of the $TP^\bullet$ complexes (still horizontaly exact on the complex level, as our objects are projectives and the horizontal complex sequences split!), from the basic lemma, we get the long exact sequence (of derived functors)

$$\begin{array}{ccccccc} \cdots & \longrightarrow & L_nT(A) & \longrightarrow & L_nT(B) & \longrightarrow & L_nT(C) \\ & & \longrightarrow & L_{n-1}T(A) & \longrightarrow \cdots & & \cdots \longrightarrow \\ & & \longrightarrow \cdots & & \cdots & \longrightarrow & L_1T(C) \\ & & \longrightarrow & T(A) & \longrightarrow & T(B) & \longrightarrow & T(C) & \longrightarrow & 0 \end{array}$$

Moreover, we have a commutative diagram corresponding to $(**)$:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & (L_nT)(A) & \longrightarrow & (L_nT)(B) & \longrightarrow & (L_nT)(C) & \longrightarrow & (L_{n-1}T)(A) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & (L_nT)(\widetilde{A}) & \longrightarrow & (L_nT)(\widetilde{B}) & \longrightarrow & (L_nT)(\widetilde{C}) & \longrightarrow & (L_{n-1}T)(\widetilde{A}) & \longrightarrow & \cdots \end{array}$$

stemming from Proposition 5.5.

We can abstract this behavior of the sequences $\{L_nT\}_{n=0}^{\infty}$ and $\{R^nT\}_{n=0}^{\infty}$ according to the following definition:

Definition 5.5 A *δ-functor* (resp. *∂-functor*) is a sequence, $\{T^n\}$, (resp. a sequence, $\{T_n\}$) of functors so that for every exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

in $\mathcal{A}$, we have a long exact sequence

$$\begin{array}{l} 0 \longrightarrow T^0(A) \longrightarrow T^0(B) \longrightarrow T^0(C) \longrightarrow \\ \longrightarrow T^1(A) \longrightarrow T^1(B) \longrightarrow T^1(C) \longrightarrow \\ \longrightarrow T^2(A) \longrightarrow \cdots \end{array}$$

and it is functorial in morphisms of exact sequences (similarly for ∂-functors, but reverse the arrows). [This means that for every commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0, \end{array}$$

where the rows are exact, the induced diagram

$$\begin{array}{ccccccccccccc} 0 & \longrightarrow & T^0(A) & \longrightarrow & T^0(B) & \longrightarrow & T^0(C) & \longrightarrow & T^1(A) & \cdots \longrightarrow & T^{n-1}(C) & \longrightarrow & T^n(A) & \longrightarrow \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & T^0(A') & \longrightarrow & T^0(B') & \longrightarrow & T^0(C') & \longrightarrow & T^1(A') & \cdots \longrightarrow & T^{n-1}(C') & \longrightarrow & T^n(A') & \longrightarrow \cdots \end{array}$$

is also commutative.]

Of course, our results on derived functors give us

Proposition 5.9 *The sequence of derived functors $\{R^nT\}$ (resp. $\{L_nT\}$) for a left-exact (resp. right-exact) functor, T, forms a δ-functor (resp. ∂-functor).*

Another δ-functor is the sequence $\{H^n(G,-)\}_{n=0}^{\infty}$ defined on the category of G-modules. To get at the characterization of derived functors, we need

Definition 5.6 A δ-functor $\{T^n\}$ is *universal* iff for all δ-functors, $\{S^n\}$, given a map (of functors), $f^0\colon T^0 \to S^0$, there exists a *unique* extension of f^0 to a map $\{f^n\colon T^n \to S^n\}$ **of δ-functors**. *Similarly for ∂-functors, but reverse the directions of the arrows.*

Remark: *Say $\{T^n\}$ and $\{S^n\}$ are universal δ-functors and $f^0\colon T^0 \cong S^0$ is an isomorphism of functors. Then, there is a unique isomorphism $\{f^n\colon T^n \to S^n\}$ of δ-functors lifting f^0. That is, universal δ-functors are determined by their components in dimension* 0.

Proof. Since $f^0\colon T^0 \cong S^0$ is an isomorphism of functors, there is a map of functors, $g^0\colon S^0 \to T^0$ so that $f_0 g_0 = \mathrm{id}$ and $g_0 f_0 = \mathrm{id}$. Universality implies that there exist unique $f^n\colon T^n \to S^n$ and $g^n\colon S^n \to T^n$ lifting f^0 and g^0. But, $f^n g^n$ and $g^n f^n$ lift $f^0 g^0$ and $g^0 f^0$, i.e., lift id. Yet, id lifts id in both cases. By uniqueness, $f^n g^n = \mathrm{id}$ and $g^n f^n = \mathrm{id}$. □

Theorem 5.10 *(Uniqueness I; Weak effaceability criterion) Say $\{T^n\}$ is a δ-functor on $\mathcal{A}$ and suppose for every $n > 0$ there is some functor, $E_n\colon \mathcal{A} \to \mathcal{A}$, which is exact and for which there is a monomorphism of functors* $\mathrm{id} \longrightarrow E_n$ *[i.e., for every object A in $\mathcal{O}\mathrm{b}(\mathcal{A})$ and all $n > 0$, we have an injection $A \longrightarrow E_n(A)$ functorially in A and E_n is exact] so that the map $T^n(A) \longrightarrow T^n(E_n(A))$ is the zero map for every $n > 0$. Then, $\{T^n\}$ is a universal δ-functor. Hence, $\{T^n\}$ is uniquely determined by T^0.*

Proof. Construct the liftings by induction on n. The case $n = 0$ is trivial since the map $f^0\colon T^0 \to S^0$ is given. Assume the lifting exists for all $r < n$. We have the exact sequence

$$0 \longrightarrow A \longrightarrow E_n(A) \longrightarrow \mathrm{cok}_A \longrightarrow 0$$

and so, we have a piece of the long exact diagram

$$\begin{array}{ccccccc} T^{n-1}(E_n(A)) & \longrightarrow & T^{n-1}(\mathrm{cok}_A) & \xrightarrow{\delta} & T^n(A) & \xrightarrow{0} & T^n(E_n(A)) \\ \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_{n-1}} & & & & \\ S^{n-1}(E_n(A)) & \longrightarrow & S^{n-1}(\mathrm{cok}_A) & \xrightarrow{\delta} & S^n(A) & & \end{array} \qquad (\dagger\dagger)$$

where the left square commutes and the rows are exact. Hence, by a simple argument, there is a unique $f_n\colon T^n(A) \to S^n(A)$ that makes the diagram commute. This construction is functorial since E_n is an exact functor; when we are done, all the diagrams commute.

Now, we need to prove uniqueness. Say we have two extensions $\{f_n\}$ and $\{g_n\}$ of f_0. We use induction to prove that $f_n = g_n$ for all n. This is obviously true for $n = 0$. Assume that uniqueness holds for all $r < n$. Write $(\dagger\dagger)$ again:

$$\begin{array}{ccccccc} T^{n-1}(E_n(A)) & \longrightarrow & T^{n-1}(\mathrm{cok}_A) & \longrightarrow & T^n(A) & \xrightarrow{0} & T^n(E_n(A)) \\ \downarrow{\scriptstyle f_{n-1}}\ \downarrow{\scriptstyle g_{n-1}} & & \downarrow{\scriptstyle f_{n-1}}\ \downarrow{\scriptstyle g_{n-1}} & & \downarrow{\scriptstyle f_n}\ \downarrow{\scriptstyle g_n} & & \\ S^{n-1}(E_n(A)) & \longrightarrow & S^{n-1}(\mathrm{cok}_A) & \longrightarrow & S^n(A) & & \end{array}.$$

As $f_{n-1} = g_{n-1}$ on all arguments, the above diagram implies $f_n = g_n$ on A. As A is arbitrary, $f_n = g_n$ and the proof is complete. □

Corollary 5.11 *Say $E_n = E$ for all n (E functorial and exact) and E satisfies the hypotheses of Theorem 5.10. (For example, this happens when $E(A)$ is $\{T^n\}$-acyclic for all A (i.e., $T^n(E(A)) = (0)$ for all A and all $n > 0$).) Then, $\{T^n\}$ is universal.*

We can apply Corollary 5.11 to the sequence $\{H^n(G, -)\}$, because $E(A) = \mathrm{Map}(G, A)$ satisfies all the hypotheses of that Corollary according to Proposition 4.54. Hence, we obtain the important

Corollary 5.12 *The sequence of functors $\{H^n(G, -)\}$ is a universal δ-functor from the category G-mod to $\mathcal{A}$b.*

Corollary 5.13 *If $E_n(A)$ is functorial and exact for every $n > 0$, and $E_n(Q)$ is T^n-acyclic for each n and for every injective Q, then every injective object of $\mathcal{A}$ is $\{T^n\}$-acyclic.*

Proof. Pick Q injective, then we have an exact sequence

$$0 \longrightarrow Q \longrightarrow E_n(Q) \longrightarrow \mathrm{cok}_Q \longrightarrow 0.$$

Since Q is injective, the sequence splits and so,

$$T^n(E_n(Q)) = T^n(Q) \amalg T^n(\mathrm{cok}_Q).$$

By assumption, the left hand side is zero; thus, $T^n(Q) = (0)$. □

Theorem 5.14 *(Uniqueness II) Say $\{T^n\}$ and $\{S^n\}$ are δ-functors on $\mathcal{A}$ and $\{f_n \colon T^n \to S^n\}$ is a map of δ-functors. If for all injectives, Q, the map $f_n(Q) \colon T^n(Q) \to S^n(Q)$ is an isomorphism (all n), then $\{f_n\}$ is an isomorphism of δ-functors. The same statement holds for ∂-functors and projectives.*

Proof. (Eilenberg) Of course, we use induction on n. First, we consider the case $n = 0$.

Step 1. I claim that $f_0 \colon T^0(A) \to S^0(A)$ is a monomorphism for all A.

Since $\mathcal{A}$ has enough injectives, we have an exact sequence

$$0 \longrightarrow A \longrightarrow Q \longrightarrow \mathrm{cok}_A \longrightarrow 0,$$

for some injective, Q. We have the commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & T^0(A) & \longrightarrow & T^0(Q) \\ & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \theta_{Q,0}} \\ 0 & \longrightarrow & S^0(A) & \longrightarrow & S^0(Q) \end{array}$$

where $\theta_{Q,0} \colon T^0(Q) \to S^0(Q)$ is an isomorphism, by hypothesis. It follows that f_0 is injective.

Step 2. The map f_0 is an isomorphism, for all A.

We have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & T^0(A) & \longrightarrow & T^0(Q) & \longrightarrow & T^0(\mathrm{cok}_A) \\ \| & & \| & & \downarrow & & \downarrow{\scriptstyle \theta_{Q,0}} & & \downarrow \\ 0 & \longrightarrow & 0 & \longrightarrow & S^0(A) & \longrightarrow & S^0(Q) & \longrightarrow & S^0(\mathrm{cok}_A), \end{array}$$

where the rightmost vertical arrow is injective by step 1 and $\theta_{Q,0}$ is an isomorphism. By the five lemma, the middle arrow is surjective, and thus bijective.

Next, consider the induction step.

Step 3. The map f_n is injective for all A.

Consider the commutative diagram

$$\begin{array}{ccccccccc} T^{n-1}(Q) & \longrightarrow & T^{n-1}(\mathrm{cok}_A) & \longrightarrow & T^n(A) & \longrightarrow & T^n(Q) & \longrightarrow & T^n(\mathrm{cok}_A) \\ \downarrow{\scriptstyle \theta_{Q,n-1}} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle \theta_{Q,n}} & & \downarrow \\ S^{n-1}(Q) & \longrightarrow & S^{n-1}(\mathrm{cok}_A) & \longrightarrow & S^n(A) & \longrightarrow & S^n(Q) & \longrightarrow & S^n(\mathrm{cok}_A). \end{array}$$

By the induction hypothesis, f_{n-1} is injective; moreover, $\theta_{Q,n-1}$ and $\theta_{Q,n}$ are bijective, by assumption, so the five lemma implies that $f_n \colon T^n(A) \to S^n(A)$ is injective.

Step 4. The map f_n is an isomorphism for all n.

By step 3, the righthand vertical arrow is an injection and by the induction hypothesis, f_{n-1} is an isomorphism. As $\theta_{Q,n}$ and $\theta_{Q,n-1}$ are isomorphisms, by the five lemma, again, f_n is surjective and thus bijective. □

Theorem 5.15 *(Uniqueness III) Given a δ-functor $\{T^n\}$ on $\mathcal{A}$, suppose that for any $A \in \mathcal{A}$, any injective Q and any exact sequence*

$$0 \longrightarrow A \longrightarrow Q \longrightarrow \operatorname{cok}_A \longrightarrow 0,$$

the sequence

$$T^{n-1}(Q) \longrightarrow T^{n-1}(\operatorname{cok}_A) \longrightarrow T^n(A) \longrightarrow 0 \quad \textit{is exact, if } n > 0.$$

Under these conditions, $\{T^n\}$ is a universal δ-functor. (Similarly for ∂-functors and projectives).

Proof. We proceed by induction. Given another δ-functor, $\{S^n\}$, and a morphism of functors $f_0 \colon T^0 \to S^0$, suppose f_0 is already extended to a morphism $f_r \colon T^r \to S^r$, for all $r \leq n-1$. Since $\mathcal{A}$ has enough injectives, we have the exact sequence

$$0 \longrightarrow A \longrightarrow Q \longrightarrow \operatorname{cok}_A \longrightarrow 0$$

and we get the diagram

$$\begin{array}{ccccccc} T^{n-1}(Q) & \longrightarrow & T^{n-1}(\operatorname{cok}_A) & \longrightarrow & T^n(A) & \longrightarrow & 0 \\ \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_{n-1}} & & \vdots{\scriptstyle \varphi_Q} & & \\ S^{n-1}(Q) & \longrightarrow & S^{n-1}(\operatorname{cok}_A) & \longrightarrow & S^n(A) & & \end{array} .$$

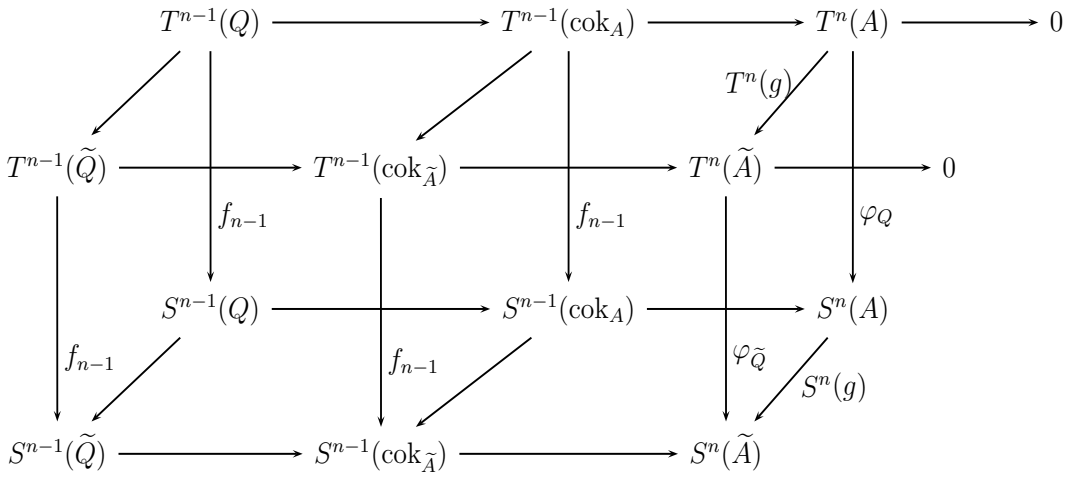
By a familiar argument, there exists only one map, φ_Q, making the diagram commute. Note that φ_Q might depend on Q. To handle dependence on Q and functoriality, take some $\widetilde{A}$ and its own exact sequence

$$0 \longrightarrow \widetilde{A} \longrightarrow \widetilde{Q} \longrightarrow \operatorname{cok}_{\widetilde{A}} \longrightarrow 0$$

and say we have a map $g \colon A \to \widetilde{A}$. Since $\widetilde{Q}$ is injective, there exist θ and $\overline{\theta}$ making the following diagram commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & Q & \longrightarrow & \operatorname{cok}_A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \overline{\theta}} & & \\ 0 & \longrightarrow & \widetilde{A} & \longrightarrow & \widetilde{Q} & \longrightarrow & \operatorname{cok}_{\widetilde{A}} & \longrightarrow & 0. \end{array}$$

We have the diagram:



All squares at top and bottom commute and the two left hand vertical squares also commute by the induction hypothesis. It follows that the righthand vertical square commutes (DX), i.e.:

$$\varphi_{\widetilde{Q}} \circ T^n(g) = S^n(g) \circ \varphi_Q.$$

If we set $g = \mathrm{id}$ (perhaps for different Q and $\widetilde{Q}$), we see that

$$\varphi_{\widetilde{Q}} = \varphi_Q,$$

so φ is independent of Q. Moreover, for any g, the righthand vertical diagram gives functoriality.

It remains to show commutativity with the connecting homomorphisms. Given an exact sequence

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$$

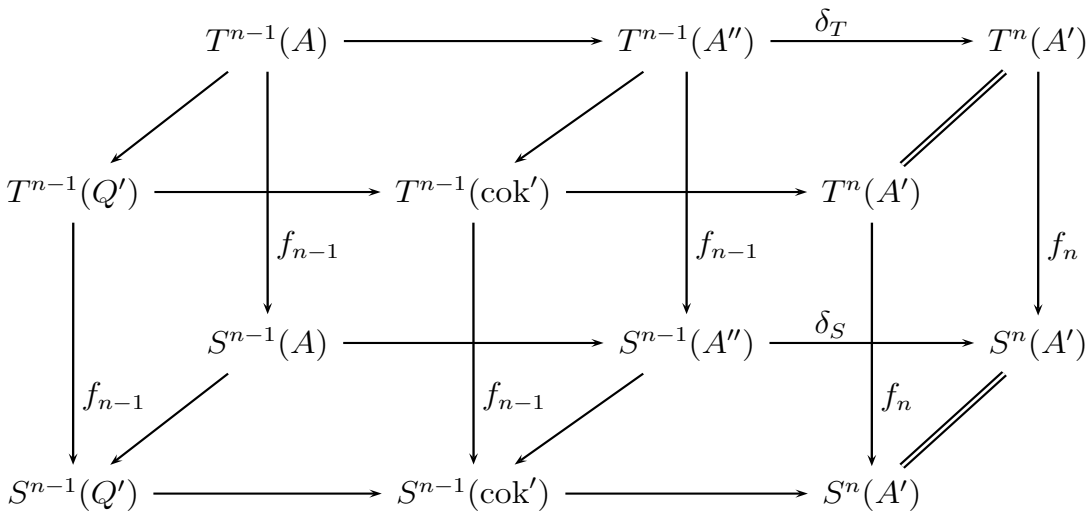
begin the resolution of A' by injectives, i.e., consider an exact sequence

$$0 \longrightarrow A' \longrightarrow Q' \longrightarrow \mathrm{cok}' \longrightarrow 0.$$

We obtain the diagram below in which θ and $\overline{\theta}$ exist making the diagram commute:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\overline{\theta}} & & \\
0 & \longrightarrow & A' & \longrightarrow & Q' & \longrightarrow & \mathrm{cok}' & \longrightarrow & 0.
\end{array}$$

Consequently, we get the diagram below in which all top and bottom diagrams commute and the left vertical cube commutes:



If we use the rightmost horizontal equalities, a diagram chase shows

$$\begin{array}{ccc} T^{n-1}(A'') & \xrightarrow{\delta_T} & T^n(A') \\ {\scriptstyle f_{n-1}}\downarrow & & \downarrow{\scriptstyle f_n} \\ S^{n-1}(A'') & \xrightarrow{\delta_S} & S^n(A') \end{array}$$

commutes (DX). □

Corollary 5.16 *The right derived (resp. left derived) functors of T are universal δ-functors (resp. universal ∂-functors). A necessary and sufficient condition that the δ-functor $\{T^n\}$ be isomorphic to the δ-functor $\{R^nT^0\}$ is that $\{T^n\}$ be universal. Similarly for ∂-functors and the sequence $\{L_nT_0\}$.*

Corollary 5.17 *For any group, G, the δ-functor $\{H^n(G,-)\}$ is isomorphic to the δ-functor $\{R^nH^0(G,-)\}$.*

5.3 Various (Co)homological Functors

There are many homological and cohomological functors all over mathematics. Here, we'll give a sample from various areas and some simple applications. By these samples, some idea of the ubiquity of (co)homological functors may be gleaned.

First of all, the functors $\mathrm{Ext}^\bullet_{\mathcal{A}}(A,B)$ and $\mathrm{Tor}^R_\bullet(A,B)$ have been defined in an asymmetric manner: We resolved A, not B. We'll investigate now what happens if we resolve B.

Pick any $B \in \mathcal{A}$ and write

$$T_B(-) = \mathrm{Hom}_{\mathcal{A}}(-,B).$$

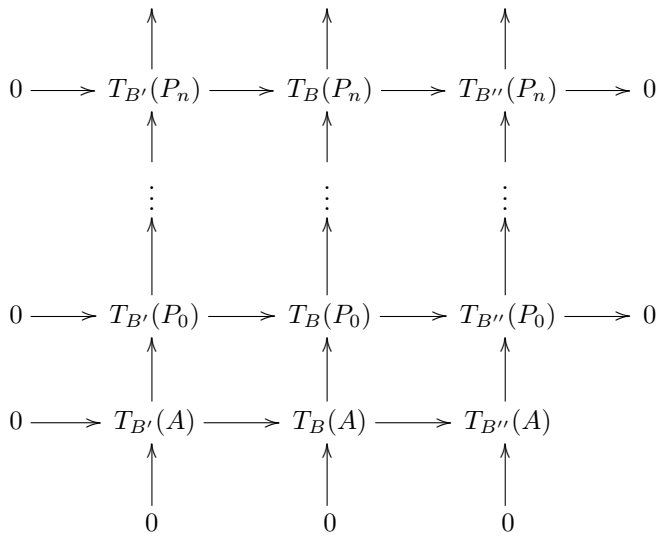
[Remember, $(R^nT_B)(A) = \mathrm{Ext}^n_{\mathcal{A}}(A,B)$.]

If $0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$ is exact and P is projective, we get the exact sequence

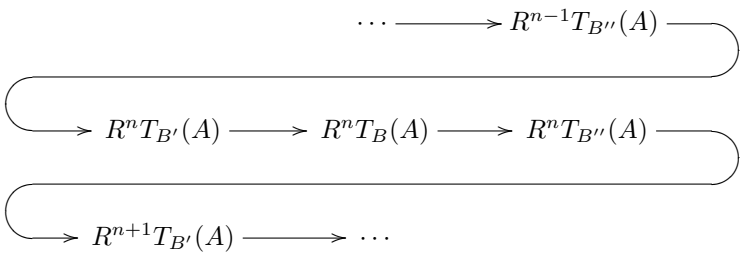
$$0 \longrightarrow T_{B'}(P) \longrightarrow T_B(P) \longrightarrow T_{B''}(P) \longrightarrow 0.$$

[Recall, P is projective iff $\mathrm{Hom}_{\mathcal{A}}(P,-)$ is exact.]

Resolve A: $P_\bullet \xrightarrow{\epsilon} A \longrightarrow 0$. We get the commutative diagram



Applying cohomology,[1] we get the long exact sequence of (co)homology:



[1] The locution "apply (co)homology" always means make the long exact sequence arising from the given short one.

Therefore, we have the exact sequence

$$\cdots \longrightarrow \mathrm{Ext}^{n-1}_{\mathcal{A}}(A, B'') \longrightarrow \mathrm{Ext}^{n}_{\mathcal{A}}(A, B') \longrightarrow \mathrm{Ext}^{n}_{\mathcal{A}}(A, B) \longrightarrow \mathrm{Ext}^{n}_{\mathcal{A}}(A, B'') \longrightarrow \mathrm{Ext}^{n+1}_{\mathcal{A}}(A, B') \longrightarrow \cdots$$

Consequently, we find that:

(1) $\mathrm{Ext}^{\bullet}_{\mathcal{A}}(A, B)$ is a functor of A and B, actually a co-functor of A and a functor of B.

(2) $\{\mathrm{Ext}^{\bullet}_{\mathcal{A}}(A, -)\}_{n=0}^{\infty}$ is a δ-functor (functorial in A).

(3) $\{\mathrm{Ext}^{\bullet}_{\mathcal{A}}(-, B)\}_{n=0}^{\infty}$ is a universal δ-functor (functorial in B).

Now, write $\widetilde{\mathrm{Ext}}^{\bullet}_{\mathcal{A}}(A, B)$ for what we get by resolving the righthand variable B (using injective resolutions). We obtain analogs of (1), (2), (3); call them $(\widetilde{1})$, $(\widetilde{2})$ and $(\widetilde{3})$. Note that

$$\widetilde{\mathrm{Ext}}^{0}_{\mathcal{A}}(A, B) = \mathrm{Hom}_{\mathcal{A}}(A, B) = \mathrm{Ext}^{0}_{\mathcal{A}}(A, B).$$

Now, $\widetilde{\mathrm{Ext}}^{\bullet}_{\mathcal{A}}(A, -)$ is a universal δ-functor and $\mathrm{Ext}^{\bullet}_{\mathcal{A}}(A, -)$ is a δ-functor. Thus, there is a unique extension

$$\widetilde{\mathrm{Ext}}^{n}_{\mathcal{A}}(A, B) \xrightarrow{\varphi_n} \mathrm{Ext}^{n}_{\mathcal{A}}(A, B),$$

which is a map of δ-functors. When B is injective, the left hand side is (0) (as derived functors vanish on injectives). Moreover, in this case, $\mathrm{Hom}_{\mathcal{A}}(-, B)$ is exact, and so,

$$R^n\mathrm{Hom}_{\mathcal{A}}(A, B) = (0), \quad \text{for all } n > 0 \text{ and all } A.$$

By Uniqueness II (Theorem 5.14), we conclude

Theorem 5.18 *The derived functor* $\mathrm{Ext}^{\bullet}_{\mathcal{A}}$ *can be computed by resolving either variable. The same result holds for* $\mathrm{Tor}^{R}_{\bullet}$ *(in* $\mathcal{M}\mathrm{od}(R)$*).*

There is a technique by which the value of $R^nT(A)$ can be computed from $R^{n-1}T(\widetilde{A})$ for a suitable $\widetilde{A}$. This is known as *décalage*[2] or *dimension shifting*. Here is how it goes for a left exact functor, T, or left exact cofunctor, S.

For T, consider A and embed it in an acyclic object for R^nT, e.g., an injective

$$0 \longrightarrow A \longrightarrow Q \longrightarrow \mathrm{cok}_A \longrightarrow 0.$$

Now apply cohomology:

$$0 \longrightarrow T(A) \longrightarrow T(Q) \longrightarrow T(\mathrm{cok}_A) \longrightarrow R^1T(A) \longrightarrow 0 \longrightarrow R^1T(\mathrm{cok}_A) \longrightarrow R^2T(A) \longrightarrow 0 \longrightarrow R^2T(\mathrm{cok}_A) \longrightarrow \cdots \longrightarrow 0 \longrightarrow R^{n-1}T(\mathrm{cok}_A) \longrightarrow R^nT(A) \longrightarrow 0 \longrightarrow \cdots$$

[2]The French word means a shift in space and is also used for time.

We find that

$$\begin{aligned} R^{n-1}T(\mathrm{cok}_A) &\xrightarrow{\sim} R^nT(A), \quad n \geq 2 \\ \mathrm{cok}(T(Q) \longrightarrow T(\mathrm{cok}_A)) &\xrightarrow{\sim} R^1T(A), \end{aligned}$$

so the suitable $\widetilde{A}$ is just cok_A.

For the cofunctor, S, project an acyclic object (for R^nS), e.g., a projective, onto A:

$$0 \longrightarrow \mathrm{Ker}_A \longrightarrow P \longrightarrow A \longrightarrow 0.$$

Just as above, we find

$$\begin{aligned} R^{n-1}S(\mathrm{Ker}_A) &\xrightarrow{\sim} R^nS(A) \\ \mathrm{cok}(S(P) \longrightarrow S(\mathrm{Ker}_A)) &\xrightarrow{\sim} R^1S(A). \end{aligned}$$

Similar statements hold for right exact functors or cofunctors and their left derived functors.

There is a very important interpretation of $\mathrm{Ext}^1_{\mathcal{A}}(A, B)$; indeed this interpretation is the origin of the word "Ext" for the derived functor of Hom. To keep notation similar to that used earlier for modules in Chapter 2, we'll replace A by M'' and B by M' and consider $\mathrm{Ext}^1_{\mathcal{A}}(M'', M')$.

Say

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \tag{E}$$

is an extension of M'' by M'. Equivalence is defined as usual: In the diagram below, the middle arrow, g, is an isomorphism that makes the diagram commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle g} & & \| & & \\ 0 & \longrightarrow & M' & \longrightarrow & \widetilde{M} & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

Apply to (E) the functor $\mathrm{Hom}_{\mathcal{A}}(M'', -)$. We get

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}}(M'', M') \longrightarrow \mathrm{Hom}_{\mathcal{A}}(M'', M) \longrightarrow \mathrm{Hom}_{\mathcal{A}}(M'', M'') \xrightarrow{\delta_{(E)}} \mathrm{Ext}^1_{\mathcal{A}}(M'', M').$$

So, $\delta_{(E)}(\mathrm{id})$ is a canonical element in $\mathrm{Ext}^1_{\mathcal{A}}(M'', M')$; it is called the *characteristic class of the extension* (E), denoted $\chi(E)$. Note: $\chi(E) = 0$ iff (E) splits.

Now, given $\xi \in \mathrm{Ext}^1_{\mathcal{A}}(M'', M')$, resolve M' by injectives:

$$0 \longrightarrow M' \longrightarrow Q^0 \longrightarrow Q^1 \longrightarrow Q^2 \longrightarrow \cdots.$$

If we apply $\mathrm{Hom}_{\mathcal{A}}(M'', -)$, we get

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{A}}(M'', M') \longrightarrow \mathrm{Hom}_{\mathcal{A}}(M'', Q^0) \xrightarrow{d_0} \mathrm{Hom}_{\mathcal{A}}(M'', Q^1) \xrightarrow{d_1} \mathrm{Hom}_{\mathcal{A}}(M'', Q^2) \longrightarrow \cdots,$$

and we have $\mathrm{Ext}^1(M'', M') = \mathrm{Ker}\ d_1/\mathrm{Im}\ d_0$. Consequently, ξ comes from some $f \in \mathrm{Hom}_{\mathcal{A}}(M'', Q^1)$ and $d_1(f) = 0$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & Q^0 & \xrightarrow{d_0} & Q^1 & \xrightarrow{d_1} & Q^2 \\ & & & & & & \uparrow{\scriptstyle f} & \nearrow_{d_1(f)=0} & \\ & & & & & & M'' & & \end{array}$$

Thus,

$$\text{Im } f \subseteq \text{Ker } d_1 = \text{Im } d_0 = X,$$

and so, f is a map $M'' \longrightarrow X \subseteq Q^1$. We get

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & Q^0 & \xrightarrow{d_0} & X & \longrightarrow & 0 \\ & & & & & & \uparrow{\scriptstyle f} & & \\ & & & & & & M'' & & \end{array} \qquad (*)$$

Taking the pullback of $(*)$ by f, we find

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & M' & \longrightarrow & Q^0 & \longrightarrow & X & \longrightarrow & 0, \end{array} \qquad (E)$$

i.e., we get an extension, (E). One checks that (E) is independent of f, but depends only on ξ. This involves two steps (DX): (E) does not change if f is replaced by $f + d_0(h)$; (E) does not change if we use another injective resolution. Hence, we've proved

Theorem 5.19 *There is a one-to-one correspondence*

$$(E) \mapsto \chi(E)$$

between equivalence classes of extensions of modules of M'' by M' and elements of $\text{Ext}^1_{\mathcal{A}}(M'', M')$.

An interpretation of $\text{Ext}^n_{\mathcal{A}}(M'', M')$ for $n \geq 2$ will be left for the exercises. The cohomological functor $\text{Ext}^\bullet_{\mathcal{A}}(A, B)$ is the most important of the various cohomological functors because many cohomological functors are special cases of it. The same holds for $\text{Tor}^R_\bullet(A, B)$ with respect to homological functors. Here are several examples of these considerations:

We begin with groups. Recall that we proved the δ-functor $\{H^n(G, A)\}$ coincided with the right-derived functors of the functor $A \rightsquigarrow A^G$. (Of course, here G is a group and A is a G-module.) We form the group ring $R = \mathbb{Z}[G]$[3]; every G-module is an R-module and conversely—in particular, every abelian group is an R-module with trivial action by G. Consider $\mathbb{Z}$ as R-module with trivial G-action and for any G-module introduce the functor

$$A \rightsquigarrow \text{Hom}_R(\mathbb{Z}, A).$$

It is left exact and its derived functors are $\text{Ext}^\bullet_R(\mathbb{Z}, A)$. But, a homomorphism $f \in \text{Hom}_R(\mathbb{Z}, A)$ is just an element of A, namely $f(1)$. And, as $\mathbb{Z}$ has trivial G-action, our element, $f(1)$, is fixed by G. Therefore

$$\text{Hom}_R(\mathbb{Z}, A) \xrightarrow{\sim} A^G,$$

and so we find

Proposition 5.20 *If G is any group and A is any G-module, there is a canonical isomorphism*

$$\text{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A) \xrightarrow{\sim} H^n(G, A), \quad \textit{all} \quad n \geq 0.$$

[3]Recall that $\mathbb{Z}[G]$ is the free $\mathbb{Z}$-module on the elements of G. Multiplication is defined by $\sigma \otimes \tau \mapsto \sigma\tau$, where $\sigma, \tau \in G$ and we extend by linearity.

As for group homology, first consider the exact sequence of G-modules

$$0 \longrightarrow I \longrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0, \qquad (*)$$

in which ϵ takes the element $\sum a_\sigma \cdot \sigma$ to $\sum a_\sigma$; that is, ϵ sends each group element to 1. The ideal I is by definition Ker ϵ; one sees easily that I is freely generated by the elements $\sigma - 1$ (for $\sigma \in G$, $\sigma \neq 1$) as a $\mathbb{Z}$-module. A little less obvious is the following:

Proposition 5.21 *The mapping* $\log(\sigma) = (\sigma - 1) (\mathrm{mod}\, I^2)$ *is an isomorphism of abelian groups*

$$\log\colon G/[G,G] \xrightarrow{\sim} I/I^2.$$

Proof. The operations on the two sides of the claimed isomorphism, log, are the group multiplication abelianized and addition respectively. Clearly, $\log(\sigma) = (\sigma - 1) (\mathrm{mod}\, I^2)$ is well-defined and

$$(\sigma\tau - 1) = (\sigma - 1) + (\tau - 1) + (\sigma - 1)(\tau - 1)$$

shows it's a homomorphism. Of course we then have $\log(\sigma^{-1}) = -(\sigma - 1)$, but this is easy to see directly. It follows immediately that $[G, G]$ lies in the kernel of log; so we do get a map

$$\log\colon G/[G,G] \longrightarrow I/I^2.$$

As I is the free $\mathbb{Z}$-module on the elements $(\sigma - 1)$, as σ ranges over G ($\sigma \neq 1$), we can define

$$\exp\colon I \longrightarrow G/[G,G],$$

via

$$\exp\left(\sum_{\sigma\neq 1} n_\sigma(\sigma - 1)\right) = \prod_{\sigma\neq 1} \sigma^{n_\sigma} \bmod [G,G]$$

and considerations entirely simililar to those above for log show that exp is a homomorphism from I to $G/[G,G]$ and that I^2 is killed by exp. It should be obvious that log and exp are mutually inverse, so we're done. □

If A is a G-module, we can tensor exact sequence $(*)$ over $\mathbb{Z}[G]$ with A; this gives

$$I \otimes_{\mathbb{Z}[G]} A \longrightarrow A \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \longrightarrow 0.$$

Of course, this shows

$$A/(IA) \xrightarrow{\sim} \mathbb{Z} \otimes_{\mathbb{Z}[G]} A.$$

The functor $A \rightsquigarrow A/IA$ is a right-exact functor from G-modules to $\mathcal{A}$b and its left derived functors, $H_n(G, A)$, are the *homology groups of G with coefficients in A*. The isomorphism we've just observed (together with the usual arguments on universal ∂-functors) allows us to conclude

Proposition 5.22 *If G is a group and A is any G-module, there is a canonical isomorphism (of ∂-functors)*

$$H_n(G, A) \xrightarrow{\sim} \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A), \quad \textit{all} \quad n \geq 0.$$

We first introduced and computed group cohomology *via* an explicit chain complex, is there a similar description for group homology? There is indeed, and while we can be quite direct and give it, perhaps it is better to make a slight detour which is necessary anyway if one is to define (co)homology of algebras in a direct manner.

Write K for a commutative ring and R for a (possibly non-commutative) K-algebra. In the case of groups, K will be $\mathbb{Z}$ and R will be $\mathbb{Z}[G]$, while for other purposes K will be a field and R the polynomial ring $K[T_1, \ldots, T_n]$; there will be still other purposes.

For an integer, $n \geq -1$, write $C_n(R)$ for the $(n+2)$-fold tensor product of R with itself over K:

$$\begin{aligned} C_n(R) &= \underbrace{R \otimes_K R \otimes_K \cdots \otimes_K R}_{n+2} \\ C_{-1}(R) &= R \\ C_{n+1}(R) &= R \otimes_K C_n(R). \end{aligned}$$

Next, introduce the module $R \otimes_K R^{\mathrm{op}}$. We want to make $R \otimes_K R^{\mathrm{op}}$ into a K-algebra by the multiplication

$$(\rho \otimes \sigma^{\mathrm{op}})(r \otimes s^{\mathrm{op}}) = \rho r \otimes \sigma^{\mathrm{op}} s^{\mathrm{op}} = \rho r \otimes (s\sigma)^{\mathrm{op}}$$

and *for this we must have K in the center of R.* To see this, pick $\lambda \in K$, set $\rho = s = 1$, set $\sigma = \lambda$, and compute

$$\begin{aligned} r\lambda \otimes_K 1^{\mathrm{op}} &= (r \otimes_K \lambda^{\mathrm{op}} 1^{\mathrm{op}}) = r \otimes_K \lambda^{\mathrm{op}} \\ &= (1 \otimes_K \lambda^{\mathrm{op}})(r \otimes_K 1^{\mathrm{op}}) \\ &= (\lambda \otimes_K 1^{\mathrm{op}})(r \otimes_K 1^{\mathrm{op}}) = \lambda r \otimes_K 1^{\mathrm{op}}. \end{aligned}$$

As r is arbitrary, we are done. So, **from now on, we shall assume K is in the center of R.** The algebra $R \otimes_K R^{\mathrm{op}}$ is called the *enveloping algebra of R over K*; it is usually denoted R^e. Now, there is a map $R^e \longrightarrow R$ *via*

$$r \otimes s^{\mathrm{op}} \mapsto rs.$$

This map is **not** a map of K-algebras, only a map of R^e-modules. (R^e acts on R *via* $(r \otimes s^{\mathrm{op}})(m) = rms$; in general, two-sided R-modules are just R^e-modules (as well as $(R^e)^{\mathrm{op}}$-modules).) It will be a K-algebra map if R is commutative.

We should also note that the map

$$r \otimes s^{\mathrm{op}} \mapsto s^{\mathrm{op}} \otimes r$$

is a K-isomorphism of K-algebras $R^e \xrightarrow{\sim} (R^e)^{\mathrm{op}}$. (DX)

It will be best to use "homogeneous notation" for elements of $C_n(R)$: $r_0 \otimes r_1 \otimes \cdots \otimes r_{n+1}$. Then $C_n(R)$ is a left R^e-module under the rule

$$(s \otimes t^{\mathrm{op}})(r_0 \otimes r_1 \otimes \cdots \otimes r_n \otimes r_{n+1}) = (sr_0) \otimes r_1 \otimes \cdots \otimes r_n \otimes (r_{n+1}t).$$

Now we'll make $\{C_n(R)\}_{n=0}^{\infty}$ into an acyclic left complex. The boundary map is

$$\partial_n(r_0 \otimes r_1 \otimes \cdots \otimes r_{n+1}) = \sum_{i=0}^{n} (-1)^i \, r_0 \otimes \cdots \otimes (r_i r_{i+1}) \otimes \cdots \otimes r_{n+1},$$

it is an R^e-homomorphism $C_n(R) \longrightarrow C_{n-1}(R)$. In particular, ∂_0 is the R^e-module map discussed above,

$$\partial_0(r_0 \otimes r_1) = r_0 r_1$$

and

$$\partial_1(r_0 \otimes r_1 \otimes r_2) = (r_0 r_1) \otimes r_2 - r_0 \otimes (r_1 r_2).$$

From these, we see $\partial_0\partial_1 = 0$ precisely because R is associative. To prove $\{C_n(R)\}$ is a complex and acyclic, introduce the map

$$\sigma_n \colon C_n(R) \longrightarrow C_{n+1}(R) \quad \textit{via} \quad \sigma_n(\xi) = 1 \otimes_K \xi.$$

The map σ_n is only an R^{op}-module map but it is injective because there is a map $\tau_n \colon C_{n+1}(R) \to C_n(R)$ given by $\tau_n(r_0 \otimes (\text{rest})) = r_0(\text{rest})$ and we have $\tau_n\sigma_n = \mathrm{id}$. Moreover, $\mathrm{Im}\,(\sigma_n)$ generates $C_{n+1}(R)$ as R-module! It is easy to check the relation

$$\partial_{n+1}\sigma_n + \sigma_{n-1}\partial_n = \mathrm{id} \quad \text{on} \quad C_n(R), \quad \text{for} \quad n \geq 0. \tag{$\dagger$}$$

Now use induction to show $\partial_{n-1}\partial_n = 0$ as follows: Above we showed it for $n = 1$, assume it up to n and apply ∂_n (on the left) to ($\dagger$), we get

$$\partial_n\partial_{n+1}\sigma_n + \partial_n\sigma_{n-1}\partial_n = \partial_n.$$

However, $\partial_n\sigma_{n-1} = \mathrm{id}_{n-1} - \sigma_{n-2}\partial_{n-1}$, by ($\dagger$) at $n-1$. So,

$$\partial_n\partial_{n+1}\sigma_n + \partial_n - \sigma_{n-2}\partial_{n-1}\partial_n = \partial_n,$$

that is, $\partial_n\partial_{n+1}\sigma_n = 0$ (because $\partial_{n-1}\partial_n = 0$). But, the image of σ_n generates C_{n+1} as R-module; so $\partial_n\partial_{n+1} = 0$, as needed. Now, notice that ∂_0 takes $C_0(R) = R^e$ onto $C_{-1}(R) = R$, and so

$$\cdots \longrightarrow C_n(R) \xrightarrow{\partial_n} C_{n-1}(R) \longrightarrow \cdots \longrightarrow C_0(R) \xrightarrow{\partial_0} R \longrightarrow 0$$

is an acyclic resolution of R as R^e-module.

Since $C_n(R) = R \otimes_K (\underbrace{R \otimes_K \cdots \otimes_K R}_{n}) \otimes_K R$, we find

$$C_n(R) = R^e \otimes_K C_n[R],$$

where

$$C_n[R] = R \otimes_K \cdots \otimes_K R, \quad n\text{-times}$$

and

$$C_0[R] = K.$$

Several things follow from this description of $C_n(R)$: First, we see exactly how $C_n(R)$ is an R^e-module and also see that it is simply the base extension of $C_n[R]$ from K to R^e. Next, we want a projective resolution, so we want to insure that $C_n(R)$ is indeed projective even over R^e. For this we prove

Proposition 5.23 *Suppose R is a K-algebra and R is projective as a K-module (in particular this holds if R is K-free, for example when K is a field). Then*

(1) $C_n[R]$ is K-projective for $n \geq 0$,

(2) $R \otimes_K C_n[R]$ is R-projective for $n \geq 0$,

(3) $C_n(R)$ is R^e-projective for $n \geq 0$.

Proof. This is a simple application of the ideas in Chapter 2, Section 2.6. Observe that (2) and (3) follow from (1) because we have

$$\mathrm{Hom}_R(R \otimes_K C_n[R], T) \xrightarrow{\sim} \mathrm{Hom}_K(C_n[R], T) \tag{$\dagger$}$$

and

$$\mathrm{Hom}_{R^e}(R^e \otimes_K C_n[R], T) \xrightarrow{\sim} \mathrm{Hom}_K(C_n[R], T) \tag{$\dagger\dagger$}$$

where T is an R-module in (†) and an R^e-module in (††). An exact sequence of R-modules (resp. R^e-modules) is exact as sequence of K-modules and (1) shows that the right sides of (†) and (††) are exact as functors of T. Such exactness characterizes projectivity; so, (2) and (3) do indeed follow from (1).

To prove (1), use induction on n and Proposition 2.47 which states in this case

$$\mathrm{Hom}_K(R \otimes_K C_{n-1}[R], T) \xrightarrow{\sim} \mathrm{Hom}_K(C_{n-1}[R], \mathrm{Hom}_K(R, T)). \qquad (*)$$

Now, $T \rightsquigarrow \mathrm{Hom}_K(R, T)$ is exact by hypothesis; so, the right hand side of $(*)$ is an exact functor of T by induction hypothesis. Consequently, $(*)$ completes the proof. □

Corollary 5.24 *If the K-algebra, R, is K-projective, then*

$$\cdots \longrightarrow C_n(R) \xrightarrow{\partial_n} C_{n-1}(R) \longrightarrow \cdots \longrightarrow C_0(R) \xrightarrow{\partial_0} R \longrightarrow 0$$

is an R^e-projective resolution of the R^e-module R.

The resolution of Corollary 5.24 is called the *standard* (or *bar*) *resolution of R*. We can define the homology and cohomology groups of the K-algebra R with coefficients in the *two-sided R-module*, M, as follows:

Define the functors

$$H_0(R, -)\colon M \rightsquigarrow M/M\mathfrak{J}$$

and

$$H^0(R, -)\colon M \rightsquigarrow \{m \in M \mid rm = mr, \quad \text{all } r \in R\} = M^R$$

to the category of K-modules. Here, the (left) ideal, $\mathfrak{J}$, of R^e is defined by the exact sequence

$$0 \longrightarrow \mathfrak{J} \longrightarrow R^e \xrightarrow{\partial_0} R \longrightarrow 0, \qquad (**)$$

and is called the *augmentation ideal of R^e*. It's easy to check that $M \rightsquigarrow M/M\mathfrak{J}$ is right exact and $M \rightsquigarrow M^R$ is left exact. We make the definition

Definition 5.7 *The n-th homology group of R with coefficients in the two-sided R-module, M*, is

$$H_n(R, M) = (L^n H_0)(M)$$

and *the nth cohomology group with coefficients in M* is

$$H^n(R, M) = (R^n H^0)(M).$$

We'll refer to these groups as the *Hochschild homology* and *cohomology groups of R* even though our definition is more general than Hochschild's–he assumed K is a field and gave an explicit (co)cycle description. We'll recover this below and for this purpose notice that

The augmententation ideal, $\mathfrak{J}$, is generated (as left R^e-ideal) by the elements $r \otimes 1 - 1 \otimes r^{\mathrm{op}}$ for $r \in R$.

To see this, observe that $\sum_i r_i \otimes s_i^{\mathrm{op}} \in \mathfrak{J}$ iff we have $\sum_i r_i s_i = 0$. But then

$$\sum_i r_i \otimes s_i^{\mathrm{op}} = \sum_i r_i \otimes s_i^{\mathrm{op}} - \sum_i r_i s_i \otimes 1 = \sum_i (r_i \otimes 1)(1 \otimes s_i^{\mathrm{op}} - s_i \otimes 1).$$

Now, to apply this, tensor our exact sequence $(**)$ with M:

$$M \otimes_{R^e} \mathfrak{J} \longrightarrow M \xrightarrow{1 \otimes \partial_0} M \otimes_{R^e} R \longrightarrow 0,$$

so we find

$$H_0(R,M) = M/M\mathfrak{J} \xrightarrow{\sim} M \otimes_{R^e} R.$$

It follows immediately that we have an isomorphism

$$H_n(R,M) \xrightarrow{\sim} \operatorname{Tor}_n^{R^e}(M,R).$$

Similarly, we take $\operatorname{Hom}_{R^e}(-,M)$ of $(**)$ and get

$$0 \longrightarrow \operatorname{Hom}_{R^e}(R,M) \longrightarrow M \xrightarrow{\theta} \operatorname{Hom}_{R^e}(\mathfrak{J},M).$$

The isomorphism

$$\operatorname{Hom}_{R^e}(R^e,M) \xrightarrow{\sim} M$$

is just

$$f \mapsto f(1),$$

thus if $f \in \operatorname{Hom}_{R^e}(R^e,M)$ and $m = f(1)$, we find for $\xi \in \mathfrak{J}$ that

$$(\theta(f))(\xi) = f(\xi) = \xi m.$$

Therefore, f is in $\operatorname{Ker}\theta$ iff $\xi m = 0$ for all $\xi \in \mathfrak{J}$, where $m = f(1)$. But, by the above, such ξ are generated by $r \otimes 1 - 1 \otimes r^{\mathrm{op}}$, and so $m \in \operatorname{Ker}\theta$ when and only when $(r \otimes 1)m = (1 \otimes r^{\mathrm{op}})m$; i.e., exactly when $rm = mr$, for all $r \in R$. We have proved that there is an isomorphism (of K-modules)

$$\operatorname{Hom}_{R^e}(R,M) \xrightarrow{\sim} M^R = H^0(R,M).$$

Once again we obtain an isomorphism

$$\operatorname{Ext}_{R^e}^n(R,M) \xrightarrow{\sim} H^n(R,M).$$

Our discussion above proves the first two statements of

Theorem 5.25 *If R is a K-algebra (with K contained in the center of R), then for any two-sided R-module, M, we have canonical, functorial isomorphisms*

$$H_n(R,M) \xrightarrow{\sim} \operatorname{Tor}_n^{R^e}(M,R)$$

and

$$H^n(R,M) \xrightarrow{\sim} \operatorname{Ext}_{R^e}^n(R,M).$$

If R is K-projective, then homology can be computed from the complex

$$M \otimes_K C_n[R]$$

with boundary operator

$$\partial_n(m \otimes r_1 \otimes \cdots \otimes r_n) = mr_1 \otimes r_2 \otimes \cdots \otimes r_n + \sum_{i=1}^{n-1}(-1)^i m \otimes r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n + (-1)^n r_n m \otimes r_1 \otimes \cdots \otimes r_{n-1};$$

while cohomology can be computed from the complex

$$\operatorname{Hom}_K(C_n[R],M)$$

with coboundary operator

$$(\delta_n f)(r_1 \otimes \cdots \otimes r_n \otimes r_{n+1}) = r_1 f(r_2 \otimes \cdots \otimes r_{n+1}) + \sum_{i=1}^{n}(-1)^i f(r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_{n+1}) (-1)^{n+1} f(r_1 \otimes \cdots \otimes r_n) r_{n+1}.$$

Proof. Only the statements about the explicit complex require proof. Since homology and cohomology are given by specific Tor's and Ext's, and since the standard resolution *is* an R^e-projective resolution of R, we can use the latter to compute these Tor's and Ext's. Here, it will be important to know the R^e-module structure of $C_n(R)$ and the fact that the map

$$r \otimes s^{\mathrm{op}} \mapsto s^{\mathrm{op}} \otimes r$$

establishes a K-algebra isomorphism of R^e and $(R^e)^{\mathrm{op}}$.

Now, consider the map

$$\Theta\colon M \otimes_{R^e} C_n(R) = M \otimes_{R^e} (R^e \otimes_K C_n[R]) \xrightarrow{\sim} M \otimes_K C_n[R].$$

Observe that M is treated as an $(R^e)^{\mathrm{op}}$-module, the action being

$$m(r \otimes s^{\mathrm{op}}) = smr.$$

Thus,

$$\begin{aligned}
\Theta\colon m \otimes_{R^e} (r_0 \otimes \cdots \otimes r_{n+1}) &= m \otimes_{R^e} (r_0 \otimes r_{n+1}^{\mathrm{op}}) \otimes_K (r_1 \otimes \cdots \otimes r_n) \\
&\mapsto [m \cdot (r_0 \otimes r_{n+1}^{\mathrm{op}})] \otimes_K (r_1 \otimes \cdots \otimes r_n) \\
&= (r_{n+1} m r_0) \otimes_K (r_1 \otimes \cdots \otimes r_n) \in M \otimes_K C_n[R].
\end{aligned}$$

We now just have to see the explicit form of the boundary map induced on $M \otimes_K C_n[R]$ by the diagram

$$\begin{array}{ccc}
M \otimes_{R^e} C_n(R) & \xleftarrow{\Theta^{-1}} & M \otimes_K C_n[R] \\
\Big\downarrow{\scriptstyle 1\otimes\partial_n} & & \\
M \otimes_{R^e} C_{n-1}(R) & \xrightarrow{\Theta} & M \otimes_K C_{n-1}[R]
\end{array}$$

This goes as follows:

$$\begin{aligned}
m \otimes_K (r_1 \otimes \cdots \otimes r_n) &\xrightarrow{\Theta^{-1}} m \otimes_{R^e} (1 \otimes 1) \otimes_K (r_1 \otimes \cdots \otimes r_n) \\
&= m \otimes_{R^e} 1 \otimes r_1 \otimes \cdots \otimes r_n \otimes 1 \\
&\xrightarrow{1\otimes\partial_n} m \otimes_{R^e} r_1 \otimes \cdots \otimes r_n \otimes 1 \\
&\quad + \sum_{i=1}^{n-1} (-1)^i m \otimes_{R^e} (1 \otimes r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n \otimes 1) \\
&\quad + (-1)^n m \otimes_{R^e} (1 \otimes r_1 \otimes \cdots \otimes r_n) \\
&\xrightarrow{\Theta} mr_1 \otimes r_2 \otimes \cdots \otimes r_n + \sum_{i=1}^{n-1} (-1)^i m \otimes r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n \\
&\quad + (-1)^n r_n m \otimes r_1 \otimes \cdots \otimes r_{n-1},
\end{aligned}$$

exactly the formula of the theorem. For cohomology we proceed precisely the same way, but remember that here M is treated as an R^e-module. Details are left as a (DX). □

When K is a field, the explicit (co)chain descriptions of $H_n(R, M)$ and $H^n(R, M)$ apply; these are Hochschild's original descriptions for the (co)homology of K-algebras, Hochschild [25, 26].

By now, it should be clear that there is more than an analogy between the (co)homology of algebras and that for groups. This is particularly evident from comparison of the original formula (Chapter 1, Section 1.4) for cohomology of groups and Hochschild's formula for the cohomology of the K-algebra, R. If we use just

analogy then R will be replaced by $\mathbb{Z}[G]$ and K by $\mathbb{Z}$; R is then free (rank $= \#(G)$) over K. But, M is just a left G-module (for cohomology) and for K-algebras, R, we assumed M was a two-sided R-module. This is easily fixed: *Make $\mathbb{Z}[G]$ act trivially on the right*. Then, $H^0(\mathbb{Z}[G], M)$ is our old M^G and the coboundary formula becomes (it is necessary only to compute on $\sigma_1 \otimes \cdots \otimes \sigma_{n+1}$ as such tensors generate):

$$\begin{aligned}(\delta_n f)(\sigma_1 \otimes \cdots \otimes \sigma_{n+1}) = {} & \sigma_1 f(\sigma_2 \otimes \cdots \otimes \sigma_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(\sigma_1 \otimes \cdots \otimes \sigma_i\sigma_{i+1} \otimes \cdots \otimes \sigma_{n+1}) \\ & + (-1)^{n+1} f(\sigma_1 \otimes \cdots \otimes \sigma_n),\end{aligned}$$

as in Chapter 1. Therefore, keeping the analogy, for homology, where we have a right G-module, we should make $\mathbb{Z}[G]$ *act trivially on the left*, and get the explicit formula:

$$\begin{aligned}\partial_n(m \otimes \sigma_1 \otimes \cdots \otimes \sigma_n) = {} & m\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \\ & + \sum_{i=1}^{n-1} (-1)^i m \otimes \sigma_1 \otimes \cdots \otimes \sigma_i\sigma_{i+1} \otimes \cdots \otimes \sigma_n \qquad (*) \\ & + (-1)^n m \otimes \sigma_1 \otimes \cdots \otimes \sigma_{n-1},\end{aligned}$$

which formula we had in mind at the beginning of this discussion several pages ago.

The ideal $\mathfrak{J}$ is generated by $\sigma \otimes 1 - 1 \otimes \sigma^{\mathrm{op}}$ as σ ranges over G ($\sigma \neq 1$). Thus $M\mathfrak{J}$ is the submodule generated by $\{m - m\sigma \mid \sigma \neq 1\}$. Now the formula

$$\sigma^{-1}m = m\sigma \qquad \text{(special for groups)}$$

turns M into a left $\mathbb{Z}[G]$-module and shows that $M\mathfrak{J}$ is exactly our old IM and therefore proves the Hochschild $H_0(\mathbb{Z}[G], M)$ is our old $H_0(G, M)$.

However, all this is heuristic, it does not prove the Hochschild groups for $\mathbb{Z}[G]$ on our *one-sided* modules are the (co)homology groups for G. For one thing, we are operating on a subcategory: The modules with trivial action on one of their sides. For another, the Hochschild groups are $\mathrm{Tor}_\bullet^{\mathbb{Z}[G]^e}(-, \mathbb{Z}[G])$ and $\mathrm{Ext}^\bullet_{\mathbb{Z}[G]^e}(\mathbb{Z}[G], -)$ not $\mathrm{Tor}_\bullet^{\mathbb{Z}[G]}(-, \mathbb{Z})$ and $\mathrm{Ext}^\bullet_{\mathbb{Z}[G]}(\mathbb{Z}, -)$. We do know that everything is correct for cohomology because of a previous argument made about universal δ-functors. Of course, it is perfectly possible to prove that the groups

$$\widetilde{H}_n(G, M) = \mathrm{Ker}\ \partial_n / \mathrm{Im}\ \partial_{n+1}$$

for ∂_n given by $(*)$ above form a universal ∂-functor—they clearly form a ∂-functor and universality will follow from the effaceability criterion (Theorem 5.10). The effaceing module will be $M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ in analogy with $\mathrm{Map}(G, M)$ (which is $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)$). Here, details are best left as an exercise.

Instead, there is a more systematic method that furthermore illustrates a basic principle handy in many situations. We begin again with our K-algebra, R, and we *assume there is a K-algebra homomorphism* $\epsilon\colon R \to K$. Note that this is the same as saying all of (DX)

(i) K is an R-module (and R contains K in its center),

(ii) There is an R-module map $R \xrightarrow{\epsilon} K$,

(iii) The composition $K \longrightarrow R \xrightarrow{\epsilon} K$ is the identity.

Examples to keep in mind are: $K = \mathbb{Z}$, $R = \mathbb{Z}[G]$ and $\epsilon(\sigma) = 1$, all $\sigma \in G$; K arbitrary (commutative), $R = K[T_1, \ldots, T_n]$ or $K\langle T_1, \ldots, T_n\rangle$ and $\epsilon(T_j) = 0$, all j.

In general, there will be no such homomorphism. However *for* **commutative** *K-algebras, R, we can arrange a "section"*[4]*, ϵ, after base extension.* Namely, we pass to $R \otimes_K R$ and set $\epsilon(r \otimes s) = rs \in R$; so now R plays the role of K and $R \otimes_K R$ the role of R. (The map $\epsilon\colon R \to K$ is also called an *augmentation of R as K-algebra.*) Hence, the basic principle is that *after base extension* (at least for commutative R) *our K-algebra has a section; we operate assuming a section and then try to use descent* (cf. Chapter 2, Section 2.8).

This technique doesn't quite work with non-commutative R, where we base extend to get $R^e = R \otimes_K R^{\mathrm{op}}$ and try $\partial_0\colon R^e \to R$ for our ϵ. We certainly find that R is an R^e-module, that ∂_0 is an R^e-module map, that the composition $R \xrightarrow{i} R^e \longrightarrow R$ ($i(r) = r \otimes 1$) is the identity; but, R is **not** in the center of R^e and R^e (with the multiplication we've given it) is not an R-algebra.

Notwithstanding this cautionary remark, we can do a descent-like comparison in the non-commutative case provided R possesses a section $\epsilon\colon R \to K$. In the first place, the section gives K a special position as R-module. We write $I = \mathrm{Ker}\ \epsilon$, this is a two-sided ideal of R called *the augmentation ideal*. Further, consider the augmentation sequence

$$0 \longrightarrow I \longrightarrow R \xrightarrow{\epsilon} K \longrightarrow 0; \tag{$\dagger$}$$

by using condition (iii) above, we see that, as K-modules, $R \cong I \amalg K$. The special position of K as R-module leads to the consideration of the ∂-functor and δ-functor:

$$\begin{aligned} \{\overline{H}_n(R, M) &= \mathrm{Tor}_n^R(M, K)\} \qquad (M \text{ an } R^{\mathrm{op}}\text{-module}) \\ \{\overline{H}^n(R, M) &= \mathrm{Ext}_R^n(K, M)\} \qquad (M \text{ an } R\text{-module}) \end{aligned}$$

which, as usual, are the derived functors of

$$M \rightsquigarrow M/MI$$

and

$$M \rightsquigarrow \{m \in M \mid (\forall \xi \in I)(\xi m = 0)\},$$

respectively. (Here, M is an R^{op}-module for the first functor and an R-module for the second.) You should keep in mind the case: $K = \mathbb{Z}$, $R = \mathbb{Z}[G]$, $\epsilon(\sigma) = 1$ (all σ) throughout what follows. *The idea is to compare the Hochschild groups $H_n(R, M)$ and $H^n(R, M)$ with their "bar" counterparts.*

Secondly, we make precise the notion of giving a two-sided R-module, M, "trivial action" on one of its sides[5]. Given M, a two-sided R-module, we make $\epsilon^* M$ and $\epsilon^{*\mathrm{op}} M$ which are respectively an R^{op}-module ("trivial action" on the left) and an R-module ("trivial action" on the right) as follows:

$$\text{For } m \in \epsilon^* M \text{ and } \lambda^{\mathrm{op}} \in R^{\mathrm{op}}, \qquad \lambda^{\mathrm{op}} \cdot m = m\lambda \qquad \text{and for } \lambda \in R, \qquad \lambda \cdot m = \epsilon(\lambda) m$$

and

$$\text{For } m \in \epsilon^{*\mathrm{op}} M \text{ and } \lambda \in R, \qquad \lambda \cdot m = \lambda m \qquad \text{and for } \lambda^{\mathrm{op}} \in R^{\mathrm{op}}, \qquad \lambda^{\mathrm{op}} \cdot m = m\epsilon(\lambda).$$

Clearly, these ideas can be used to promote one-sided R-modules to two-sided ones (i.e., to R^e-modules), *viz*:

[4]The term "section" is geometric: We have the "structure map" $\mathrm{Spec}\, R \longrightarrow \mathrm{Spec}\, K$ (corresponding to $K \longrightarrow R$) and ϵ gives a continuous map: $\mathrm{Spec}\, K \longrightarrow \mathrm{Spec}\, R$ so that $\mathrm{Spec}\, K \xrightarrow{\epsilon} \mathrm{Spec}\, R \longrightarrow \mathrm{Spec}\ K$ is the identity.

[5]Our earlier, heuristic, discussion was sloppy. For example, in the group ring case and for trivial action on the right, we stated that $\mathbb{Z}[G]$ acts trivially on the right. But, $n \cdot 1 = n \in \mathbb{Z}[G]$ and $m \cdot n \neq m$ if $n \neq 1$; so, our naive idea must be fixed.

Any R, R^{op}, or R^e-module is automatically a K-module and, as K is commutative so that $K^{\mathrm{op}} = K$, we see that $\lambda \cdot m = m \cdot \lambda$ for $\lambda \in K$ in any of these cases. Now if we have an R-module, M, we make R^e operate by

$$(r \otimes s^{\mathrm{op}}) \cdot m = rm\epsilon(s) = r\epsilon(s)m = \epsilon(s)rm,$$

and similarly for R^{op}-modules, M, we use the action

$$(r \otimes s^{\mathrm{op}}) \cdot m = \epsilon(r)ms = m\epsilon(r)s = ms\epsilon(r).$$

When we use the former action and pass from an R-module to an R^e-module, we denote that R^e-module by $\epsilon_*^{\mathrm{op}}(M)$; similarly for the latter action, we get the R^e-module $\epsilon_*(M)$. And so we have pairs of functors

$$\begin{cases} \epsilon^*\colon R^e\text{-mod} \rightsquigarrow R^{\mathrm{op}}\text{-mod} \\ \epsilon_*\colon R^{\mathrm{op}}\text{-mod} \rightsquigarrow R^e\text{-mod} \end{cases}$$

and

$$\begin{cases} \epsilon^{*\mathrm{op}}\colon R^e\text{-mod} \rightsquigarrow R\text{-mod} \\ \epsilon_*^{\mathrm{op}}\colon R\text{-mod} \rightsquigarrow R^e\text{-mod} \end{cases}$$

As should be expected, each pair above is a pair of adjoint functors, the upper star is left adjoint to the lower star and we get the following (proof is (DX)):

Proposition 5.26 *If R is a K-algebra with a section $\epsilon\colon R \to K$, then ϵ^* is left-adjoint to ϵ_* and similarly for $\epsilon^{*\mathrm{op}}$ and ϵ_*^{op}. That is, if M is any R^e-module and T and T' are respectively arbitrary R^{op} and R-modules, we have*

$$\begin{aligned} \mathrm{Hom}_{R^{\mathrm{op}}}(\epsilon^* M, T) &\cong \mathrm{Hom}_{R^e}(M, \epsilon_* T) \\ \mathrm{Hom}_R(\epsilon^{*\mathrm{op}} M, T') &\cong \mathrm{Hom}_{R^e}(M, \epsilon_*^{\mathrm{op}} T'). \end{aligned}$$

Lastly, we come to the comparison of the Hochschild groups with their "bar" counterparts. At first, it will be simpler conceptually and notationally (fewer tensor product signs) to pass to a slightly more general case: *R and $\widetilde{R}$ are merely rings and K and $\widetilde{K}$ are chosen modules over R and $\widetilde{R}$ respectively*. In addition we are given module *surjections* $R \xrightarrow{\epsilon} K$ and $\widetilde{R} \xrightarrow{\widetilde{\epsilon}} \widetilde{K}$. By a *map of the pair* $(\widetilde{R}, \widetilde{K})$ *to* (R, K), we understand a ring homomorphism $\varphi\colon \widetilde{R} \to R$ so that $\varphi(\mathrm{Ker}\ \widetilde{\epsilon}) \subseteq \mathrm{Ker}\ \epsilon$. Of course, Ker ϵ and Ker $\widetilde{\epsilon}$ are just left ideals and we obtain a map of groups, $\overline{\varphi}\colon \widetilde{K} \to K$ and a commutative diagram

$$\begin{array}{ccc} \widetilde{R} & \xrightarrow{\varphi} & R \\ {\scriptstyle\widetilde{\epsilon}}\downarrow & & \downarrow{\scriptstyle\epsilon} \\ \widetilde{K} & \xrightarrow{\overline{\varphi}} & K. \end{array}$$

Now the ring map $\varphi\colon \widetilde{R} \to R$ makes every R-module an $\widetilde{R}$-module (same for R^{op}-modules). So, *K is an $\widetilde{R}$-module, and the diagram shows $\overline{\varphi}$ is an $\widetilde{R}$-module map*.

Suppose $\widetilde{P}_\bullet \longrightarrow \widetilde{K} \longrightarrow 0$ is an $\widetilde{R}$-projective resolution of $\widetilde{K}$ and $P_\bullet \longrightarrow K \longrightarrow 0$ is an R-projective resolution of K. We form $R \otimes_{\widetilde{R}} \widetilde{K}$, then we get an R-module map

$$\theta\colon R \otimes_{\widetilde{R}} \widetilde{K} \longrightarrow K$$

via

$$\theta(r \otimes_{\widetilde{R}} \widetilde{k}) = r\overline{\varphi}(\widetilde{k}).$$

(Note that as $\overline{\varphi}$ is an $\widetilde{R}$-module, this makes sense.) Now the complex $R \otimes_{\widetilde{R}} \widetilde{P}_\bullet$ is R-projective and surjects to $R \otimes_{\widetilde{R}} \widetilde{K}$.

By a slight generalization of Theorem 5.2, our R-module map lifts uniquely in $\mathrm{Kom}(R\text{-mod})$ to a map

$$\Theta\colon R \otimes_{\widetilde{R}} \widetilde{P}_\bullet \longrightarrow P_\bullet$$

(over θ, of course). Thus, if M is an R^{op}-module, we get the map on homology

$$H_\bullet(M \otimes_{\widetilde{R}} \widetilde{P}_\bullet) = H_\bullet(M \otimes_R (R \otimes_{\widetilde{R}} \widetilde{P}_\bullet) \longrightarrow H_\bullet(M \otimes_R P_\bullet),$$

while if M is an R-module, we get the map on cohomology

$$H^\bullet(\mathrm{Hom}_R(P_\bullet, M)) \longrightarrow H^\bullet(\mathrm{Hom}_R(R \otimes_{\widetilde{R}} \widetilde{P}_\bullet, M)) = H^\bullet(\mathrm{Hom}_{\widetilde{R}}(\widetilde{P}_\bullet, M)).$$

But, $H_\bullet(M \otimes_{\widetilde{R}} \widetilde{P}_\bullet)$ computes $\mathrm{Tor}_\bullet^{\widetilde{R}}(M, \widetilde{K})$ (where, M is an $\widetilde{R}^{\mathrm{op}}$-module through φ) and $H_\bullet(M \otimes_R P_\bullet)$ computes $\mathrm{Tor}_\bullet^{R}(M, K)$. This gives the map of ∂-functors

$$\mathrm{Tor}_\bullet^{\widetilde{R}}(M, \widetilde{K}) \longrightarrow \mathrm{Tor}_\bullet^{R}(M, K).$$

Similarly, in cohomology we get the map of δ-functors

$$\mathrm{Ext}^\bullet_R(K, M) \longrightarrow \mathrm{Ext}^\bullet_{\widetilde{R}}(\widetilde{K}, M).$$

Our arguments give the first statement of

Theorem 5.27 *If $\varphi\colon (\widetilde{R}, \widetilde{K}) \to (R, K)$ is a map of pairs, then there are induced maps of ∂ and δ–functors*

$$H_\bullet(M, \varphi)\colon \mathrm{Tor}_\bullet^{\widetilde{R}}(M, \widetilde{K}) \longrightarrow \mathrm{Tor}_\bullet^{R}(M, K)$$

(for $M \in R^{\mathrm{op}}$-mod), and

$$H^\bullet(M, \varphi)\colon \mathrm{Ext}^\bullet_R(K, M) \longrightarrow \mathrm{Ext}^\bullet_{\widetilde{R}}(\widetilde{K}, M)$$

(for $M \in R$-mod).

Moreover, the following three statements are equivalent:

(1) $\begin{cases} \text{a) } \theta\colon R \otimes_{\widetilde{R}} \widetilde{K} \to K \text{ is an isomorphism, and} \\ \text{b) } \mathrm{Tor}_n^{\widetilde{R}}(R, \widetilde{K}) = (0) \text{ for } n > 0, \end{cases}$

(2) Both maps $H_\bullet(M, \varphi)$ and $H^\bullet(M, \varphi)$ are isomorphisms for all M,

(3) The map $H_\bullet(M, \varphi)$ is an isomorphism for all M.

Proof. (1) $\Longrightarrow$ (2). Write $\widetilde{P}_\bullet \longrightarrow \widetilde{K} \longrightarrow 0$ for a projective resolution of $\widetilde{K}$. Then $R \otimes_{\widetilde{R}} \widetilde{P}_\bullet \longrightarrow R \otimes_{\widetilde{R}} \widetilde{K} \longrightarrow 0$ is an R-projective complex over $R \otimes_{\widetilde{R}} \widetilde{K}$. By (1)b), it is acyclic and by (1)a) we obtain an R-projective resolution of K. Thus, we may choose as R-projective resolution of K the acyclic complex $R \otimes_{\widetilde{R}} \widetilde{P}_\bullet$. But then, Θ is the identity and (2) follows.

(2) $\Longrightarrow$ (3). This is a tautology.

(3) $\Longrightarrow$ (1). We apply the isomorphism $H_\bullet(M, \varphi)$ for $M = R$. This gives us the isomorphism

$$\mathrm{Tor}_\bullet^{\widetilde{R}}(R, \widetilde{K}) \xrightarrow{\sim} \mathrm{Tor}_\bullet^{R}(R, K).$$

We get (1)a) from the case 0 and (1)b) from $n > 0$. □

Corollary 5.28 *If $\varphi\colon (\widetilde{R}, \widetilde{K}) \to (R, K)$ is a map of pairs and conditions (1)a) and b) of Theorem 5.27 hold, then for any $\widetilde{R}$-projective resolution of $\widetilde{K}$, say $\widetilde{P}_\bullet \longrightarrow \widetilde{K} \longrightarrow 0$, the complex $R \otimes_{\widetilde{R}} \widetilde{P}_\bullet$ is an R-projective resolution of K.*

Proof. This is exactly what we showed in (1) $\Longrightarrow$ (2). $\square$

We apply these considerations to the comparison of the Hochschild groups and their bar counterparts. The idea is to cast R^e in the role of $\widetilde{R}$ (and, since $(R^e)^{\mathrm{op}}$ is K-isomorphic to R^e by the map $\tau\colon s^{\mathrm{op}}\otimes r \mapsto r\otimes s^{\mathrm{op}}$, cast $(R^e)^{\mathrm{op}}$ as $\widetilde{R}$, too). The role of $\widetilde{K}$ is played by R for R^e and by R^{op} for $(R^e)^{\mathrm{op}}$. Then R and K are just themselves and, in the op-case, we use R^{op} and K.

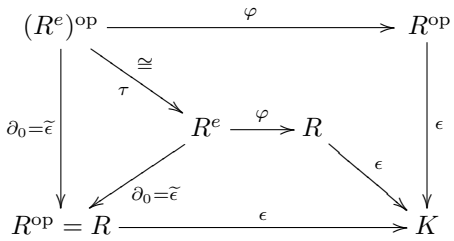
Now $\partial_0\colon R^e \to R$, resp. $\partial_0\colon (R^e)^{\mathrm{op}} \to R^{\mathrm{op}}$, by $\partial_0(r\otimes s^{\mathrm{op}}) = rs$, resp. $\partial_0(s^{\mathrm{op}}\otimes r) = s^{\mathrm{op}}r^{\mathrm{op}} = (rs)^{\mathrm{op}}$, is an R^e-module map, resp. an $(R^e)^{\mathrm{op}}$-module map. Moreover, the diagram

$$\begin{array}{ccc} (R^e)^{\mathrm{op}} & \xrightarrow[\tau]{\sim} & R^e \\ {\scriptstyle\partial_0}\downarrow & & \downarrow{\scriptstyle\partial_0} \\ R^{\mathrm{op}} & \xrightarrow[=]{\mathrm{op}} & R \end{array}$$

commutes for our formulae for ∂_0. So, we cast ∂_0 as $\widetilde{\epsilon}$. But *we need the map of pairs and this is where our section, ϵ, is essential*. Define $\varphi\colon R^e \to R$ (resp. $(R^e)^{\mathrm{op}} \longrightarrow R^{\mathrm{op}}$) by

$$\varphi(r\otimes s^{\mathrm{op}}) = r\epsilon(s) \qquad (\text{resp.} \quad \varphi(s^{\mathrm{op}}\otimes r) = s^{\mathrm{op}}\epsilon(r)).$$

Clearly, φ is a ring homomorphism and as $\operatorname{Ker}\widetilde{\epsilon}$ is generated by $r\otimes 1 - 1\otimes r^{\mathrm{op}}$ (resp. $r^{\mathrm{op}}\otimes 1 - 1\otimes r$), we find $\varphi(\operatorname{Ker}\widetilde{\epsilon}) \subseteq \operatorname{Ker}\epsilon$. There results the commutative diagram of the map of pairs:



Now consider an R-module, M (resp. an R^{op}-module, M), how does φ make M an R^e (resp. $(R^e)^{\mathrm{op}}$)-module? This way:

$$\begin{aligned} (r\otimes s^{\mathrm{op}})\cdot m &= \varphi(r\otimes s^{\mathrm{op}})\cdot m = r\epsilon(s)m \\ (\text{resp.}\quad (s^{\mathrm{op}}\otimes r)\cdot m &= \varphi(s^{\mathrm{op}}\otimes r)\cdot m = s^{\mathrm{op}}\epsilon(r)\cdot m = ms\epsilon(r)). \end{aligned}$$

That is, the R-module, M, goes over to the R^e-module $\epsilon_*^{\mathrm{op}}(M)$ and the R^{op}-module, M, goes over to the $(R^e)^{\mathrm{op}}$-module $\epsilon_*(M)$. Therefore, the map of pairs yields the *comparison maps*

$$\begin{aligned} H_\bullet(M,\varphi)\colon H_\bullet(R,\epsilon_*(M)) = \operatorname{Tor}_\bullet^{R^e}(\epsilon_*(M),R) &\longrightarrow \operatorname{Tor}_\bullet^R(M,K) = \overline{H}_\bullet(R,M) \\ H^\bullet(M,\varphi)\colon \overline{H}^\bullet(R,M) = \operatorname{Ext}^\bullet_R(K,M) &\longrightarrow \operatorname{Ext}^\bullet_{R^e}(R,\epsilon_*^{\mathrm{op}}(M)) = H^\bullet(R,\epsilon_*^{\mathrm{op}}(M)). \end{aligned}$$

Theorem 5.29 *If R is K-projective, then the comparison maps*

$$H_\bullet(M,\varphi)\colon H_\bullet(R,\epsilon_*(M)) \longrightarrow \overline{H}_\bullet(R,M)$$

and

$$H^\bullet(M,\varphi)\colon \overline{H}^\bullet(R,M) \longrightarrow H^\bullet(R,\epsilon_*^{\mathrm{op}}(M))$$

are isomorphisms of ∂ (resp. δ)-functors. Moreover, if $\widetilde{P}_\bullet \longrightarrow R \longrightarrow 0$ is an R^e-projective resolution of R, then $\widetilde{P}_\bullet \otimes_R K$ is an R-projective resolution of K.

Proof. Everything will follow from Theorem 5.27 once we verify conditions (1)a) and b) of that theorem. Here, there is the non-commutativity of R that might cause some confusion. Recall that R^e operates *on the right* on a module, N, *via*

$$n \cdot (r \otimes s^{\mathrm{op}}) = snr;$$

so, R^e operates on $\epsilon_* N$ *via*

$$n \cdot (r \otimes s^{\mathrm{op}}) = \epsilon(s)nr.$$

We apply this when N is R–itself and M is any two-sided R-module. For $\rho \otimes_{R^e} m \in \epsilon_* R \otimes_{R^e} M$, we observe that

$$\epsilon(s)\rho r \otimes_{R^e} m = \rho \cdot (r \otimes s^{\mathrm{op}}) \otimes_{R^e} m = \rho \otimes_{R^e} rms; \qquad (*)$$

hence, the map

$$\alpha \colon \epsilon_* R \otimes_{R^e} M \longrightarrow M \otimes_R K$$

via

$$\alpha(\rho \otimes_{R^e} m) = \rho m \otimes_R 1$$

is well–defined. The only (mildly) tricky thing to check is that α preserves relation $(*)$. But, α of the left side of $(*)$ is $\epsilon(s)\rho rm \otimes_R 1$ and α of the right side of $(*)$ is $\rho rms \otimes_R 1$. Now,

$$zs \otimes_R 1 = z \otimes_R \epsilon(s) = z\epsilon(s) \otimes_R 1;$$

so, α agrees on the left and right sides of $(*)$. And now we see that α is an isomorphism of K-modules because the map

$$\beta \colon M \otimes_R K \longrightarrow \epsilon_* R \otimes_{R^e} M$$

via

$$\beta(m \otimes_R \kappa) = \kappa \otimes_{R^e} m$$

is its inverse. (Note that β is well-defined for:

$$m\rho \otimes_R \kappa = m \otimes_R \epsilon(\rho)\kappa$$

and

$$\epsilon(\rho)\kappa \otimes_{R^e} m = \kappa \cdot (1 \otimes \rho^{\mathrm{op}}) \otimes_{R^e} m = \kappa \otimes_{R^e} m\rho = \beta(m\rho \otimes_R \kappa),$$

while

$$\epsilon(\rho)\kappa \otimes_{R^e} m = \beta(m \otimes_R \epsilon(\rho)\kappa), \qquad \text{as required.)}$$

However,

$$\alpha\beta(m \otimes_R \kappa) = \alpha(\kappa \otimes_{R^e} m) = \kappa m \otimes_R 1 = m \otimes_R \kappa$$

$$\beta\alpha(\rho \otimes_{R^e} m) = \beta(\rho m \otimes_R 1) = 1 \otimes_{R^e} \rho m = \rho \otimes_{R^e} m.$$

We can now apply the K-module isomorphism α. First, take $M = R\,(= \widetilde{K})$. We find that

$$\alpha \colon \epsilon_* R \otimes_{R^e} R \xrightarrow{\sim} R \otimes_R K = K$$

and $\epsilon_* R$ is just R as $\widetilde{R}\,(= R^e$-module). This gives (1)a). To see (1)b), take $\widetilde{P}_\bullet \longrightarrow R \longrightarrow 0$ an $R^e\,(= \widetilde{R})$-projective resolution. We choose $M = \widetilde{P}_\bullet$ an R^e-module (i.e., a complex of same). Now apply α:

$$\mathrm{Tor}^{\widetilde{R}}_\bullet(R, \widetilde{K}) = \mathrm{Tor}^{R^e}_\bullet(\epsilon_* R, R) = H_\bullet(\epsilon_* R \otimes_{R^e} \widetilde{P}_\bullet) \xrightarrow[\alpha]{\sim} H_\bullet(\widetilde{P}_\bullet \otimes_R K).$$

But, R is K-projective and so (by the usual arguments (DX)) $\widetilde{P}_\bullet$ is R^{op}-projective which means the last homology complex computes $\mathrm{Tor}^R_\bullet(R, K)$. We've shown

$$\mathrm{Tor}^{\widetilde{R}}_n(R, \widetilde{K}) \xrightarrow[\alpha]{\sim} \mathrm{Tor}^R_n(R, K).$$

Yet, R is free (so flat) over R and so $\mathrm{Tor}_n^R(R,K) = (0)$ when $n > 0$; we are done. □

Of course, we should apply all this to the standard resolution, $C_\bullet(R)$, when R is K-projective. Here,

$$C_n(R) \otimes_R K = R \otimes_K C_n[R] \otimes_K R \otimes_R K \xrightarrow{\sim} R \otimes_K C_n[R]$$

via the map

$$\Theta_n(r_0 \otimes \cdots \otimes r_{n+1} \otimes_R \kappa) = \epsilon(r_{n+1})\kappa(r_0 \otimes \cdots \otimes r_n).$$

As in the proof of Theorem 5.25, the standard boundary map induces a boundary map, $\overline{\partial}_n$, on $R \otimes_K C_n[R]$, by the formula $\overline{\partial}_n = \Theta_{n-1} \circ \partial_n \circ \Theta_n^{-1}$, and we find

$$\overline{\partial}_n(r_0 \otimes r_1 \otimes \cdots \otimes r_n) = \sum_{i=0}^{n-1}(-1)^i r_0 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n + (-1)^n \epsilon(r_n) r_0 \otimes \cdots \otimes r_{n-1}.$$

This gives us our R-projective resolution $R \otimes_K C_\bullet[R] \longrightarrow K \longrightarrow 0$ with which we can compute. The case when $r_0 = 1$ is most important:

$$\overline{\partial}_n(1 \otimes r_1 \otimes \cdots \otimes r_n) = r_1 \otimes \cdots \otimes r_n + \sum_{i=1}^{n-1}(-1)^i r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n + (-1)^n \epsilon(r_n)(1 \otimes r_1 \otimes \cdots \otimes r_{n-1}).$$

Now, for a right R-module, M, the groups $\mathrm{Tor}_\bullet^R(M,K)$ are the homology of

$$M \otimes_R R \otimes_K C_\bullet[R] = M \otimes_K C_\bullet[R]$$

under $1 \otimes_R \overline{\partial}$. We find

$$\begin{aligned}\overline{\partial}_n(m \otimes_K r_1 \otimes_K \cdots \otimes_K r_n) = {} & m r_1 \otimes_K r_2 \otimes_K \cdots \otimes_K r_n \\ & + \sum_{i=1}^{n-1}(-1)^i m \otimes_K r_1 \otimes_K \cdots \otimes_K r_i r_{i+1} \otimes_K \cdots \otimes_K r_n \\ & + (-1)^n \epsilon(r_n) m \otimes_K r_1 \otimes_K \cdots \otimes_K r_{n-1}.\end{aligned}$$

Therefore, we recover Hochschild's homology formula for $\epsilon_*(M)$, and when $R = \mathbb{Z}[G]$ and $K = \mathbb{Z}$ (with $\epsilon(\sigma) = 1$, all $\sigma \in G$) we also recover the explicit boundary formula for $H_\bullet(G,M)$.

For a left R-module, M, the groups $\mathrm{Ext}^\bullet_R(K,M)$ are the cohomology of

$$\mathrm{Hom}_R(R \otimes_R C_\bullet[R], M) = \mathrm{Hom}_K(C_\bullet[R], M).$$

If, as usual, we write $f(r_1,\ldots,r_n)$ for $f(r_1 \otimes_K r_2 \otimes_K \cdots \otimes_K r_n)$, then

$$\begin{aligned}(\overline{\delta}_n f)(r_1,\ldots,r_{n+1}) = {} & r_1 f(r_2,\ldots,r_{n+1}) \\ & + \sum_{i=1}^{n}(-1)^i f(r_1,\ldots,r_i r_{i+1},\ldots,r_n) \\ & + (-1)^{n+1}\epsilon(r_{n+1}) f(r_1,\ldots,r_n).\end{aligned}$$

Here, $f \in \mathrm{Hom}_K(C_n[R], M)$. Once again, we recover Hochschild's cohomology formula for $\epsilon_*^{\mathrm{op}}(M)$, and when $R = \mathbb{Z}[G]$, *etc.*, we get our explicit coboundary formula for $H^\bullet(G,M)$.

But, we've done more; all this applies to any K-algebra, R, with a section (especially for K-projective algebras). In particular, we might apply it to $R = K[T_1,\ldots,T_n]$ or $R = K\langle T_1,\ldots,T_n\rangle$, with $\epsilon(T_j) = 0$ for $j = 1,2,\ldots,n$. The standard resolution though is very inefficient for we must know $m \otimes r_1 \otimes \cdots \otimes r_l$

or $f(r_1, \ldots, r_l)$ on *all* monomials r_j of whatever degree. Instead we will find a better resolution, but we postpone this until Section 5.5 where it fits better.

Let us turn to the cohomology of sheaves and presheaves. These objects have been introduced already and we assume that Problem 69 has been mastered. Here, we'll be content to examine ordinary topological spaces (as in part (a) of that exercise) and (pre)sheaves on them. The most important fact is that the categories of presheaves and sheaves of R-modules on the space X have enough injectives. Let us denote by $\mathcal{P}(X, R\text{-mod})$ and $\mathcal{S}(X, R\text{-mod})$ these two abelian categories. Remember that

$$0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$$

is exact in $\mathcal{P}(X, R\text{-mod})$ iff the sequence of R-modules

$$0 \longrightarrow F'(U) \longrightarrow F(U) \longrightarrow F''(U) \longrightarrow 0$$

is exact for *every* open U of X. But for sheaves, the situation is more complicated:

$$0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$$

is exact in $\mathcal{S}(X, R\text{-mod})$ iff

(a) $0 \longrightarrow F'(U) \longrightarrow F(U) \longrightarrow F''(U)$ is exact for every open U or X *and*

(b) For each open U and each $\xi \in F''(U)$, there is an open cover $\{U_\alpha \longrightarrow U\}_\alpha$ so that each $\xi_\alpha \, (= \rho_U^{U_\alpha}(\xi))$ is the image of some $\eta_\alpha \in F(U_\alpha)$ under the map $F(U_\alpha) \longrightarrow F''(U_\alpha)$.

A more perspicacious way of saying this is the following: Write $i\colon \mathcal{S}(X, R\text{-mod}) \rightsquigarrow \mathcal{P}(X, R\text{-mod})$ for the full embedding which regards a sheaf as a presheaf. There is a functor, $\#\colon \mathcal{P}(X, R\text{-mod}) \rightsquigarrow \mathcal{S}(X, R\text{-mod})$ which is left adjoint to i. That is, for $F \in \mathcal{S}$ and $G \in \mathcal{P}$, we have

$$\mathrm{Hom}_{\mathcal{S}}(G^{\#}, F) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{P}}(G, i(F)).^6$$

We can now say (b) this way: If $\mathrm{cok}(F \longrightarrow F'')$ is the presheaf cokernel

$$\mathrm{cok}(F \longrightarrow F'')(U) = \mathrm{cok}(F(U) \longrightarrow F''(U)),$$

then $\mathrm{cok}(F \longrightarrow F'')^{\#} = (0)$.

Given $x \in X$, and a (pre)sheaf, F, we define the *stalk of* F *at* x, denoted F_x, by

$$F_x = \varinjlim_{\{U \ni x\}} F(U).$$

It's easy to see that $(F^{\#})_x = F_x$ for any presheaf, F. Stalks are important because of the following simple fact:

Proposition 5.30 *If $F \xrightarrow{\varphi} G$ is a map of sheaves, then φ is injective (surjective, bijective) if and only if the induced map $\varphi_x\colon F_x \to G_x$ on stalks is injective (surjective, bijective) for every $x \in X$.*

We leave the proof as a (DX).

[6] One constructs # by two successive limits. Given U, open in X, write $G^{(+)}(U)$ for

$$G^{(+)}(U) = \varinjlim_{\{U_\alpha \longrightarrow U\}} \mathrm{Ker}\,\Big(\prod_\alpha G(U_\alpha) \rightrightarrows \prod_{\beta,\gamma} G(U_\beta \cap U_\gamma)\Big)$$

(the limit taken over all open covers of U) and set $G^{\#}(U) = G^{(+)(+)}(U)$.

This result is false for presheaves, they are not local enough.

Property (a) above shows that i is left-exact and the proposition shows $\#$ is exact. To get at the existence of enough injectives, we investigate what happens to $\mathcal{P}(X, R\text{-mod})$ and $\mathcal{S}(X, R\text{-mod})$ if we have a map of spaces $f\colon X \to Y$. In the first place, if F is a (pre)sheaf on X, we can define a (pre)sheaf f_*F, called the *direct image of F by f via*

$$(f_*F)(V) = F(f^{-1}(V)), \quad V \text{ open in } Y.$$

A simple check shows that the direct image of a sheaf is again a sheaf. Now, in the second place, we want a functor $f^*\colon \mathcal{P}(Y) \rightsquigarrow \mathcal{P}(X)$ (resp. $\mathcal{S}(Y) \rightsquigarrow \mathcal{S}(X)$) which will be left adjoint to f_*. If we knew the (classical) way to get a sheaf from its stalks, we could set $(f^*G)_x = G_{f(x)}$ for $G \in \mathcal{S}(Y)$ and $x \in X$ any point. But from our present point of view this can't be done. However, our aim is for an adjoint functor, so we can use the method of D. Kan [30].

We start we a presheaf, G, on Y and take an open set, U, of X. We set

$$(f^*G)(U) = \varinjlim_{\{f^{-1}(V) \supseteq U\}} G(V),$$

here, as noted, V ranges over all opens of Y with $f^{-1}(V) \supseteq U$. Then, f^*G is a presheaf (of R-modules) on X. If G is a sheaf on Y, we form f^*G, as above, and then take $(f^*G)^{\#}$. We'll continue to denote the latter sheaf by f^*G if no confusion results. Once the idea of defining f^*G by a direct limit is in hand, it is easy to prove (and the proof will be left as a (DX)):

Proposition 5.31 *If $f\colon X \to Y$ is a map of topological spaces, then the functors f^* from $\mathcal{P}(Y)$ to $\mathcal{P}(X)$ (resp. from $\mathcal{S}(Y)$ to $\mathcal{S}(X)$) are left adjoint to the direct image functors. That is, for $G \in \mathcal{P}(Y)$ and $F \in \mathcal{P}(X)$ (resp. $G \in \mathcal{S}(Y)$ and $F \in \mathcal{S}(X)$), we have functorial isomorphisms*

$$\mathrm{Hom}_{\mathcal{P}(X)}(f^*G, F) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{P}(Y)}(G, f_*F)$$

(resp.

$$\mathrm{Hom}_{\mathcal{S}(X)}(f^*G, F) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{S}(Y)}(G, f_*F)).$$

Moreover, we have $(f^*G)_x = G_{f(x)}$, for all $x \in X$.

Since $\varinjlim$ is an exact functor on R-mod, our definition of the presheaf f^*G shows that *f^* is an exact functor $\mathcal{P}(Y) \rightsquigarrow \mathcal{P}(X)$*. The statement in the proposition about stalks shows (by Proposition 5.30) that *f^* is also an exact functor $\mathcal{S}(Y) \rightsquigarrow \mathcal{S}(X)$*. Of course, *$f_*$ is a left-exact functor on sheaves and an exact functor on presheaves*.

There is a useful lemma that connects pairs of adjoint functors and injectives—it is what we'll use to get enough injectives in $\mathcal{P}$ and $\mathcal{S}$.

Lemma 5.32 *Say $\mathcal{A}$ and $\mathcal{B}$ are abelian categories and $\alpha\colon \mathcal{A} \rightsquigarrow \mathcal{B}$ and $\beta\colon \mathcal{B} \rightsquigarrow \mathcal{A}$ are functors with β left adjoint to α. If β is exact, then α carries injectives of $\mathcal{A}$ to injectives of $\mathcal{B}$.*

Proof. Take an injective, Q, of $\mathcal{A}$ and consider the co-functor (on $\mathcal{B}$)

$$T \rightsquigarrow \mathrm{Hom}_{\mathcal{B}}(T, \alpha(Q)).$$

By adjointness, this is exactly

$$T \rightsquigarrow \mathrm{Hom}_{\mathcal{A}}(\beta(T), Q).$$

Now, $\mathrm{Hom}_{\mathcal{A}}(\beta(-), Q)$ is the composition of the exact functor β with the exact functor $\mathrm{Hom}_{\mathcal{A}}(-, Q)$ (the latter being exact as Q is injective). But then, $\mathrm{Hom}_{\mathcal{B}}(-, \alpha(Q))$ is exact, i.e., $\alpha(Q)$ is injective in $\mathcal{B}$. □

If we apply the lemma to the cases $\alpha = i$, $\beta = \#$; $\alpha = f_*$, $\beta = f^*$, we get

Corollary 5.33 *Let $f\colon X \to Y$ be a map of topological spaces and write $\mathcal{P}(X)$, etc. for the categories of R-module presheaves on X, etc. Further consider the functors $i\colon \mathcal{S}(X) \rightsquigarrow \mathcal{P}(X)$ and $\#\colon \mathcal{P}(X) \rightsquigarrow \mathcal{S}(X)$. Then,*

(1) If Q is an injective in $\mathcal{P}(X)$, the presheaf $f_*(Q)$ is injective on Y.

(2) If Q is an injective in $\mathcal{S}(X)$, the sheaf $f_*(Q)$ is injective on Y.

(3) If Q is an injective sheaf on X, then $i(Q)$ is an injective presheaf on X.

Theorem 5.34 *If X is a topological space, then the category $\mathcal{S}(X, R\text{-mod})$ possesses enough injectives.*

Proof. Pick any point, ξ, of X and consider the map of spaces $i_\xi\colon \{\xi\} \hookrightarrow X$. The categories $\mathcal{P}(\{\xi\})$ and $\mathcal{S}(\{\xi\})$ are each just R-mod, and for any module, M, we have

$$i_{\xi *}(M)(U) = \begin{cases} M & \text{if } \xi \in U \\ (0) & \text{if } \xi \notin U. \end{cases}$$

For any sheaf F on X, look at its stalk, F_ξ, at ξ and embed F_ξ into an injective R-module Q_ξ (say $j_\xi\colon F_\xi \hookrightarrow Q_\xi$ is the embedding). We form $i_{\xi *}(Q_\xi)$ which is an injective sheaf on X by Corollary 5.33 and then form $Q = \prod_{\xi \in X} i_{\xi *}(Q_\xi)$, again an injective sheaf on X. Note that

$$Q(U) = \prod_{\xi \in U} Q_\xi.$$

Now, I claim that the map $\theta\colon F \to Q$ *via*

$$\text{for } z \in F(U)\colon \theta(z) = (j_\xi(z_\xi))_{\xi \in U},$$

where z_ξ is the image of z in F_ξ, is the desired embedding. If $\theta(z) = 0$, then for each $\xi \in U$, the elements $j_\xi(z_\xi) = 0$; as j_ξ is an embedding, we get $z_\xi = 0$. By the definition of stalk, there is a neighborhood, U_ξ, of ξ in U where $\rho_U^{U_\xi}(z) = 0$. These neighborhoods give a covering of U, so we see that z goes to zero under the map

$$F(U) \longrightarrow \prod_{\xi \in U} F(U_\xi). \tag{+}$$

But, this map is injective by the sheaf axiom; so, $z = 0$. □

Remark: The theorem is also true for presheaves and our proof above works for "good" presheaves; that is, those for which the maps (+) are indeed injective. (For general presheaves, G, the presheaf $G^{(+)}$ will satisfy (+) is injective). We can modify the argument to get the result for $\mathcal{P}(X)$ or use a different argument; this will be explored in the exercises.

To define cohomology with coefficients in a sheaf, F, on X, we consider the functor

$$\Gamma\colon F \rightsquigarrow F(X).$$

We already know this is left exact and we define *the cohomology of X with coefficients in F* by

$$H^\bullet(X, F) = (R^\bullet\Gamma)(F).$$

A little more generally, if U is open in X, we can set $\Gamma_U(F) = F(U)$ and then

$$H^\bullet(U, F) = (R^\bullet\Gamma_U)(F).$$

If we assume proved the existence of enough injectives in $\mathcal{P}(X)$, then for a presheaf, G, we set

$$\check{H}^0(X,G) = G^{(+)}(X) = \varinjlim_{\{U_\alpha \longrightarrow U\}} \operatorname{Ker}\left(\prod_\alpha G(U_\alpha) \rightrightarrows \prod_{\beta,\gamma} G(U_\beta \cap U_\gamma)\right)$$

and define

$$\check{H}^\bullet(X,G) = (R^\bullet \check{H}^0)(G).$$

There is an explicit complex that computes $\check{H}^\bullet(X,G)$, see the exercises. The R-modules $\check{H}^\bullet(X,G)$ are called the *Čech cohomology groups of X with coefficients in the presheaf G*. Again, as above, we can generalize to cohomology over an open, U.

Pick open $U \subseteq X$, and write $\mathfrak{R}_U$ for the presheaf

$$\mathfrak{R}_U(V) = \begin{cases} R & \text{if } V \subseteq U \\ (0) & \text{if } V \not\subseteq U \end{cases}$$

(so, $\mathfrak{R}_X$ is the constant presheaf, R). Also write R_U for the sheaf $(\mathfrak{R}_U)^\#$. It turns our that the $\mathfrak{R}_U$ form a set of generators for $\mathcal{P}(X)$, while the same is true for the R_U in $\mathcal{S}(X)$. Moreover, we have

Proposition 5.35 *If X is a topological space and U is a given open set, then we have an isomorphism of δ-functors*

$$H^\bullet(U,-) \cong \operatorname{Ext}^\bullet_{\mathcal{S}(X)}(R_U,-)$$

on the category $\mathcal{S}(X)$ to R-mod.

Proof. All we have to check is that they agree in dimension 0. Now,

$$\operatorname{Hom}_{\mathcal{S}(X)}(R_U,F) \cong \operatorname{Hom}_{\mathcal{P}(X)}(\mathfrak{R}_U, i(F)).$$

Notice that $\rho^V_U \colon \mathfrak{R}(U) \to \mathfrak{R}(V)$ is just the identity if $V \subseteq U$ and is the zero map otherwise. It follows that

$$\operatorname{Hom}_{\mathcal{P}(X)}(\mathfrak{R}_U, i(F)) \cong \operatorname{Hom}_{R\text{-mod}}(R, F(U)) = F(U),$$

and we are done. □

We don't compute $\operatorname{Ext}^\bullet_{\mathcal{S}(X)}(R_U,F)$ by projectively resolving R_U—such a resolution doesn't exist in $\mathcal{S}(X)$. Rather, we injectively resolve F.

Recall that we have the left exact functor $i \colon \mathcal{S}(X) \rightsquigarrow \mathcal{P}(X)$, so we can inquire as to its right derived functors, $R^\bullet i$. The usual notation for $(R^\bullet i)(F)$ is $\mathcal{H}^\bullet(F)$—these are presheaves. We compute them as follows:

Proposition 5.36 *The right derived functors $\mathcal{H}^\bullet(F)$ are given by*

$$\mathcal{H}^\bullet(F)(U) = H^\bullet(U,F).$$

Proof. It should be clear that for fixed F, each $H^p(U,F)$ is functorial in U; that is, $U \rightsquigarrow H^p(U,F)$ is a presheaf. Moreover, it is again clear that

$$F \rightsquigarrow H^\bullet(U,F)$$

is a δ-functor from $\mathcal{S}(X)$ to $\mathcal{P}(X)$. If Q is injective in $\mathcal{S}(X)$, we have $H^p(U,Q) = (0)$ when $p > 0$; so, our δ-functor is effaceable. But, for $p = 0$, the R-module $H^0(U,F)$ is just $F(U)$; i.e., it is just $\mathcal{H}^0(F)(U)$. By the uniqueness of universal δ-functors, we are done. □

For the computation of the cohomology of sheaves, manageable injective resolutions turn out to be too hard to find. Sometimes one can prove cohomology can be computed by the Čech method applied to $i(F)$, and then the explicit complex of the exercises works quite well. This will depend on subtle properties of the space, X. More generally, Godement [18] showed that a weaker property than injectivity was all that was needed in a resolution of F to compute the R-module $H^\bullet(X,F)$. This is the notion of flasqueness.[7]

[7] The French word "flasque" can be loosely translated as "flabby".

Definition 5.8 A sheaf, F, on the space X is *flasque* if and only if for each pair of opens $V \subseteq U$ of X, the map

$$\rho_U^V \colon F(U) \to F(V)$$

is surjective. Of course, this is the same as $F(X) \longrightarrow F(U)$ being surjective for each open, U.

Here are two useful lemmas that begin to tell us how flasque sheaves intervene in cohomology.:

Lemma 5.37 *The following are equivalent statements about a sheaf, F', on the space X:*

(1) Every short exact sequence in $\mathcal{S}(X)$

$$0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$$

is exact in $\mathcal{P}(X)$.

(2) For every open U of X, the R-module $H^1(U, F')$ is zero.

Proof. (1) $\Longrightarrow$ (2). Embed F' in an injective and pick open $U \subseteq X$. From $0 \longrightarrow F' \longrightarrow Q \longrightarrow \mathrm{cok} \longrightarrow 0$, we get

$$0 \longrightarrow F'(U) \longrightarrow Q(U) \longrightarrow \mathrm{cok}(U) \longrightarrow H^1(U, F') \longrightarrow (0);$$

By (1), $0 \longrightarrow F'(U) \longrightarrow Q(U) \longrightarrow \mathrm{cok}(U) \longrightarrow 0$ is exact; so, $H^1(U, F') = (0)$.

(2) $\Longrightarrow$ (1). Just apply cohomology over U to the short exact sequence $0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$. We get

$$0 \longrightarrow F'(U) \longrightarrow F(U) \longrightarrow F''(U) \longrightarrow H^1(U, F').$$

By (2), we're done as U is an arbitrary open. □

Lemma 5.38 *Say F' is a flasque sheaf and $0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$ is exact in $\mathcal{S}(X)$. Then it is exact in $\mathcal{P}(X)$. Moreover, if $0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$ is exact in $\mathcal{S}(X)$, then F is flasque if and only if F'' is flasque (of course, F' is always assumed to be flasque).*

Proof. Pick any open $U \subseteq X$; all we must prove is that $F(U) \longrightarrow F''(U)$ is surjective. Write Σ for the collection of pairs (V, σ) where V is open, $V \subseteq U$ and σ is a lifting to $F(V)$ of $\rho_U^V(s) \in F''(V)$ for some $s \in F''(U)$ fixed once and for all. As s admits liftings to F *locally on* U, our set Σ is non-empty. Now partially order Σ in the standard way: $(V, \sigma) \leq (\widetilde{V}, \widetilde{\sigma})$ iff $V \subseteq \widetilde{V}$ and $\rho_{\widetilde{V}}^V(\widetilde{\sigma}) = \sigma$. Of course, Σ is inductive and Zorn's Lemma yields a maximal lifting, σ_0, of s defined on $V_0 \subseteq U$. We must prove $V_0 = U$.

Were it not, there would exist $\xi \in U$ with $\xi \notin V_0$. Now the stalk map $F_\xi \longrightarrow F''_\xi$ is surjective, so the image of s in some small neighborhood, $U(\xi)$, of ξ in U lifts to an element $\tau \in F(U(\xi))$. We will get an immediate contradiction if $U(\xi) \cap V_0 = \emptyset$, for then $\widetilde{U} = U(\xi) \cup V_0$ has two opens as a *disjoint* cover and $F(\widetilde{U}) = F(U(\xi)) \prod F(V_0)$ by the sheaf axiom. The pair $\langle \tau, \sigma_0 \rangle$ is a lifting of s to a bigger open than V_0—a contradiction.

Therefore, we may assume $U(\xi) \cap V_0 \neq \emptyset$—it is here that the flasqueness of F' enters. For on the intersection both $\rho_{U(\xi)}^{U(\xi)\cap V_0}(\tau)$ and $\rho_{V_0}^{U(\xi)\cap V_0}(\sigma_0)$ lift $\rho_U^{U(\xi)\cap V_0}(s)$. Thus, there is an "error" $\epsilon \in F'(U(\xi) \cap V_0)$, so that

$$\rho_{V_0}^{U(\xi)\cap V_0}(\sigma_0) - \rho_{U(\xi)}^{U(\xi)\cap V_0}(\tau) = \epsilon.$$

As F' is flasque, ϵ lifts to $F'(U(\xi))$; call it ϵ again on this bigger open. Then $\tau + \epsilon$ also lifts $\rho_U^{U(\xi)}(s)$ and $\tau + \epsilon$ and σ_0 now agree on $U(\xi) \cap V_0$; so, the sheaf axiom shows we get a lifting to the bigger open $U(\xi) \cup V_0$—our last contradiction. Thus, $U = V_0$.

For the second statement, in which F' is given as a flasque sheaf, pick open $V \subseteq U$ in X. We have the commutative diagam

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F'(U) & \longrightarrow & F(U) & \longrightarrow & F''(U) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \rho'} & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho''} & & \\ 0 & \longrightarrow & F'(V) & \longrightarrow & F(V) & \longrightarrow & F''(V) & \longrightarrow & 0, \end{array}$$

in which $\mathrm{Coker}\,(\rho') = (0)$, By the snake lemma

$$\mathrm{Coker}\,(\rho) \xrightarrow{\sim} \mathrm{Coker}\,(\rho''),$$

and we are done. □

Remark: There is an important addendum to Lemma 5.37. We mention this as the method of argument is fundamental in many applications. This addendum is: *The statement*

(3) $\check{H}^1(U, i(F')) = (0)$ *for all* U *open in* X*, is equivalent to either properties (1) or (2) of Lemma 5.37.*

Let us show (3) $\Longleftrightarrow$ (1). So say (3) holds. This means given any open cover of U, say $U = \bigcup_\alpha U_\alpha$, and any elements $z_{\alpha\beta} \in F'(U_\alpha \cap U_\beta)$ so that

$$z_{\alpha\beta} = -z_{\beta\alpha} \quad \text{and} \quad z_{\alpha\gamma} = z_{\alpha\beta} + z_{\beta\gamma} \quad \text{on } U_\alpha \cap U_\beta \cap U_\gamma \tag{$*$}$$

we can find elements $z_\alpha \in F'(U_\alpha)$ so that $z_{\alpha\beta} = z_\alpha - z_\beta$ on $U_\alpha \cap U_\beta$. Now suppose we have $s \in F''(U_\alpha)$, we can cover U by opens U_α so that the $s_\alpha = \rho_U^{U_\alpha}(s) \in F''(U_\alpha)$ lift to $\sigma_\alpha \in F(U_\alpha)$ for all α. The elements $\sigma_\alpha - \sigma_\beta \in F(U_\alpha \cap U_\beta)$ are not necessarily 0 but go to zero in $F''(U_\alpha \cap U_\beta)$. That is, if we set $z_{\alpha\beta} = \sigma_\alpha - \sigma_\beta$, the $z_{\alpha\beta}$ belong to $F'(U_\alpha \cap U_\beta)$. These $z_{\alpha\beta}$ satisfy $(*)$ and so by (3) we get $z_{\alpha\beta} = z_\alpha - z_\beta$ for various $z_\alpha \in F'(U_\alpha)$. Thus

$$z_\alpha - z_\beta = \sigma_\alpha - \sigma_\beta \quad \text{on } U_\alpha \cap U_\beta,$$

that is

$$\sigma_\alpha - z_\alpha = \sigma_\beta - z_\beta \quad \text{on } U_\alpha \cap U_\beta.$$

This equality and the sheaf axiom for F give us an element $\sigma \in F(U)$ with $\rho_U^{U_\alpha}(\sigma) = \sigma_\alpha - z_\alpha$. The z_α go to zero in F'', thus σ lifts s and this shows $F(U) \longrightarrow F''(U)$ is surjective.

To show (1) $\Longrightarrow$ (3), we simply embed F' in an injective again to get $0 \longrightarrow F' \longrightarrow Q \longrightarrow \mathrm{cok} \longrightarrow 0$ in $\mathcal{S}(X)$. By (1), the sequence

$$0 \longrightarrow i(F') \longrightarrow i(Q) \longrightarrow i(\mathrm{cok}) \longrightarrow 0$$

is exact in $\mathcal{P}(X)$ and $i(Q)$ is an injective of $\mathcal{P}(X)$. Apply Čech cohomology (a δ-functor on $\mathcal{P}(X)$):

$$0 \longrightarrow F'(U) \longrightarrow Q(U) \longrightarrow \mathrm{cok}(U) \longrightarrow \check{H}^1(U, i(F')) \longrightarrow 0$$

is exact. Since $Q(U) \longrightarrow \mathrm{cok}(U)$ is surjective, by (1), we get (3). □

Proposition 5.39 *Every injective sheaf is a flasque sheaf. For every flasque sheaf,* F*, and every open* U*, we have* $H^n(U, F) = (0)$ *for* $n > 0$*.*

Proof. Pick open $V \subseteq U$, call our injective sheaf Q. Since $V \subseteq U$, we have the exact sequence

$$0 \longrightarrow R_V \longrightarrow R_U \longrightarrow \mathrm{cok} \longrightarrow 0$$

in $\mathcal{S}(X)$. Now $\mathrm{Hom}_{\mathcal{S}(X)}(-, Q)$ is an exact functor; so

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{S}(X)}(\mathrm{cok}, Q) \longrightarrow \mathrm{Hom}_{\mathcal{S}(X)}(R_U, Q) \longrightarrow \mathrm{Hom}_{\mathcal{S}(X)}(R_V, Q) \longrightarrow 0$$

is exact. The middle and right-hand groups are $Q(U)$ and $Q(V)$ respectively; so Q is flasque.

Let's prove the second statement by induction on n. Take a flasque sheaf, F. By Lemmas 5.37 and 5.38, we have $H^1(U, F) = (0)$ for all open U. Now embed F in an injective sheaf

$$0 \longrightarrow F \longrightarrow Q \longrightarrow \text{cok} \longrightarrow 0.$$

By Lemma 5.38 and the above, the sheaf cok is also flasque. So by our induction hypothesis all the groups $H^p(U, \text{cok}) = (0)$ for $1 \leq p \leq n-1$. Now apply cohomology to our exact sequence; this gives

$$H^p(U, \text{cok}) \xrightarrow{\sim} H^{p+1}(U, F), \quad \text{for } p \geq 1.$$

When $p = n-1$ this gives the induction step for F. □

The important part of this proposition is that *flasque sheaves are acyclic objects over every open U of X*; that is, $H^n(U, F) = (0)$ for all $n > 0$ and every open U. And now we have the following general

Proposition 5.40 *Suppose $\mathcal{A}$ is an abelian category, T is a left exact functor from $\mathcal{A}$ to R-mod and*

$$0 \longrightarrow F \longrightarrow L_0 \longrightarrow L_1 \longrightarrow \cdots$$

is an acyclic resolution of F by $R^\bullet T$-acyclic objects $L_0, L_1, \ldots$ (That is, $(R^pT)(L_j) = (0)$, all $p > 0$, all $j \geq 0$.) Then the cohomology of the complex

$$T(L_0) \longrightarrow T(L_1) \longrightarrow T(L_2) \longrightarrow \cdots$$

computes the derived functors of T on the object F (i.e., the $(R^nT)(F)$, $n \geq 0$).

Proof. We use induction on n and décalage. (There are other methods of proof, *e.g.*, by double complexes.) Of course, the assertion for $n = 0$ is true and trivial, being independent of resolutions. So assume for an object G resolved by a sequence of the L's, we have $(R^pT)(G) = H^p(T(L_\bullet))$ for $0 \leq p \leq n-1$. Then the sequence,

$$0 \longrightarrow F \longrightarrow L_0 \longrightarrow \text{cok} \longrightarrow 0$$

yields the resolution

$$0 \longrightarrow \text{cok} \longrightarrow L_1 \longrightarrow L_2 \longrightarrow \cdots \tag{$\dagger$}$$

and the cohomology sequence

$$0 \longrightarrow T(F) \longrightarrow T(L_0) \longrightarrow T(\text{cok}) \longrightarrow (R^1T)(F) \longrightarrow \cdots$$
$$\longrightarrow (R^pT)(L_0) \longrightarrow (R^pT)(\text{cok}) \longrightarrow (R^{p+1}T)(F) \longrightarrow (R^{p+1}T)(L_0) \longrightarrow \cdots.$$

If $p \geq 1$, we get

$$(R^pT)(\text{cok}) \xrightarrow{\sim} (R^{p+1}T)(F)$$

while for $p = 0$, we get

$$T(L_0) \longrightarrow T(\text{cok}) \longrightarrow (R^1T)(F) \longrightarrow 0. \tag{$\dagger\dagger$}$$

Now by induction hypothesis on n, $(R^pT)(\text{cok})$ is the pth cohomology of $T(L_1) \longrightarrow T(L_2) \longrightarrow \cdots$, for $p \leq n-1$. This is exactly the $p+1$ cohomology of $T(L_0) \longrightarrow T(L_1) \longrightarrow \cdots$, that is $H^{p+1}(T(L_\bullet))$. So,

$$H^{p+1}(T(L_\bullet)) = (R^pT)(\text{cok}) \xrightarrow{\sim} (R^{p+1}T)(F)$$

if $1 \leq p \leq n-1$. As long as $n \geq 2$, we can set $p = n-1$ and get the induction step.

So, all that remains is the step from $n = 0$ to $n = 1$. From (†), we see

$$T(\mathrm{cok}) \xrightarrow{\sim} \mathrm{Ker}\,(T(L_1) \longrightarrow T(L_2)).$$

By the short exact sequence for F, L_0, cok, we find that $\mathrm{Im}\,(T(L_0) \longrightarrow T(\mathrm{cok}))$ is exactly the image $(T(L_0) \longrightarrow T(L_1))$; that means

$$T(\mathrm{cok})/T(L_0) = H^1(T(L_\bullet)).$$

But, we know

$$T(\mathrm{cok})/T(L_0) \xrightarrow{\sim} (R^1T)(F)$$

by (††), and we are done. □

Of course, we apply this to resolving a sheaf, F, by flasque sheaves. If we do this, we get a complex (upon applying Γ_U) and so from its cohomology we compute the $H^p(U, F)$. It remains to give a canonical procedure for resolving each F by flasque sheaves. This is Godement's method of "discontinuous sections".

Definition 5.9 For a sheaf, F, write $\mathcal{G}(F)$ for the presheaf

$$\mathcal{G}(F)(U) = \prod_{x \in U} F_x,$$

and call $\mathcal{G}(F)$ the *sheaf of discontinuous sections of* F.

Remarks:

(1) $\mathcal{G}(F)$ is always a sheaf.

(2) $\mathcal{G}(F)$ *is flasque*. For, a section over V of $\mathcal{G}(F)$ is merely a function on V to $\bigcup_{x \in V} F_x$ so that its value at x lies in F_x. We merely extend by zero outside V and get our lifting to a section of U (with $U \supseteq V$).

(3) *There is a canonical embedding* $F \longrightarrow \mathcal{G}(F)$. To see this, if $s \in F(U)$, we have $s(x) \in F_x$, its image in $F_x = \varinjlim_{V \ni x} F(V)$. We send s to the function $x \mapsto s(x)$ which lies in $\mathcal{G}(F)(U)$. Now, if s and t go to the same element of $\mathcal{G}(F)(U)$, we know for each $x \in U$, there is a small open $U(x) \subseteq U$ where $s = t$ on $U(x)$ (i.e., $\rho_U^{U(x)}(s) = \rho_U^{U(x)}(t)$). But these $U(x)$ cover U, and the sheaf axiom says $s = t$ in $F(U)$.

Therefore, $\mathcal{S}(X, R\text{-mod})$ has enough flasques; *so every sheaf, F, possesses a canonical flasque resolution* (the Godement resolution) : Namely

$$\begin{array}{l} 0 \longrightarrow F \longrightarrow \mathcal{G}(F) \longrightarrow \mathrm{cok}_1 \longrightarrow 0 \\ 0 \longrightarrow \mathrm{cok}_1 \longrightarrow \mathcal{G}(\mathrm{cok}_1) \longrightarrow \mathrm{cok}_2 \longrightarrow 0 \\ \qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots \\ 0 \longrightarrow \mathrm{cok}_n \longrightarrow \mathcal{G}(\mathrm{cok}_n) \longrightarrow \mathrm{cok}_{n+1} \longrightarrow 0 \cdots \end{array}$$

This gives

$$0 \longrightarrow F \longrightarrow \mathcal{G}_0(F) \longrightarrow \mathcal{G}_1(F) \longrightarrow \cdots \longrightarrow \mathcal{G}_n(F) \longrightarrow \cdots,$$

where we have set

$$\mathcal{G}_0(F) = \mathcal{G}(F) \quad \text{and} \quad \mathcal{G}_n(F) = \mathcal{G}(\mathrm{cok}_n) \quad \text{when } n \geq 1.$$

It's not hard to extend all our results on sheaves of R-modules to sheaves of $\mathcal{O}_X$-modules, where $\mathcal{O}_X$ is a *sheaf of rings on* X. To replace maps of spaces, we need the notion of a *map of ringed spaces* (i.e., of pairs $(X, \mathcal{O}_X)$ in which $\mathcal{O}_X$ is a sheaf of rings on X): By a map $(X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ of ringed spaces, we understand a pair (f, φ) in which f is a map $X \longrightarrow Y$ and φ is a map of sheaves $\mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ (over

Y). For intuition think of $\mathcal{O}_X$ as the sheaf of germs of continuous functions on X. If F is an $\mathcal{O}_X$-module, then f_*F will be an $\mathcal{O}_Y$-module thanks to the map $\mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$. But if G is an $\mathcal{O}_Y$-module, f^*G is *not* an $\mathcal{O}_X$-module. We must augment the notion of inverse image. Our map $\varphi\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ corresponds by adjunction to a map $\widetilde{\varphi}\colon f^*\mathcal{O}_Y \to \mathcal{O}_X$. Now f^*G *is* an $f^*\mathcal{O}_Y$-module, so we form

$$(f,\varphi)^*G = \mathcal{O}_X \otimes_{f^*\mathcal{O}_Y} f^*G$$

and get our improved notion of inverse image—an $\mathcal{O}_X$-module.

Finally, to end this long section we give some results (of a very elementary character) concerning $\operatorname{Tor}^R_\bullet(-,-)$ and properties of special rings, R. The first of these works for every ring:

Proposition 5.41 *Say M is an R-module (resp. R^{op}-module), then the following are equivalent:*

(1) M is R-flat.

(2) For all Z, we have $\operatorname{Tor}^R_n(Z,M) = (0)$, for all $n > 0$.

(3) For all Z, we have $\operatorname{Tor}^R_1(Z,M) = (0)$.

Proof. (1) $\Longrightarrow$ (2). Since the functor $Z \rightsquigarrow Z \otimes_R M$ is exact, its derived functors are zero for $n > 0$, i.e., (2) holds.

(2) $\Longrightarrow$ (3). This is a tautology.

(3) $\Longrightarrow$ (1). Given an exact sequence

$$0 \longrightarrow Z' \longrightarrow Z \longrightarrow Z'' \longrightarrow 0$$

tensor with M and take cohomology. We get the following piece of the long exact sequence

$$\cdots \longrightarrow \operatorname{Tor}^R_1(Z'',M) \longrightarrow Z' \otimes_R M \longrightarrow Z \otimes_R M \longrightarrow Z'' \otimes_R M \longrightarrow 0.$$

By (3), we have $\operatorname{Tor}^R_1(Z'',M) = (0)$, so the tensored sequence is exact. □

For the rest, we'll assume R is a domain. Now for a P.I.D. we know divisibility of a module is the same as injectivity. That's not true in general, but we have

Proposition 5.42 *If R is an integral domain, every injective R-module is divisible. Conversely, if a module is divisible and torsion free it is injective.*

Proof. We use the exact sequence

$$0 \longrightarrow R \xrightarrow{r} R$$

(R is a domain) for a given element ($\neq 0$) of R. The functor $\operatorname{Hom}_R(-,Q)$ is exact as Q is injective. Then we get

$$Q = \operatorname{Hom}_R(R,Q) \xrightarrow{r} \operatorname{Hom}_R(R,Q) = Q \longrightarrow 0$$

is exact. As r is arbitrary, Q is divisible.

Next, assume M is a torsion-free, divisible module. For an exact sequence

$$0 \longrightarrow \mathfrak{A} \longrightarrow R,$$

suppose we have an R-module map $\varphi\colon \mathfrak{A} \to M$. We need only prove φ extends to a map $R \longrightarrow M$. Of course, this means we need to find $m \in M$, the image of 1 under our extension of φ, so that

$$(\forall r \in \mathfrak{A})(\varphi(r) = rm).$$

Now for each fixed $r \in \mathfrak{A}$, the divisibility of M shows there is an element, $m(r) \in M$, so that

$$\varphi(r) = r \cdot m(r).$$

This element of M is *uniquely* determined by r because M is torsion-free. Now pick $s \in \mathfrak{A}$, $s \neq 0$, consider sr. We have

$$\varphi(sr) = s\varphi(r) = srm(r).$$

But, $sr = rs$; so

$$\varphi(sr) = \varphi(rs) = r\varphi(s) = rsm(s).$$

By torsion freeness, again, we find $m(r) = m(s)$. So, all the elements $m(r)$ are the same, m; and we're done. □

Write $F = \mathrm{Frac}(R)$. The field F is a torsion-free divisible, R-module; it is therefore an injective R-module (in fact, it is the injective hull of R). The R-module, F/R, is an R-module of some importance. For example, $\mathrm{Hom}_R(F/R, M) = (0)$ provided M is torsion-free. In terms of F/R we have the

Corollary 5.43 *If M is a torsion-free module, then M is injective iff $\mathrm{Ext}^1_R(F/R, M) = (0)$. In particular, for torsion-free modules, M, the following are equivalent*

(1) M is injective

(2) $\mathrm{Ext}^n_R(F/R, M) = (0)$ all $n > 0$

(3) $\mathrm{Ext}^1_R(F/R, M) = (0)$.

Proof. Everything follows from the implication (3) $\Longrightarrow$ (1). For this, we have the exact sequence

$$0 \longrightarrow R \longrightarrow F \longrightarrow F/R \longrightarrow 0$$

and so (using $\mathrm{Hom}_R(F/R, M) = (0)$) we find

$$0 \longrightarrow \mathrm{Hom}_R(F, M) \xrightarrow{\theta} M \longrightarrow \mathrm{Ext}^1_R(F/R, M)$$

is exact. The map, θ, takes f to $f(1)$. By (3), θ is an isomorphism. Given $m \in M$ and $r \neq 0$ in R, there is some $f\colon F \to M$, with $f(1) = m$. Let $q = f(1/r)$, then

$$rq = rf(1/r) = f(1) = m;$$

so, M is divisible and Proposition 5.42 applies. □

The field F is easily seen to be $\varinjlim_{\lambda} (\frac{1}{\lambda}R)$, where we use the Artin ordering on R: $\lambda \leq \mu$ iff $\lambda \mid \mu$. Consequently, F is a right limit of projective (indeed, free of rank one) modules. Now tensor commutes with right limits, therefore so does $\mathrm{Tor}^R_\bullet$ (DX). This gives us

$$\mathrm{Tor}^R_n(F, M) = \varinjlim_{\lambda} \mathrm{Tor}^R_n\left(\frac{1}{\lambda}R, M\right) = (0), \quad \text{if } n > 0.$$

That is, F is a flat R-module. Moreover, we have

Proposition 5.44 *If R is an integral domain and M is any R-module, then $\mathrm{Tor}^R_1(F/R, M) = t(M)$, the torsion submodule of M. The R-modules $\mathrm{Tor}^R_p(F/R, M)$ vanish if $p \geq 2$.*

Proof. Use the exact sequence

$$0 \longrightarrow R \longrightarrow F \longrightarrow F/R \longrightarrow 0$$

and tensor with M. We get

$$0 \longrightarrow \mathrm{Tor}_1^R(F/R, M) \longrightarrow R \otimes_R M\,(= M) \longrightarrow F \otimes_R M \longrightarrow F/R \otimes_R M \longrightarrow 0$$

and, further back along the homology sequence

$$(0) = \mathrm{Tor}_{p+1}^R(F, M) \longrightarrow \mathrm{Tor}_{p+1}^R(F/R, M) \longrightarrow \mathrm{Tor}_p^R(R, M) = (0)$$

for all $p \geq 1$. Thus, all will be proved when we show

$$t(M) = \mathrm{Ker}\,(M \longrightarrow F \otimes_R M).$$

Since $F \otimes_R M = \varinjlim_{\lambda} (\frac{1}{\lambda}R \otimes_R M)$, we see $\xi \in \mathrm{Ker}\,(M \longrightarrow F \otimes_R M)$ iff there is some $\lambda\ (\neq 0)$ with $\xi \in \mathrm{Ker}\,(M \longrightarrow \frac{1}{\lambda}R \otimes_R M)$. But, R is a domain, so multiplication by λ is an isomorphism of $\frac{1}{\lambda}R$ and R. This gives us the commutative diagram

$$\begin{array}{ccc} M & \longrightarrow & \left(\frac{1}{\lambda}\right) R \otimes_R M \\ \Big\downarrow & & \Big\downarrow \text{mult. by } \lambda \\ M & = & R \otimes_R M \end{array}$$

and we see immediately that the left vectical arrow is also multiplication by λ. Hence $\xi \in \mathrm{Ker}\,(M \longrightarrow (\frac{1}{\lambda}R) \otimes_R M)$ when and only when $\lambda\xi = 0$, and we are done. □

The name and symbol for $\mathrm{Tor}_\bullet^R$ arose from this proposition.

When R is a P.I.D., the module, F/R, being divisible is injective. Consequently,

Proposition 5.45 *If R is a P.I.D., the sequence*

$$0 \longrightarrow R \longrightarrow F \longrightarrow F/R \longrightarrow 0$$

is an injective resolution of R. Hence, $\mathrm{Ext}_R^p(M, R) = (0)$ if $p \geq 2$, while

$$\mathrm{Ext}_R^1(M, R) = \mathrm{Coker}\,(\mathrm{Hom}_R(M, F) \longrightarrow \mathrm{Hom}_R(M, F/R)).$$

When M is a finitely generated R-module, we find

$$\mathrm{Ext}_R^1(M, R) = \mathrm{Hom}_R(t(M), F/R).$$

Proof. We know the exact sequence is an injective resolution of R and we use it to compute the Ext's. This gives all but the last statement. For that, observe that

$$0 \longrightarrow t(M) \longrightarrow M \longrightarrow M/t(M) \longrightarrow 0$$

is split exact because $M/t(M)$ is free when R is a P.I.D. and M is f.g. Now F is torsion free, so

$$\mathrm{Hom}_R(M, F) = F^\alpha, \quad \alpha = \mathrm{rank}\, M/t(M)$$

and

$$\mathrm{Hom}_R(M, F/R) = \mathrm{Hom}_R(t(M), F/R)\ \amalg\ (F/R)^\alpha.$$

Therefore, $\mathrm{Ext}_R^1(M, R)$ computed as the cokernel has the value claimed above. □

For torsion modules, M, the R-module $\mathrm{Hom}_R(M, F/R)$ is usually called the *dual of M* and its elements are *characters of M*. The notation for the dual of M is M^D. With this terminology, we obtain

Corollary 5.46 *Suppose R is a P.I.D. and M is a f.g. R-module. Then the equivalence classes of extensions of M by R are in 1–1 correspondence with the characters of the torsion submodule of M.*

5.4 Spectral Sequences; First Applications

The invariants provided by homological algebra are obtained from the computation of the (co)homology of a given complex. In general, this is not an easy task—we need all the help we can get. Experience shows that many complexes come with a natural filtration (for example, the complex of differential forms on a complex manifold with its Hodge filtration). In this case, if the filtration satisfies a few simple properties, we can go a long way toward computing (co)homology provided there is a suitable beginning provided for us.

So let $C^\bullet$ be a complex (say computing cohomology) and suppose $C^\bullet$ is filtered. This means there is a family of subobjects, $\{F^pC^\bullet\}_{p\in\mathbb{Z}}$, of $C^\bullet$ such that

$$\cdots \supseteq F^pC^\bullet \supseteq F^{p+1}C^\bullet \supseteq \cdots .$$

We also assume that $\bigcup_p F^pC^\bullet = C^\bullet$ and $\bigcap_p F^pC^\bullet = (0)$. Moreover, if d is the coboundary map of the complex $C^\bullet$ (also called *differentiation*), we assume that

(1) The filtration $\{F^pC^\bullet\}$ and d are compatible, which means that $d(F^pC^\bullet) \subseteq F^pC^\bullet$, for all p.

(2) The filtration $\{F^pC^\bullet\}$ is compatible with the grading on $C^\bullet$, i.e.,

$$F^pC^\bullet = \coprod_q F^pC^\bullet \cap C^{p+q} = \coprod_q C^{p,q},$$

where $C^{p,q} = F^pC^\bullet \cap C^{p+q}$. Then, each $F^pC^\bullet$ is itself a filtered graded complex as are the $F^pC^\bullet/F^{p+r}C^\bullet$, for all $r > 0$.

Remarks:

(1) We have $F^pC^\bullet = \coprod_q C^{p,q}$, the elements in $C^{p,q}$ have *degree* $p+q$.

(2) The $C^{p,q}$'s are subobjects of C^{p+q}.

(3) The $C^{p,q}$'s filter C^{p+q}, and p is the *index of filtration*.

Now, $C^\bullet$ possesses cohomology; $H^\bullet(C^\bullet)$. Also, $F^pC^\bullet$ possesses cohomology, $H^\bullet(F^pC^\bullet)$. There is a map of complexes $F^pC^\bullet \hookrightarrow C^\bullet$, so we have a map $H^\bullet(F^pC^\bullet) \longrightarrow H^\bullet(C^\bullet)$, the image is denoted $H^\bullet(C^\bullet)^p$ and the $H^\bullet(C^\bullet)^p$'s filter $H^\bullet(C^\bullet)$. So, $H^\bullet(C^\bullet)$ is graded and filtered. Thus, we can make

$$H(C)^{p,q} = H^\bullet(C^\bullet)^p \cap H^{p+q}(C^\bullet).$$

There is a graded complex, $\mathrm{gr}(C^\bullet)$, induced by F on $C^\bullet$, defined as

$$\mathrm{gr}(C^\bullet)^n = F^nC^\bullet/F^{n+1}C^\bullet.$$

So, we have $\mathrm{gr}(C^\bullet) = \coprod_n \mathrm{gr}(C^\bullet)^n$ and it follows that

$$\begin{aligned}
\mathrm{gr}(C^\bullet) &= \coprod_p (F^pC^\bullet/F^{p+1}C^\bullet) \\
&= \coprod_p \left[\left(\coprod_q F^pC^\bullet \cap C^{p+q} \right) \Big/ \left(\coprod_q F^{p+1}C^\bullet \cap C^{p+q} \right) \right] \\
&= \coprod_p \coprod_q (F^pC^\bullet \cap C^{p+q})/(F^{p+1}C^\bullet \cap C^{p+q}) \\
&= \coprod_{p,q} C^{p,q}/C^{p+1,q-1}.
\end{aligned}$$

So, we get

$$\mathrm{gr}(C^\bullet) = \coprod_{p,q} C^{p,q}/C^{p+1,q-1} = \coprod_{p,q} \mathrm{gr}(C)^{p,q},$$

with $\mathrm{gr}(C)^{p,q} = C^{p,q}/C^{p+1,q-1}$. Similarly, $H^\bullet(\mathrm{gr}(C^\bullet))$ is also bigraded; we have

$$H^\bullet(\mathrm{gr}(C^\bullet)) = \coprod_{p,q} H(\mathrm{gr}(C))^{p,q},$$

where $H(\mathrm{gr}(C))^{p,q} = H^{p+q}(F^pC^\bullet/F^{p+1}C^\bullet)$.

Finally, we also have the graded pieces of $H^{p+q}(C^\bullet)$ in its filtration,

$$\mathrm{gr}(H(C))^{p,q} = H(C)^{p,q}/H(C)^{p+1,q-1} = H^{p+q}(C^\bullet) \cap H^\bullet(C^\bullet)^p / H^{p+q}(C^\bullet) \cap H^\bullet(C^\bullet)^{p+1}.$$

As a naive example of a filtration, we have $F^pC^\bullet = \coprod_{n\geq p} C^n$.

The rest of this section is replete with indices—a veritable orgy of indices. *The definitions to remember are four*: $C^{p,q}$, $\mathrm{gr}(C)^{p,q}$, $H(\mathrm{gr}(C))^{p,q}$ *and* $\mathrm{gr}(H(C))^{p,q}$. Now $C^\bullet$ is filtered and it leads to the graded object $\mathrm{gr}(C^\bullet)$. One always considers $\mathrm{gr}(C^\bullet)$ as a "simpler" object than $C^\bullet$. Here's an example to keep in mind which demonstrates this idea of "simpler". Let C be the ring of power series in one variable, x, over some field, k. Convergence is irrelevant here, just use formal power series. Let F^pC be the collection of power series beginning with terms involving x^{p+1} or higher. We feel that in F^pC the term of a series involving x^{p+1} is the "dominating term", but there are all the rest of the terms. How to get rid of them? Simply pass to $F^pC/F^{p+1}C$, in this object only the term involving x^{p+1} survives. So $\mathrm{gr}(C)$ is the coproduct of the simplest objects: the single terms $a_{p+1}x^{p+1}$. It is manifestly simpler than C. Ideally, we would like to compute the cohomology, $H^\bullet(C^\bullet)$, of $C^\bullet$. However, experience shows that this is usually not feasible, but instead we can begin by computing $H^\bullet(\mathrm{gr}(C^\bullet))$ because $\mathrm{gr}(C^\bullet)$ is simpler than $C^\bullet$. Then, a spectral sequence is just the passage from $H^\bullet(\mathrm{gr}(C^\bullet))$ to $\mathrm{gr}(H^\bullet(C^\bullet))$; this is not quite $H^\bullet(C^\bullet)$ but is usually good enough.

The following assumption makes life easier in dealing with the convergence of spectral sequences: A filtration is *regular* iff for every $n \geq 0$, there is some $\mu(n) \geq 0$, so that for all $p > \mu(n)$, we have $F^pC^\bullet \cap C^n = (0)$.

Definition 5.10 A *cohomological spectral sequence* is a quintuple,

$$\mathcal{E} = \langle E_r^{p,q}, d_r^{p,q}, \alpha_r^{p,q}, E, \beta^{p,q} \rangle,$$

where

(1) $E_r^{p,q}$ is some object in $\mathcal{O}\mathrm{b}(\mathcal{A})$, with $p, q \geq 0$ and $2 \leq r \leq \infty$ (the subscript r is called the *level*).

(2) $d_r^{p,q}\colon E_r^{p,q} \to E_r^{p+r,q-r+1}$ is a morphism such that $d_r^{p,q} \circ d_r^{p-r,q+r-1} = 0$, for all $p, q \geq 0$ and all $r < \infty$.

(3) $\alpha_r^{p,q}\colon \mathrm{Ker}\ d_r^{p,q}/\mathrm{Im}\ d_r^{p-r,q+r-1} \to E_{r+1}^{p,q}$ is an isomorphism, for all p, q, all $r < \infty$.

(4) E is a graded, filtered object from $\mathcal{A}$, so that each F^pE is graded by the $E^{p,q} = F^pE \cap E^{p+q}$.

(5) $\beta^{p,q}\colon E_\infty^{p,q} \to \mathrm{gr}(E)^{p,q}$ is an isomorphism, for all p, q (where $\mathrm{gr}(E)^{p,q} = E^{p,q}/E^{p+1,q-1}$).

Remarks:

(1) The whole definition is written in the compact form

$$E_2^{p,q} \underset{p}{\Longrightarrow} E$$

and E is called the *end* of the spectral sequence. The index p is called the *filtration index*, $p + q$ is called the *total* or *grading index* and q the *complementary index*.

(2) If $r > q+1$, then Im $d_r^{p,q} = (0)$ and if $r > p$, then Im $d_r^{p-r,q+r-1} = (0)$. So, if $r > \max\{p, q+1\}$, then (3) implies that $E_r^{p,q} = E_{r+1}^{p,q}$, i.e., the sequence of $E_r^{p,q}$ stabilizes for $r >> 0$.

(3) In general, when $E_r^{p,q}$ stabilizes, $E_r^{p,q} \neq E_\infty^{p,q}$. Further assumptions must be made to get $E_r^{p,q} = E_\infty^{p,q}$ for $r >> 0$.

(4) It is customary to define spectral sequence beginning from $r = 2$, even though the terms $E_i^{p,q}$ are often defined and meaningful for $r = 1$, and even for $r = 0$. However, in the case of double complexes, the natural starting point is indeed $r = 2$, as pointed out in Cartan and Eilenberg [9] (Chapter XV, page 332).

(5) One can instead make the definition of a *homological spectral sequence* by passing to the "third quadrant" ($p \leq 0$ and $q \leq 0$) and changing arrows around after lowering indices in the usual way, *viz*: H^{-n} becomes H_n. Further, one can make 2^{nd} or 4^{th} quadrant spectral sequences or those creeping beyond the quadrant boundaries. All this will be left to the reader—the cohomological case will be quite enough for us.

Spectral sequences can be introduced in many ways. The one chosen here leads immediately into applications involving double complexes but is weaker if one passes to triangulated and derived categories. No mastery is possible except by learning the various methods together with their strengths and weaknesses. In the existence proof given below there are many complicated diagrams and indices. I urge you to read as far as the definition of $Z_r^{p,q}$ and $B_r^{p,q}$ (one–half page) and skip the rest of the proof on a first reading.

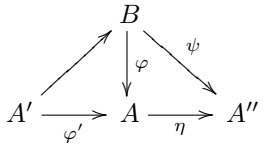
Theorem 5.47 *Say $C^\bullet$ is a filtered right complex whose filtration is compatible with its grading and differentiation. Then, $H^\bullet(C^\bullet)$ possesses a filtration (and is graded) and there exists a spectral sequence*

$$E_2^{p,q} \underset{p}{\Longrightarrow} H^\bullet(C^\bullet),$$

in which $E_2^{p,q}$ is the cohomology of $H^\bullet(\mathrm{gr}(C^\bullet))$—so that $E_1^{p,q} = H(\mathrm{gr}(C))^{p,q} = H^{p+q}(F^pC^\bullet/F^{p+1}C^\bullet))$. If the filtration is regular, the objects $E_\infty^{p,q}$ $(= \mathrm{gr}(H^\bullet(C^\bullet))^{p,q} = H(C)^{p,q}/H(C)^{p+1,q-1} =$ composition factors in the filtration of $H^{p+q}(C^\bullet))$ are exactly the $E_r^{p,q}$ when $r >> 0$.

In the course of the proof of Theorem 5.47, we shall make heavy use of the following simple lemma whose proof will be left as an exercise:

Lemma 5.48 *(Lemma (L)) Let*



be a commutative diagram with exact bottom row. Then, η induces an isomorphism Im φ/Im $\varphi' \xrightarrow{\sim}$ Im ψ.

Proof of Theorem 5.47. First, we need to make $Z_r^{p,q}$ and $B_r^{p,q}$ and set $E_r^{p,q} = Z_r^{p,q}/B_r^{p,q}$.

Consider the exact sequence (we will *drop the notation $C^\bullet$ in favor of C for clarity*)

$$0 \longrightarrow F^pC \longrightarrow F^{p-r+1}C \longrightarrow F^{p-r+1}C/F^pC \longrightarrow 0.$$

Upon applying cohomology, we obtain

$$\cdots \longrightarrow H^{p+q-1}(F^{p-r+1}C) \longrightarrow H^{p+q-1}(F^{p-r+1}C/F^pC) \xrightarrow{\delta^*} H^{p+q}(F^pC) \longrightarrow \cdots$$

There is also the natural map $H^{p+q}(F^pC) \longrightarrow H^{p+q}(F^pC/F^{p+1}C)$ induced by the projection $F^pC \longrightarrow F^pC/F^{p+1}C$. Moreover, we have the projection $F^pC/F^{p+r}C \longrightarrow F^pC/F^{p+1}C$, which induces a map on cohomology

$$H^{p+q}(F^pC/F^{p+r}C) \longrightarrow H^{p+q}(F^pC/F^{p+1}C).$$

Set

$$\begin{aligned} Z_r^{p,q} &= \mathrm{Im}\,(H^{p+q}(F^pC/F^{p+r}C) \longrightarrow H^{p+q}(F^pC/F^{p+1}C)) \\ B_r^{p,q} &= \mathrm{Im}\,(H^{p+q-1}(F^{p-r+1}C/F^pC) \longrightarrow H^{p+q}(F^pC/F^{p+1}C)), \end{aligned}$$

the latter map being the composition of δ^* and the projection (where $r \geq 1$).

The inclusion $F^{p-r+1}C \subseteq F^{p-r}C$ yields a map $F^{p-r+1}C/F^pC \longrightarrow F^{p-r}C/F^pC$; hence we obtain the inclusion relation $B_r^{p,q} \subseteq B_{r+1}^{p,q}$. In a similar way, the projection $F^pC/F^{p+r+1}C \longrightarrow F^pC/F^{p+r}C$ yields the inclusion $Z_{r+1}^{p,q} \subseteq Z_r^{p,q}$. When $r = \infty$, the coboundary map yields the inclusion $B_\infty^{p,q} \subseteq Z_\infty^{p,q}$ (remember, $F^\infty C = (0)$). Consequently, we can write

$$\cdots \subseteq B_r^{p,q} \subseteq B_{r+1}^{p,q} \subseteq \cdots \subseteq B_\infty^{p,q} \subseteq Z_\infty^{p,q} \subseteq \cdots \subseteq Z_{r+1}^{p,q} \subseteq Z_r^{p,q} \subseteq \cdots .$$

Set

$$E_r^{p,q} = Z_r^{p,q}/B_r^{p,q}, \quad \text{where } 1 \leq r \leq \infty, \text{ and } \quad E_n = H^n(C).$$

Then, $E = \coprod_n E_n = H(C)$, filtered by the $H(C)^p$'s, as explained earlier. When $r = 1$, $B_1^{p,q} = (0)$ and

$$Z_1^{p,q} = H^{p+q}(F^pC/F^{p+1}C);$$

We obtain $E_1^{p,q} = H^{p+q}(F^pC/F^{p+1}C) = H(\mathrm{gr}(C))^{p,q}$. On the other hand, when $r = \infty$ (remember, $F^{-\infty}C = C$), we get

$$\begin{aligned} Z_\infty^{p,q} &= \mathrm{Im}\,(H^{p+q}(F^pC) \longrightarrow H^{p+q}(F^pC/F^{p+1}C)) \\ B_\infty^{p,q} &= \mathrm{Im}\,(H^{p+q-1}(C/F^pC) \longrightarrow H^{p+q}(F^pC/F^{p+1}C)). \end{aligned}$$

Now the exact sequence $0 \longrightarrow F^pC/F^{p+1}C \longrightarrow C/F^{p+1}C \longrightarrow C/F^pC \longrightarrow 0$ yields the cohomology sequence

$$\cdots \longrightarrow H^{p+q-1}(C/F^pC) \xrightarrow{\delta^*} H^{p+q}(F^pC/F^{p+1}C) \longrightarrow H^{p+q}(C/F^{p+1}C) \longrightarrow \cdots$$

and the exact sequence $0 \longrightarrow F^pC \longrightarrow C \longrightarrow C/F^pC \longrightarrow 0$ gives rise to the connecting homomorphism $H^{p+q-1}(C/F^pC) \longrightarrow H^{p+q}(F^pC)$. Consequently, we obtain the commutative diagram (with exact bottom row)

$$\begin{array}{ccccc} & & H^{p+q}(F^pC) & & \\ & \nearrow & \downarrow & \searrow & \\ H^{p+q-1}(C/F^pC) & \longrightarrow & H^{p+q}(F^pC/F^{p+1}C) & \longrightarrow & H^{p+q}(C/F^{p+1}C) \end{array}$$

and Lemma (L) yields an isomorphism

$$\xi^{p,q}\colon E_\infty^{p,q} = Z_\infty^{p,q}/B_\infty^{p,q} \longrightarrow \mathrm{Im}\,(H^{p+q}(F^pC) \longrightarrow H^{p+q}(C/F^{p+1}C)).$$

But another application of Lemma (L) to the diagram

$$\begin{array}{ccccc} & & H^{p+q}(F^pC) & & \\ & \nearrow & \downarrow & \searrow & \\ H^{p+q}(F^{p+1}C) & \longrightarrow & H^{p+q}(C) & \longrightarrow & H^{p+q}(C/F^{p+1}C) \end{array}$$

gives us the isomorphism

$$\eta^{p,q}\colon \mathrm{gr}(H(C))^{p,q} \longrightarrow \mathrm{Im}\,(H^{p+q}(F^pC) \longrightarrow H^{p+q}(C/F^{p+1}C)).$$

Thus, $(\eta^{p,q})^{-1} \circ \xi^{p,q}$ is the isomorphism $\beta^{p,q}$ required by part (5) of Definition 5.10.

Only two things remain to be proven to complete the proof of Theorem 5.47. They are the verification of (2) and (3) of Definition 5.10, and the observation that $E_\infty^{p,q}$, as defined above, is the common value of the $E_r^{p,q}$ for $r >> 0$. The verification of (2) and (3) depends upon Lemma (L). Specifically, we have the two commutative diagrams (with obvious origins)

$$\begin{array}{ccccc} & & H^{p+q}(F^pC/F^{p+r}C) & & \\ & \nearrow & \downarrow & \searrow^{\theta} & \\ H^{p+q}(F^pC/F^{p+r+1}C) & \longrightarrow & H^{p+q}(F^pC/F^{p+1}C) & \xrightarrow[\delta^*]{} & H^{p+q+1}(F^{p+1}C/F^{p+r+1}C) \end{array}$$

and

$$\begin{array}{ccccc} & & H^{p+q}(F^pC/F^{p+r}C) & & \\ & \nearrow & \downarrow & \searrow^{\theta} & \\ H^{p+q}(F^{p+1}C/F^{p+r}C) & \xrightarrow[\delta^*]{} & H^{p+q+1}(F^{p+r}C/F^{p+r+1}C) & \longrightarrow & H^{p+q+1}(F^{p+1}C/F^{p+r+1}C). \end{array}$$

Here, the map θ is the composition

$$H^{p+q}(F^pC/F^{p+r}C) \longrightarrow H^{p+q+1}(F^{p+r}C) \longrightarrow H^{p+q+1}(F^{p+1}C/F^{p+r+1}C).$$

Now, Lemma (L) yields the following facts:

$$\begin{aligned} Z_r^{p,q}/Z_{r+1}^{p,q} &\xrightarrow{\sim} \mathrm{Im}\ \theta, \\ B_{r+1}^{p+r,q-r+1}/B_r^{p+r,q-r+1} &\xrightarrow{\sim} \mathrm{Im}\ \theta, \end{aligned}$$

that is,

$$\delta_r^{p,q}\colon Z_r^{p,q}/Z_{r+1}^{p,q} \xrightarrow{\sim} B_{r+1}^{p+r,q-r+1}/B_r^{p+r,q-r+1}.$$

As $B_r^{p,q} \subseteq Z_s^{p,q}$ for every r and s, there is a surjection

$$\pi_r^{p,q}\colon E_r^{p,q} \longrightarrow Z_r^{p,q}/Z_{r+1}^{p,q}$$

with kernel $Z_{r+1}^{p,q}/B_r^{p,q}$; and there exists an injection

$$\sigma_{r+1}^{p+r,q-r+1}\colon B_{r+1}^{p+r,q-r+1}/B_r^{p+r,q-r+1} \longrightarrow E_r^{p+r,q-r+1}.$$

The composition $\sigma_{r+1}^{p+r,q-r+1} \circ \delta_r^{p,q} \circ \pi_r^{p,q}$ is the map $d_r^{p,q}$ from $E_r^{p,q}$ to $E_r^{p+r,q-r+1}$ required by (2). Observe that,

$$\mathrm{Im}\ d_r^{p-r,q+r-1} = B_{r+1}^{p,q}/B_r^{p,q} \subseteq Z_{r+1}^{p,q}/B_r^{p,q} = \mathrm{Ker}\ d_r^{p,q};$$

hence

$$H(E_r^{p,q}) = \mathrm{Ker}\ d_r^{p,q}/\mathrm{Im}\ d_r^{p-r,q+r-1} \cong Z_{r+1}^{p,q}/B_{r+1}^{p,q} = E_{r+1}^{p,q},$$

as required by (3).

To prove that $E_\infty^{p,q}$ as defined above is the common value of $E_r^{p,q}$ for large enough r, we must make use of the regularity of our filtration. Consider then the commutative diagram

$$\begin{array}{ccccc} & & H^{p+q}(F^pC/F^{p+r}C) & & \\ & \nearrow & \downarrow & \searrow^{\lambda} & \\ H^{p+q}(F^pC) & \longrightarrow & H^{p+q}(F^pC/F^{p+1}C) & \longrightarrow & H^{p+q+1}(F^{p+1}C) \end{array}$$

where λ is the composition

$$H^{p+q}(F^pC/F^{p+r}C) \xrightarrow{\delta^*} H^{p+q+1}(F^{p+r}C) \longrightarrow H^{p+q+1}(F^{p+1}C).$$

By Lemma (L), we have $Z_r^{p,q}/Z_\infty^{p,q} \xrightarrow{\sim}$ Im λ. However, if $r > \mu(p+q+1) - p$, then δ^* is the zero map. This shows Im $\lambda = (0)$; hence, we have proven

$$Z_r^{p,q} = Z_\infty^{p,q} \quad \text{for } r > \mu(p+q+1) - p.$$

By our assumptions, the filtration begins with $C = F^0C$, therefore if $r > p$ we find $B_r^{p,q} = B_\infty^{p,q}$. Hence, for

$$r > \max\{p, \mu(p+q+1) - p\}$$

the $E_r^{p,q}$ equal $E_\infty^{p,q}$. □

Remark: Even if our filtration does not start at 0, we can still understand $E_\infty^{p,q}$ from the $E_r^{p,q}$ when the filtration is regular. To see this, note that since cohomology commutes with right limits, we have

$$\varinjlim_r B_r^{p,q} = B_\infty^{p,q},$$

and this implies $\bigcup_r B_r^{p,q} = B_\infty^{p,q}$. Hence, we obtain maps

$$E_r^{p,q} = Z_r^{p,q}/B_r^{p,q} \longrightarrow Z_s^{p,q}/B_s^{p,q} = E_s^{p,q}$$

for $s \geq r > \mu(p+q+1) - p$, and these maps are surjective. (The maps are in fact induced by the $d_r^{p-r,q+r-1}$'s because of the equality

$$E_r^{p,q}/\text{Im } d_r^{p-r,q+r-1} = (Z_r^{p,q}/B_r^{p,q})/(B_{r+1}^{p,q}/B_r^{p,q}) = E_{r+1}^{p,q}$$

for $r > \mu(p+q+1) - p$.) Obviously, the right limit of the surjective mapping family

$$E_r^{p,q} \longrightarrow E_{r+1}^{p,q} \longrightarrow \cdots \longrightarrow E_s^{p,q} \longrightarrow \cdots$$

is the group $Z_\infty^{p,q}/(\bigcup B_r^{p,q}) = E_\infty^{p,q}$; so, each element of $E_\infty^{p,q}$ arises from $E_r^{p,q}$ if $r >> 0$ (for fixed p, q). Regularity is therefore still an important condition for spectral sequences that are first and second quadrant or first and fourth quadrant.

It is not true in general that $Z_\infty^{p,q} = \bigcap_r Z_r^{p,q}$ or that $\varprojlim_r Z_r^{p,q} = Z_\infty^{p,q}$. In the first case, we have a *weakly convergent* spectral sequence. In the second case, we have a *strongly convergent* spectral sequence.

Remark: Let us keep up the convention of the above proof in which the complex C appears without the "dot". Then, by (5) of our theorem we find

$$E_\infty^{p,q} = (H^{p+q}(C) \cap H(C)^p)/(H^{p+q}(C) \cap H(C)^{p+1}),$$

so that, for $p+q=n$, *the* $E_\infty^{p,q} = E_\infty^{p,n-p}$ *are the composition factors in the filtration*

$$H^n(C) \supseteq H^n(C)^1 \supseteq H^n(C)^2 \supseteq \cdots \supseteq H^n(C)^\nu \supseteq \cdots .$$

To understand a spectral sequence, it is important to have in mind a pictorial representation of it in its entirety. We are to imagine an "apartment house"; on the r^{th} floor the apartments are labelled $E_r^{p,q}$ and a plan of the r^{th} floor is exactly the points of the pq-plane. The roof of the apartment building is the ∞-floor. In addition, there is the map $d_r^{p,q}$ on the r^{th} floor; it goes "over r and down $r-1$". Hence, a picture of the r^{th} floor is shown in Figure 5.1:

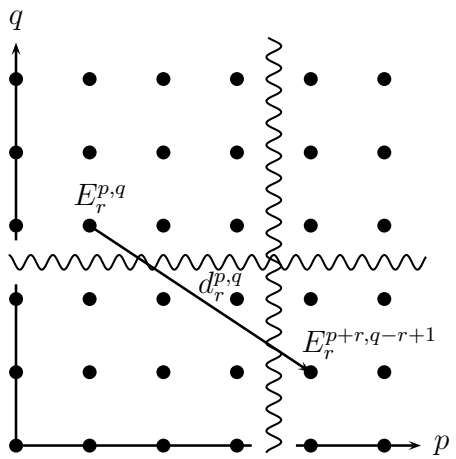


Figure 5.1: The $E_r^{p,q}$ terms of a spectral sequence ("r^{th} floor")

The entire edifice is depicted in Figure 5.2. One passes vertically directly to the apartment above by forming cohomology (with respect to d_r); so, one gets to the roof by repeated formings of cohomology at each higher level.

Once on the roof—at the ∞-level—the points on the line $p+q=n$, i.e., the groups $E_\infty^{0,n}, E_\infty^{1,n-1}, \ldots, E_\infty^{n,0}$, are the composition factors for the filtration of $H^n(C)$:

$$H^n(C) \supseteq H^n(C)^1 \supseteq H^n(C)^2 \supseteq \cdots \supseteq H^n(C)^n \supseteq (0);$$

See Figure 5.3.

To draw further conclusions in situations that occur in practice, we need three technical lemmas. Their proofs should be skipped on a first reading and they are only used to isolate and formalize conditions frequently met in the spectral sequences of applications. We'll label them Lemmas A, B, C as their conclusions are only used to get useful theorems on the sequences.

First, observe that if for some r, there are integers n and $p_1 > p_0$ so that $E_r^{\nu,n-\nu} = (0)$ whenever $\nu \neq p_0, \nu \neq p_1$, then certainly $E_s^{\nu,n-\nu} = (0)$ for every s with $r \leq s \leq \infty$. If the filtration is regular, then $E_\infty^{p_0,n-p_0}$ and $E_\infty^{p_1,n-p_1}$ are the only possible non-zero composition factors for $H^n(C)$ and therefore we obtain the exact sequence

$$0 \longrightarrow E_\infty^{p_1,n-p_1} \longrightarrow H^n(C) \longrightarrow E_\infty^{p_0,n-p_0} \longrightarrow 0. \qquad (\dagger)$$

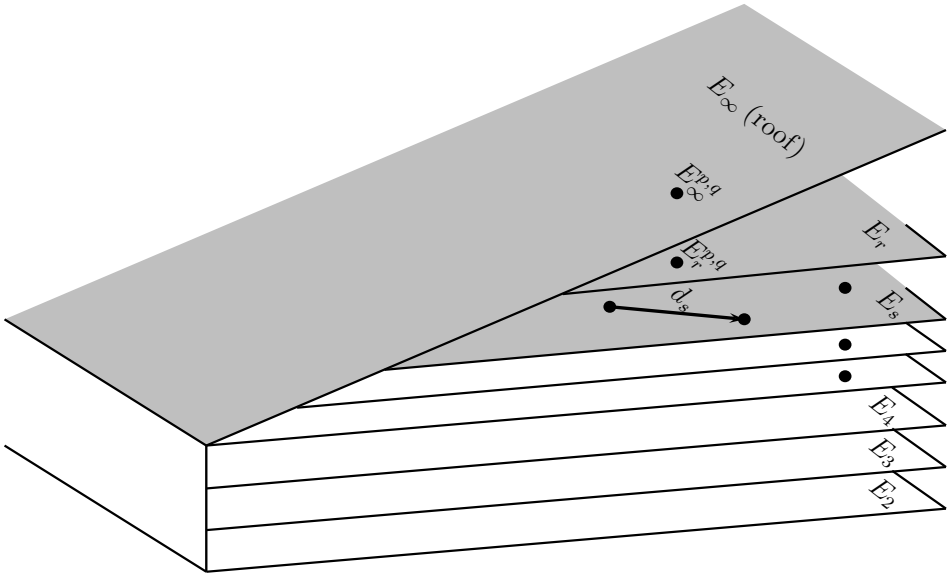


Figure 5.2: The entire spectral sequence (regular filtration)

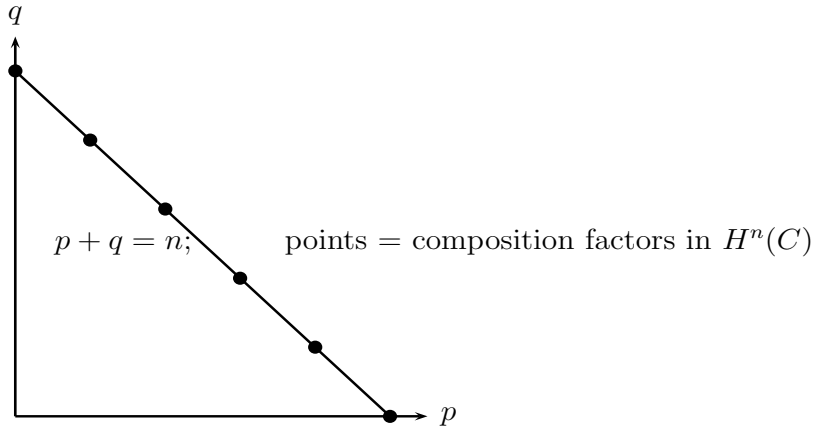


Figure 5.3: The $E_\infty^{p,q}$ terms of a spectral sequence ("roof level")

Lemma 5.49 *(Lemma A) Let $E_2^{p,q} \Longrightarrow H^\bullet(C)$ be a spectral sequence with a regular filtration. Assume there are integers $r; p_1 > p_0; n$ so that*

$$E_r^{u,v} = (0) \quad \textit{for} \quad \begin{cases} u+v = n, u \neq p_0, p_1 \\ u+v = n+1, u \geq p_1 + r \\ u+v = n-1, u \leq p_0 - r. \end{cases}$$

Then, there is an exact sequence

$$E_r^{p_1, n-p_1} \longrightarrow H^n(C) \longrightarrow E_r^{p_0, n-p_0}. \qquad (A)$$

Proof. The remarks above and the first hypothesis yield sequence (†). In the proof of Theorem 5.47, we saw that

$$\operatorname{Im} d_t^{p_0-t,n-p_0+t-1} = B_{t+1}^{p_0,n-p_0}/B_t^{p_0,n-p_0}.$$

We take $\infty > t \geq r$, let $u = p_0 - t$ and $v = n - p_0 + t - 1$. Using these u and v and the third hypothesis, we deduce $B_t^{p_0,n-p_0}$ is constant for $t \geq r$. Therefore, $B_\infty^{p_0,n-p_0} = B_r^{p_0,n-p_0}$. This gives an injection $E_\infty^{p_0,n-p_0} \hookrightarrow E_r^{p_0,n-p_0}$.

Next, with $u = p_1 + t; v = n - p_1 - t + 1$ and $\infty > t \geq r$, the second hypothesis shows that $\operatorname{Ker} d_t^{p_1+t,n-p_1-t+1} = (0)$ and the latter is $Z_{t+1}^{p_1+t,n-p_1-t+1}/B_t^{p_1+t,n-p_1-t+1}$. But,

$$B_r^{\bullet,\bullet} \subseteq B_t^{\bullet,\bullet} \subseteq B_\infty^{\bullet,\bullet} \subseteq Z_\infty^{\bullet,\bullet} \subseteq Z_{t+1}^{\bullet,\bullet},$$

and so we get

$$B_{t+1}^{p_1+t,n-p_1-t+1} = B_t^{p_1+t,n-p_1-t+1}, \quad \infty \geq t \geq r.$$

However, from the proof of Theorem 5.47, we find

$$Z_t^{p_1,n-p_1}/Z_{t+1}^{p_1,n-p_1} \simeq B_{t+1}^{p_1+t,n-p_1-t+1}/B_t^{p_1+t,n-p_1-t+1};$$

and therefore $Z_t^{p_1,n-p_1}$ is constant for $\infty > t \geq r$. By the regularity of the filtration, we find $Z_r^{p_1,n-p_1} = Z_\infty^{p_1,n-p_1}$. This gives a surjection $E_r^{p_1,n-p_1} \longrightarrow E_\infty^{p_1,n-p_1}$, and if we combine (†), our injection for $p_0, n-p_0$ and the surjection for $p_1, n-p_1$ we get sequence (A). □

Lemma 5.50 *(Lemma B) Suppose that $E_2^{p,q} \Longrightarrow H^\bullet(C)$ is a spectral sequence with a regular filtration. Assume that there are integers $s \geq r; p, n$ so that*

$$E_r^{u,v} = (0) \quad \textit{for} \quad \begin{cases} u+v = n-1, u \leq p-r \\ u+v = n, u \neq p \textit{ and } u \leq p+s-r \\ u+v = n+1, p+r \leq u \textit{ and } u \neq p+s. \end{cases}$$

Then, there is an exact sequence

$$H^n(C) \longrightarrow E_r^{p,n-p} \longrightarrow E_r^{p+s,(n+1)-(p+s)}. \tag{B}$$

Proof. We apply $d_r^{p,n-p}$ to $E_r^{p,n-p}$ and land in $E_r^{p+r,n-p-r+1}$ which is (0) by hypothesis three. Also, $E_r^{p-r,n-p+r-1}$ is (0) by the first hypothesis, so the image of $d_r^{p-r,n-p+r-1}$ is (0). This shows $E_r^{p,n-p} = E_{r+1}^{p,n-p}$. Repeat, but with d_{r+1}; as long as $r+1 < s$ we can continue using hypotheses one and three. Thus we obtain $E_r^{p,n-p} = E_s^{p,n-p}$. Now apply $d_t^{p,n-p}$ to $E_t^{p,n-p}$ where $t \geq s+1$. Hypothesis three shows our map is zero and similarly the map $d_t^{p-t,n-p+t-1}$ is zero by hypothesis one. So, for all t, with $\infty > t \geq s+1$, we get $E_t^{p,n-p} = E_{t+1}^{p,n-t}$. As the filtration is regular, we obtain $E_{s+1}^{p,n-p} = E_\infty^{p,n-p}$.

Next, by hypothesis two with $u = p + (s-r)$ (provided $s > r$, otherwise there is nothing to prove), we see that $\operatorname{Im} d_r^{p+s-r,n-(p+s-r)}$ is (0). Thus,

$$B_{r+1}^{p+s,(n+1)-(p+s)} = B_r^{p+s,(n+1)-(p+s)}.$$

Should $s > r+1$, we continue because

$$(0) = \operatorname{Im} d_{r+1}^{p+s-(r+1),n-(p+s-(r+1))}.$$

This gives

$$B_{r+2}^{p+s,(n+1)-(p+s)} = B_{r+1}^{p+s,(n+1)-(p+s)}.$$

Hence, we get

$$B_s^{p+s,(n+1)-(p+s)} = B_r^{p+s,(n+1)-(p+s)}$$

by repetition. Of course, this gives the *inclusion*

$$E_s^{p+s,(n+1)-(p+s)} \subseteq E_r^{p+s,(n+1)-(p+s)}.$$

Lastly, by hypothesis one, $E_r^{p-s,(n-1)-(p-s)} = (0)$; so, $E_t^{p-s,(n-1)-(p-s)} = (0)$ for every $t \geq r$. Take $t = s$, then $d_s^{p-s,(n-1)-(p-s)}$ vanishes, and in the usual way we get

$$B_{s+1}^{p,n-p} = B_s^{p,n-p}.$$

But then, we obtain an inclusion

$$E_{s+1}^{p,n-p} \hookrightarrow E_s^{p,n-p}.$$

However, the kernel of $d_s^{p,n-p}$ is $Z_{s+1}^{p,n-p}/B_s^{p,n-p} = E_{s+1}^{p,n-p}$; therefore we get the exact sequence

$$0 \longrightarrow E_{s+1}^{p,n-p} \longrightarrow E_s^{p,n-p} \xrightarrow{d_s^{p,n-p}} E_s^{p+s,(n+1)-(p+s)}.$$

And now we have a surjection $H^n(C) \longrightarrow E_\infty^{p,n-p}$ because $E_\infty^{u,n-u} = (0)$ when $u \leq p + s - r$ $(r \neq p)$ by hypothesis two. If we put all this together, we get sequence (B). □

In a similar manner (see the exercises) one proves

Lemma 5.51 *(Lemma C) If $E_2^{p,q} \Longrightarrow H^\bullet(C)$ is a spectral sequence with a regular filtration and if there exist integers $s \geq r; p, n$ so that*

$$E_r^{u,v} = (0) \quad \textit{for} \quad \begin{cases} u + v = n + 1, u \geq p + r \\ u + v = n, p + r - s \leq u \neq p \\ u + v = n - 1, p - s \neq u \leq p - r, \end{cases}$$

then, there is an exact sequence

$$E_r^{p-s,(n-1)-(p-s)} \longrightarrow E_r^{p,n-p} \longrightarrow H^n(C). \tag{C}$$

Although Lemmas A, B, C are (dull and) technical, they do emphasize one important point: *For any level r, if $E_r^{p,q}$ lies on the line $p + q = n$, then d_r takes it to a group on the line $p + q = n + 1$ and it receives a d_r from a group on the line $p + q = n - 1$.* From this we obtain immediately

Corollary 5.52 *(Corollary D) Say $E_2^{p,q} \Longrightarrow H^\bullet(C)$ is a regularly filtered spectral sequence and there are integers r, n so that*

$$E_r^{p,q} = (0) \quad \textit{for} \quad \begin{cases} p + q = n - 1 \\ p + q = n + 1. \end{cases}$$

Then, $E_r^{p,n-p} = E_\infty^{p,n-p}$ and the $E_r^{p,n-p}$ are the composition factors for $H^n(C)$ in its filtration.

Now we wish to apply Lemmas A, B, C and we begin with the simplest case—a case for which we do not need these Lemmas. A spectral sequence $E_2^{p,q} \Longrightarrow H^\bullet(C)$ *degenerates at (level) r* when and only when for each n there is a $q(n)$ so that

$$E_r^{n-q,q} = (0) \quad \text{if } q \neq q(n).$$

Of course then $E_s^{n-q,q} = (0)$ when $q \neq q(n)$ for all $s \geq r$; so that, in the regular case, we have $E_\infty^{n-q,q} = (0)$ if $q \neq q(n)$. If we have $q(n + 1) > q(n) - (r - 1)$ for all n (e.g., if $q(n)$ is constant), then $E_r^{n-q,q} = E_\infty^{n-q,q}$ for every n and q and we deduce that

$$H^n(C) = E_\infty^{n-q(n),q(n)} = E_r^{n-q(n),q(n)}$$

for all n. This proves

Proposition 5.53 *When the filtration of C is regular and the spectral sequence*

$$E_2^{p,q} \Longrightarrow H^\bullet(C)$$

degenerates at r, then $H^n(C) = E_\infty^{n-q(n),q(n)}$. If in addition, $q(n+1) > q(n) - (r-1)$ for all n, then

$$H^n(C) \cong E_r^{n-q(n),q(n)}$$

for every n.

Theorem 5.54 *(Zipper Sequence) Suppose $E_2^{p,q} \Longrightarrow H^\bullet(C)$ is a regularly convergent spectral sequence and there exist integers p_0, p_1, r with $p_1 - p_0 \geq r \geq 1$ so that $E_r^{u,v} = (0)$ for all $u \neq p_0$ or p_1. Then we have the exact zipper sequence*

$$\cdots \longrightarrow E_r^{p_1,n-p_1} \longrightarrow H^n(C) \longrightarrow E_r^{p_0,n-p_0} \longrightarrow E_r^{p_1,n+1-p_1} \longrightarrow H^{n+1}(C) \longrightarrow \cdots$$

Dually, if there are integers q_0, q_1, r with $q_1 - q_0 \geq r - 1 \geq 1$ so that $E_r^{u,v} = (0)$ for $v \neq q_0$ or q_1, then the zipper sequence is

$$\cdots \longrightarrow E_r^{n-q_0,q_0} \longrightarrow H^n(C) \longrightarrow E_r^{n-q_1,q_1} \longrightarrow E_r^{n+1-q_0,q_0} \longrightarrow H^{n+1}(C) \longrightarrow \cdots$$

Proof. Write $s = p_1 - p_0 \geq r$ and apply Lemmas A, B and C (check the hypotheses using $u + v = n$). By splicing the exact sequences of those lemmas, we obtain the zipper sequence. Dually, write $s = 1 + q_1 - q_0 \geq r$, set $p_0 = n - q_1$ and $p_1 = n - q_0$. Then Lemmas A, B and C again apply and their exact sequences splice to give the zipper sequence. □

The name "zipper sequence" comes from the following picture. In it, the dark arrows are the maps $E_r^{p_0,n-p_0} \longrightarrow E_r^{p_1,n+1-p_1}$ and the dotted arrows are the compositions $E_r^{p_1,n+1-p_1} \longrightarrow H^{n+1} \longrightarrow E_r^{p_0,n+1-p_0}$ (one is to imagine these arrows passing through the H^{n+1} somewhere behind the plane of the page). As you see, the arrows zip together the vertical lines $p = p_0$ and $p = p_1$.

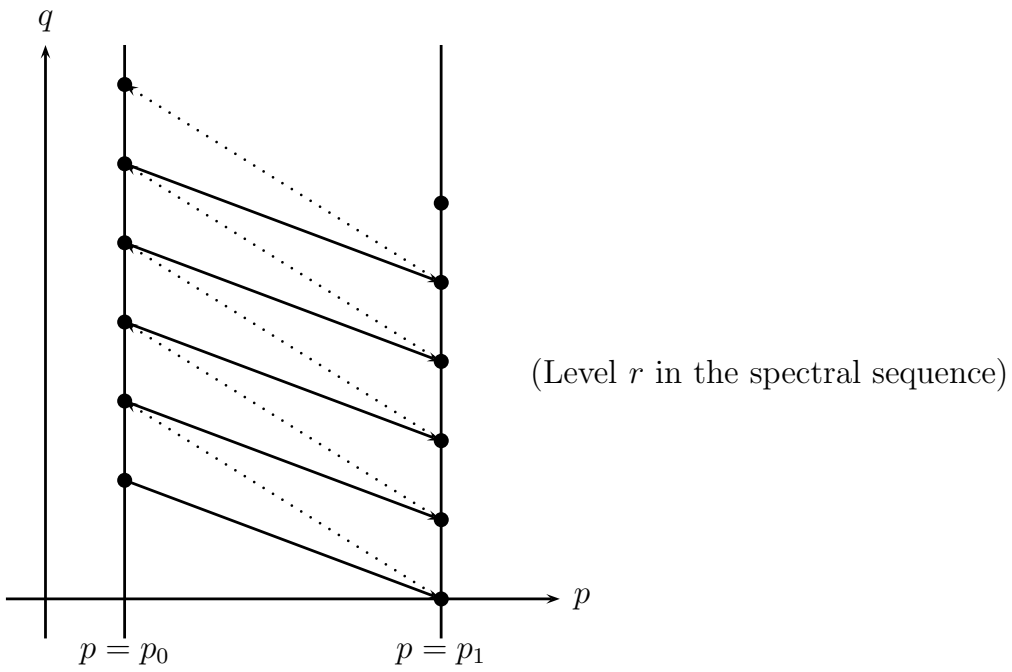


Figure 5.4: Zipper Sequence

Theorem 5.55 *(Edge Sequence) Suppose that $E_2^{p,q} \Longrightarrow H^\bullet(C)$ is a regularly convergent spectral sequence and assume there is an integer $n \geq 1$ so that $E_2^{p,q} = (0)$ for every q with $0 < q < n$ and all p (no hypothesis if $n = 1$). Then $E_2^{r,0} \cong H^r(C)$ for $r = 0, 1, 2, \ldots, n-1$ and*

$$0 \longrightarrow E_2^{n,0} \longrightarrow H^n(C) \longrightarrow E_2^{0,n} \longrightarrow E_2^{n+1,0} \longrightarrow H^{n+1}(C)$$

is exact (edge sequence). In particular, with no hypotheses on the vanishing of $E_2^{p,q}$, we have the exact sequence

$$0 \longrightarrow E_2^{1,0} \longrightarrow H^1(C) \longrightarrow E_2^{0,1} \xrightarrow{d_2^{0,1}} E_2^{2,0} \longrightarrow H^2(C).$$

Proof. Since we have a cohomological (first quadrant) spectral sequence all the differentials $d_l^{r,0}$ vanish for all l and if $l \geq n$ no differential $d_l^{p,q}$ hits $E_l^{r,0}$ if $p \geq 0$ and $r \leq n-1$. All the differentials $d_l^{p,q}$ are 0 if $q < n$ and so we find $E_2^{r,0} \cong E_\infty^{r,0}$ for $0 \leq r \leq n-1$. But, only one non-zero term $E_\infty^{p,q}$ exists on the line $r = p + q$ for $r < n$ by our hypothesis on the vanishing; so, indeed $E_2^{r,0} \cong E_\infty^{r,0} = H^r(C)$ when $0 \leq r \leq n-1$.

For $E_l^{n,0}$, since $d_{n-p}^{p,n-p-1} \colon E_{n-p}^{p,n-p-1} \to E_{n-p}^{n,0}$, and since $p \geq 0$ implies $q \leq n-1$, we see that no non-zero differential hits $E_l^{n,0}$ for any l. Thus, $E_2^{n,0} \cong E_\infty^{n,0}$ and we get the injection $E_2^{n,0} \longrightarrow H^n(C)$. Apply Lemma A with $p_0 = 0, p_1 = n, r = 2$ to find the sequence

$$0 \longrightarrow E_2^{n,0} \longrightarrow H^n(C) \longrightarrow E_2^{0,n}. \qquad (*)$$

Next, in Lemma B, take $r = 2, s = n+1 \geq 2$, and $p = 0$. Sequence (B) splices to $(*)$ to yield

$$0 \longrightarrow E_2^{n,0} \longrightarrow H^n(C) \longrightarrow E_2^{0,n} \longrightarrow E_2^{n+1,0}. \qquad (**)$$

And, lastly, use Lemma C with $r = 2, s = n+1 \geq 2$, the n of Lemma C to be our $n+1 = s$ and $p = n+1$. Upon splicing Lemma C onto $(**)$ we find the edge sequence

$$0 \longrightarrow E_2^{n,0} \longrightarrow H^n(C) \longrightarrow E_2^{0,n} \longrightarrow E_2^{n+1,0} \longrightarrow H^{n+1}(C). \qquad \square$$

Obviously, the edge sequence gets its name from the fact that the $E_2^{p,q}$ which appear in it lie on the edge of the quadrant in the picture of E_2 as points (of the first quadrant) in the pq-plane. Equally obvious is the notion of a *morphism of spectral sequences*. Whenever C and $\widetilde{C}$ are graded, filtered complexes and $g \colon C \to \widetilde{C}$ is a morphism of such complexes, we find an induced morphism

$$\mathrm{ss}(g) \colon E_2^{p,q} \Longrightarrow H^\bullet(C) \mapsto \widetilde{E}_2^{p,q} \Longrightarrow H^\bullet(\widetilde{C})$$

of spectral sequences.

Theorem 5.56 *Suppose C and $\widetilde{C}$ are graded filtered complexes and write $E^{\bullet,\bullet}(C)$ and $E^{\bullet,\bullet}(\widetilde{C})$ for their associated spectral sequences. Assume both filtrations are regular and $g^\bullet \colon E^{\bullet,\bullet}(C) \to E^{\bullet,\bullet}(\widetilde{C})$ is a spectral sequence morphism. If, for some $r \geq 2$, the level r map $g_r^\bullet \colon E_r^{\bullet,\bullet} \to \widetilde{E}_r^{\bullet,\bullet}$ is an isomorphism, then for every $s \geq r$ the level s map, $g_s^\bullet$, is also an isomorphism (also for $s = \infty$) and we have an induced isomorphism on the graded cohomology*

$$\mathrm{gr}H(g^\bullet) \colon \mathrm{gr}H^\bullet(C) \xrightarrow{\sim} \mathrm{gr}H^\bullet(\widetilde{C}).$$

Proof. The proof of this is obvious because by regularity $E_\infty^{p,q} = E_s^{p,q}$ for $s >> 0$. But for H^n, its graded pieces are the $E_\infty^{p,n-p}$, and $p \geq 0$. Thus, $p \leq n$ and $q \leq n$; so, our choice $s = s(n) >> 0$ will do to get

$$E_s^{p,q} = E_\infty^{p,q} \qquad (\text{all } p, q \text{ with } p + q = n).$$

These groups are exactly the graded pieces of H^n as we've remarked and $\coprod_{p+q=n} g_s^{p,q}$ is our isomorphism. $\square$

Our technical results on spectral sequences are over, now we actually need some spectral sequences to use them on. Big sources of spectral sequences are double complexes. So, let $C = \coprod_{p,q} C^{p,q}$ be a doubly-graded complex (we assume that $p, q \geq 0$). We have two differentiations:

$$\begin{aligned} d_{\mathrm{I}}^{p,q} &: C^{p,q} \longrightarrow C^{p+1,q}, \qquad \text{(horizontal)} \\ d_{\mathrm{II}}^{p,q} &: C^{p,q} \longrightarrow C^{p,q+1} \qquad \text{(vertical)} \end{aligned}$$

such that

$$d_{\mathrm{I}} \circ d_{\mathrm{I}} = d_{\mathrm{II}} \circ d_{\mathrm{II}} = 0.$$

We will require

$$d_{\mathrm{II}}^{p+1,q} \circ d_{\mathrm{I}}^{p,q} + d_{\mathrm{I}}^{p,q+1} \circ d_{\mathrm{II}}^{p,q} = 0, \quad \textit{for all } p, q.$$

Then we get the (singly graded) *total complex*

$$C = \coprod_n \left(\coprod_{p+q=n} C^{p,q} \right)$$

with *total differential* $d_T = d_{\mathrm{I}} + d_{\mathrm{II}}$. We immediately check that $d_T \circ d_T = 0$. There are two filtrations

$$F_{\mathrm{I}}^p C = \coprod_{r \geq p,q} C^{r,q} \quad \text{and} \quad F_{\mathrm{II}}^q C = \coprod_{p,s \geq q} C^{p,s}.$$

Both have every compatibility necessary and give filtrations on the total complex and are regular. Therefore, we find two spectral sequences

$$\mathrm{I}_2^{p,q} \underset{p}{\Longrightarrow} H^\bullet(C) \quad \text{and} \quad \mathrm{II}_2^{p,q} \underset{q}{\Longrightarrow} H^\bullet(C).$$

Observe that

$$\begin{aligned} \mathrm{gr}_{\mathrm{I}}(C) &= \coprod \mathrm{gr}_{\mathrm{I}}^p(C) \\ &= \coprod (F_{\mathrm{I}}^p C / F_{\mathrm{I}}^{p+1} C) \\ &= \coprod_p \left(\coprod_q C^{p,q} \right) \end{aligned}$$

and $E_{\mathrm{I}}^{p,q} = H^{p,q}(\mathrm{gr}_{\mathrm{I}}^p(C))$, which is just $H_{\mathrm{II}}^{p,q}(C)$. Now, we need to compute $d_1^{p,q}$ in spectral sequence (I). It is induced by the connecting homomorphism arising from the short exact sequence

$$0 \longrightarrow F_{\mathrm{I}}^{p+1} C / F_{\mathrm{I}}^{p+2} C \longrightarrow F_{\mathrm{I}}^p C / F_{\mathrm{I}}^{p+2} C \longrightarrow F_{\mathrm{I}}^p C / F_{\mathrm{I}}^{p+1} C \longrightarrow 0.$$

Pick $\xi \in H_{\mathrm{II}}^{p,q}(C)$, represented by a cocycle with respect to d_{II} in C^{p+q}, call it x. The connecting homomorphism ($= d_1$) is given by "$d_T x$". But, $d_T x = d_{\mathrm{I}} x + d_{\mathrm{II}} x = d_{\mathrm{I}} x$, as $d_{\mathrm{II}} x = 0$. Therefore, d_1 is exactly the map induced on $H_{\mathrm{II}}^{p,q}(C)$ by d_{I}. It follows that

$$\mathrm{I}_2^{p,q} = Z_2^{p,q} / B_2^{p,q} = H_{\mathrm{I}}^p(H_{\mathrm{II}}^q(C)).$$

We have therefore proved

Theorem 5.57 *Given a double complex $C = \coprod_{p,q} C^{p,q}$, we have two regular spectral sequences converging to the cohomology of the associated total complex:*

$$H_{\mathrm{I}}^p(H_{\mathrm{II}}^q(C)) \underset{p}{\Longrightarrow} H^\bullet(C)$$

and

$$H_{\mathrm{II}}^q(H_{\mathrm{I}}^p(C)) \underset{q}{\Longrightarrow} H^\bullet(C).$$

It still is not apparent where we'll find an ample supply of double complexes so as to use the above theorem. A very common source appears as the answer to the following

Problem. Given two left-exact functors $F\colon \mathcal{A} \to \mathcal{B}$ and $G\colon \mathcal{B} \to \mathcal{C}$ between abelian categories (with enough injectives, etc.), we have $GF\colon \mathcal{A} \to \mathcal{C}$ (left-exact); how can we compute $R^n(GF)$ if we know R^pF and R^qG?

In order to answer this question, we need to introduce special kinds of injective resolutions of complexes.

Definition 5.11 A *Cartan–Eilenberg injective resolution* of a complex, C, (with $C^k = (0)$ if $k < 0$) is a resolution

$$0 \longrightarrow C^\bullet \longrightarrow Q^{\bullet\,0} \longrightarrow Q^{\bullet\,1} \longrightarrow Q^{\bullet\,2} \longrightarrow \cdots,$$

in which each $Q^{\bullet\,j} = \coprod_i Q^{i,j}$ is a complex (differential d^{ij}) and every $Q^{i,j}$ injective and so that if we write $Z^{i,j} = \operatorname{Ker} d^{i,j}$; $B^{i,j} = \operatorname{Im} d^{i-1,j}$ and $H^{i,j} = Z^{i,j}/B^{i,j}$, we have the injective resolutions

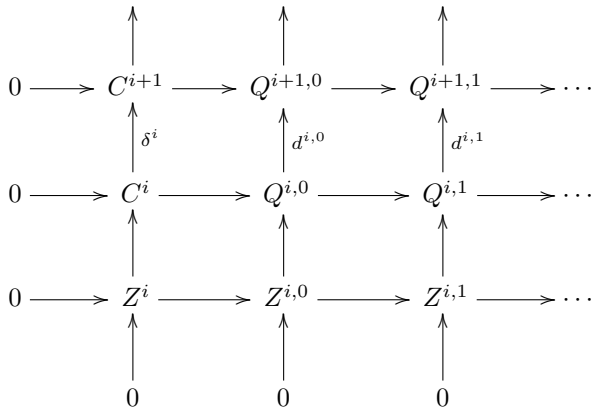
$$(1) \qquad 0 \longrightarrow C^i \longrightarrow Q^{i,0} \longrightarrow Q^{i,1} \longrightarrow \cdots$$

$$(2) \qquad 0 \longrightarrow Z^i(C) \longrightarrow Z^{i,0} \longrightarrow Z^{i,1} \longrightarrow \cdots$$

$$(3) \qquad 0 \longrightarrow B^i(C) \longrightarrow B^{i,0} \longrightarrow B^{i,1} \longrightarrow \cdots$$

$$(4) \qquad 0 \longrightarrow H^i(C) \longrightarrow H^{i,0} \longrightarrow H^{i,1} \longrightarrow \cdots.$$

The way to remember this complicated definition is through the following diagram:



Proposition 5.58 *Every complex, C, has a Cartan–Eilenberg resolution, $0 \longrightarrow C \longrightarrow Q^\bullet$, where the $\{Q^{i,j}\}$ form a double complex. Here, we have suppressed the grading indices of C and the Q^j.*

Proof. We begin with injective resolutions $0 \longrightarrow B^0(C) \longrightarrow B^{0,\bullet}$; $0 \longrightarrow B^1(C) \longrightarrow B^{1,\bullet}$ and $0 \longrightarrow H^0(C) \longrightarrow H^{0,\bullet}$ of $B^0(C)$; $B^1(C)$; $H^0(C)$. Now, we have exact sequences

$$0 \longrightarrow B^0(C) \longrightarrow Z^0(C) \longrightarrow H^0(C) \longrightarrow 0$$

and

$$0 \longrightarrow Z^0(C) \longrightarrow C^0 \xrightarrow{\delta^0} B^1(C) \longrightarrow 0;$$

so, by Proposition 5.1, we get injective resolutions $0 \longrightarrow Z^0(C) \longrightarrow Z^{0,\bullet}$ and $0 \longrightarrow C^0 \longrightarrow Q^{0,\bullet}$, so that

$$0 \longrightarrow B^{0,\bullet} \longrightarrow Z^{0,\bullet} \longrightarrow H^{0,\bullet} \longrightarrow 0$$

and

$$0 \longrightarrow Z^{0,\bullet} \longrightarrow Q^{0,\bullet} \longrightarrow B^{1,\bullet} \longrightarrow 0$$

are exact.

For the induction step, assume that the complexes $B^{i-1,\bullet}$, $Z^{i-1,\bullet}$, $H^{i-1,\bullet}$, $Q^{i-1,\bullet}$ and $B^{i,\bullet}$ are determined and satisfy the required exactness properties ($i \geq 1$). Pick any injective resolution $H^{i,\bullet}$ of $H^i(C)$, then using the exact sequence

$$0 \longrightarrow B^i(C) \longrightarrow Z^i(C) \longrightarrow H^i(C) \longrightarrow 0$$

and Proposition 5.1, we get an injective resolution $0 \longrightarrow Z^i(C) \longrightarrow Z^{i,\bullet}$ so that

$$0 \longrightarrow B^{i,\bullet} \longrightarrow Z^{i,\bullet} \longrightarrow H^{i,\bullet} \longrightarrow 0$$

is exact. Next, pick an injective resolution, $0 \longrightarrow B^{i+1}(C) \longrightarrow B^{i+1,\bullet}$, of $B^{i+1}(C)$ and use the exact sequence

$$0 \longrightarrow Z^i(C) \longrightarrow C^i \xrightarrow{\delta^i} B^{i+1}(C) \longrightarrow 0$$

and Proposition 5.1 to get an injective resolution $0 \longrightarrow C^i \longrightarrow Q^{i,\bullet}$ so that

$$0 \longrightarrow Z^{i,\bullet} \longrightarrow Q^{i,\bullet} \longrightarrow B^{i+1,\bullet} \longrightarrow 0$$

is exact. The differential $d_{\mathrm{II}}^{i,j}$ of the double complex $\{Q^{i,j}\}$ is the composition

$$Q^{i,j} \longrightarrow B^{i+1,j} \longrightarrow Z^{i+1,j} \longrightarrow Q^{i+1,j}$$

and the differential $d_{\mathrm{I}}^{i,j}$ is given by

$$d_{\mathrm{I}}^{i,j} = (-1)^i \epsilon^{i,j},$$

where, $\epsilon^{i,\bullet}$ is the differential of $Q^{i,\bullet}$. The reader should check that $\{Q^{i,j}\}$ is indeed a Cartan–Eilenberg resolution and a double complex (DX). □

Note that, due to the exigencies of notation (we resolved our complex $C^\bullet$ horizontally) the usual conventions of horizontal and vertical were interchanged in the proof of Proposition 5.58 at least as far as Cartesian coordinate notation is concerned. This will be rectified during the proof of the next theorem, which is the result about spectral sequences having the greatest number of obvious applications and forms the solution to the problem posed before.

Theorem 5.1 *(Grothendieck) Let $F\colon \mathcal{A} \to \mathcal{B}$ and $G\colon \mathcal{B} \to \mathcal{C}$ be two left-exact functors between abelian categories (with enough injectives, etc.) and suppose that $F(Q)$ is G-acyclic whenever Q is injective, which means that $R^pG(FQ) = (0)$, if $p > 0$. Then, we have the spectral sequence of composed functors*

$$R^qG((R^pF)(A)) \underset{q}{\Longrightarrow} (R^\bullet(GF))(A).$$

Proof. Pick some object $A \in \mathcal{A}$ and resolve it by injectives to obtain the resolution $0 \longrightarrow A \longrightarrow Q^\bullet(A)$:

$$0 \longrightarrow A \longrightarrow Q^0 \longrightarrow Q^1 \longrightarrow Q^2 \longrightarrow \cdots.$$

If we apply GF to $Q^\bullet(A)$ and compute cohomology, we get $R^n(GF)(A)$. If we just apply F to $Q^\bullet(A)$, we get the complex:

$$F(Q^0) \longrightarrow F(Q^1) \longrightarrow F(Q^2) \longrightarrow \cdots, \qquad (FQ^\bullet(A))$$

whose cohomology is $R^qF(A)$.

Now resolve the complex $FQ^\bullet(A)$ in the vertical direction by a Cartan-Eilenberg resolution. There results a double complex of injectives (with exact columns)

$$\begin{array}{ccccccc}
\vdots & & \vdots & & \vdots & & \\
\uparrow & & \uparrow & & \uparrow & & \\
Q^{0,1} & \longrightarrow & Q^{1,1} & \longrightarrow \cdots \longrightarrow & Q^{n,1} & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
Q^{0,0} & \longrightarrow & Q^{1,0} & \longrightarrow \cdots \longrightarrow & Q^{n,0} & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
F(Q^0) & \longrightarrow & F(Q^1) & \longrightarrow \cdots \longrightarrow & F(Q^n) & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
0 & & 0 & & 0 & &
\end{array}$$

in the category $\mathcal{B}$. Apply the functor G to this double complex to obtain a new double complex we will label C:

$$\begin{array}{ccccccc}
\vdots & & \vdots & & \vdots & & \\
\uparrow & & \uparrow & & \uparrow & & \\
G(Q^{0,1}) & \longrightarrow & G(Q^{1,1}) & \longrightarrow \cdots \longrightarrow & G(Q^{n,1}) & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
G(Q^{0,0}) & \longrightarrow & G(Q^{1,0}) & \longrightarrow \cdots \longrightarrow & G(Q^{n,0}) & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
GF(Q^0) & \longrightarrow & GF(Q^1) & \longrightarrow \cdots \longrightarrow & GF(Q^n) & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
0 & & 0 & & 0 & &
\end{array} \quad , \tag{C}$$

in which, by hypothesis, *all the columns are still exact*. Therefore, using the notations for the two spectral sequences converging to $H^\bullet(C)$, we have $H^\bullet_{\mathrm{II}}(C) = (0)$ so that (by our first remarks)

$$H^\bullet(C) \cong R^\bullet(GF)(A).$$

From the second spectral sequence, we get

$$\mathrm{II}_2^{l,m} = H^l_{\mathrm{II}}(H^m_{\mathrm{I}}(C)) \underset{l}{\Longrightarrow} R^\bullet(GF)(A).$$

Since we used a Cartan-Eilenberg resolution of $FQ^\bullet(A)$, we have the following injective resolutions

$$\begin{array}{rcl}
0 & \longrightarrow & Z^p(FQ^\bullet(A)) \longrightarrow Z^{p,0} \longrightarrow Z^{p,1} \longrightarrow \cdots \\
0 & \longrightarrow & B^p(FQ^\bullet(A)) \longrightarrow B^{p,0} \longrightarrow B^{p,1} \longrightarrow \cdots \\
0 & \longrightarrow & H^p(FQ^\bullet(A)) \longrightarrow H^{p,0} \longrightarrow H^{p,1} \longrightarrow \cdots ,
\end{array}$$

for all $p \geq 0$. Moreover, the exact sequences

$$0 \longrightarrow Z^{p,\bullet} \longrightarrow Q^{p,\bullet} \longrightarrow B^{p+1,\bullet} \longrightarrow 0$$

and

$$0 \longrightarrow B^{p,\bullet} \longrightarrow Z^{p,\bullet} \longrightarrow H^{p,\bullet} \longrightarrow 0$$

are split because the terms are injectives of $\mathcal{B}$. Therefore, the sequences

$$0 \longrightarrow G(Z^{p,\bullet}) \longrightarrow G(Q^{p,\bullet}) \longrightarrow G(B^{p+1,\bullet}) \longrightarrow 0$$

and

$$0 \longrightarrow G(B^{p,\bullet}) \longrightarrow G(Z^{p,\bullet}) \longrightarrow G(H^{p,\bullet}) \longrightarrow 0$$

are still exact and we find

$$H^p_{\mathrm{I}}(C^{\bullet,q}) = G(H^{p,q}).$$

But, the $H^{p,\bullet}$ form an injective resolution of $H^p(FQ^\bullet(A))$ and the latter is just $R^pF(A)$. So, $G(H^{p,\bullet})$ is the complex whose cohomology is exactly $R^qG(R^pF(A))$. Now, this cohomology is $H^q_{\mathrm{II}}(G(H^{p,\bullet}))$ and $H^p_{\mathrm{I}}(C^{\bullet,\bullet})$ is $G(H^{p,\bullet})$ by the above. We obtain

$$R^qG(R^pF(A)) = H^q_{\mathrm{II}}(H^p_{\mathrm{I}}(C^{\bullet,\bullet})) = \mathrm{II}_2^{q,p} \underset{q}{\Longrightarrow} H^\bullet(C).$$

Since $H^\bullet(C) \cong R^\bullet(GF)(A)$, we are done. □

There are many applications of the Spectral Sequence of Composed Functors. We give just a few of these.

(I) The Hochschild-Serre Spectral Sequence for the Cohomology of Groups

Write G for a (topological) group, N for a (closed) normal subgroup and A for a (continuous) G-module. (Our main interest for non-finite or non-discrete groups is in the case of profinite groups because of their connection with Galois cohomology in the non-finite case. For a profinite group, the G-module is always given the discrete topology and the action $G \prod A \longrightarrow A$ is assumed continuous.)

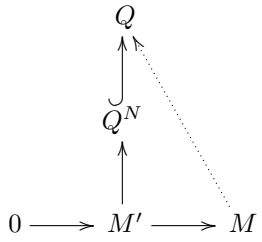
We have three categories: G-mod, G/N-mod and $\mathcal{A}$b. And we have the two functors

$$A \rightsquigarrow H^0(N, A) = A^N \qquad (G\text{-mod} \rightsquigarrow G/N\text{-mod}),$$

and

$$B \rightsquigarrow H^0(G/N, B) = B^{G/N} \qquad (G/N\text{-mod} \rightsquigarrow \mathcal{A}\mathrm{b}).$$

Of course, their composition is exactly $A \rightsquigarrow A^G$. To apply Grothendieck's Theorem, we have to show that if Q is an injective G-module, then Q^N is G/N-cohomologically trivial. But, I claim Q^N is, in fact, G/N-injective. To see this, take $0 \longrightarrow M' \longrightarrow M$ exact in G/N-mod and look at the diagram (in G-mod)



Every G/N-module is a G-module (*via* the map $G \longrightarrow G/N$) and Q is G-injective; so, the dotted arrow exists as a G-homomorphism rendering the diagram commutative. Let θ be the dotted arrow; look at $\mathrm{Im}\,\theta$.

If $q = \theta(m)$ and $\sigma \in N \subseteq G$, then $\sigma q = \theta(\sigma m) = \theta(m) = q$, because M is a G/N-module so N acts trivially on it. Therefore $q \in Q^N$ and so θ factors through Q^N, as required.

We obtain the Hochschild-Serre SS

$$H^p(G/N, H^q(N, A)) \underset{p}{\Longrightarrow} H^\bullet(G, A). \tag{HS}$$

Here is an application of importance for profinite groups (and Galois cohomology). If G is profinite, write c.d.$(G) \leq r$ (resp. c.d.$_p(G) \leq r$) provided $H^s(G, M) = (0)$ whenever M is a $\mathbb{Z}$-torsion G-module (resp. p-torsion G-module) and $s > r$. This notion is uninteresting for finite groups (see the exercises for the reason).

Theorem 5.2 *(Tower Theorem) If G is a profinite group and N is a closed normal subgroup, then*

$$\text{c.d.}(G) \leq \text{c.d.}(N) + \text{c.d.}(G/N).$$

(also true for c.d.$_p$*).*

Proof. We may assume c.d.$(N) \leq a < \infty$ and c.d.$(G/N) \leq b < \infty$, otherwise the result is trivial. Let M be a torsion G-module and suppose $n > a + b$. All we need show is $H^n(G, M) = (0)$. Write $n = p + q$ with $p \geq 0$, $q \geq 0$. In the Hochschild-Serre SS, the terms

$$E_2^{p,q} = H^p(G/N, H^q(N, M))$$

must vanish. For if $p \leq b$, then $q > a$ and $H^q(N, M)$ is zero by hypothesis. Now M is torsion therefore M^N is torsion and we saw in Chapter 4 that $H^q(N, M)$ is always torsion if $q > 0$ as it is a right limit of torsion groups. So, if $q \leq a$, then $p > b$ and $E_2^{p,q} = (0)$ by hypothesis on G/N. Therefore, $E_s^{p,q} = (0)$ for all s with $2 \leq s \leq \infty$, when $p + q = n > a + b$. Hence, the terms in the composition series for $H^n(G, M)$ all vanish and we're done.

(II) The Leray Spectral Sequence

The set-up here is a morphism

$$\pi \colon (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$$

of ringed spaces (c.f. Section 5.3) and the three categories are: $\mathcal{S}(X)$, $\mathcal{S}(Y)$, $\mathcal{A}$b. The functors are

$$\pi_* \colon \mathcal{S}(X) \rightsquigarrow \mathcal{S}(Y)$$

and

$$H^0(Y, -) \colon \mathcal{S}(Y) \rightsquigarrow \mathcal{A}\text{b}.$$

Of course, $H^0(X, -) \colon \mathcal{S}(X) \rightsquigarrow \mathcal{A}$b is the composition $H^0(Y, -) \circ \pi_*$. We must show that if Q is an injective sheaf on X, then $\pi_* Q$ is cohomologically trivial on Y. Now every injective is flasque and flasque sheaves are cohomologically trivial; so, it will suffice to prove π_* takes flasque sheaves on X to flasque sheaves on Y.

But this is trivial, for if U and V are open on Y and $V \subseteq U$, then $\pi^{-1}(V) \subseteq \pi^{-1}(U)$ and

$$\begin{array}{ccc} \pi_* F(U) & = & F(\pi^{-1}(U)) \\ \downarrow & & \downarrow \\ \pi_* F(V) & = & F(\pi^{-1}(V)) \end{array}$$

shows that surjectivity of the left vertical arrow follows from surjectivity on the right. We therefore obtain the Leray Spectral Sequence

$$H^p(Y, R^q\pi_* F) \underset{p}{\Longrightarrow} H^\bullet(X, F). \tag{LSS}$$

Unfortunately, full use of this spectral sequence demands considerable control of the sheaves $R^q\pi_* F$ and this is vitally affected by the map π; that is, by the "relative geometry and topology of X *vis a vis* Y". We must leave matters as they stand here.

(III) The Čech Cohomology Spectral Sequence

Once again, let $(X, \mathcal{O}_X)$ be a ringed space and write $\mathcal{S}(X)$ and $\mathcal{P}(X)$ for the categories of sheaves of $\mathcal{O}_X$-modules and presheaves of $\mathcal{O}_X$-modules. We also have two left exact functors from $\mathcal{P}(X)$ to $\mathcal{A}$b. Namely, if $\{U_\alpha \longrightarrow X\}_\alpha$ is an open cover of X and $G \in \mathcal{P}(X)$, then $H^0(\{U_\alpha \longrightarrow X\}_\alpha, G)$ is in $\mathcal{A}$b and we have $\check{H}^0(X, G)$, where the latter abelian group is what we called $G^{(+)}(X)$ in footnote 6 of Section 5.3. For the three abelian categories: $\mathcal{S}(X)$, $\mathcal{P}(X)$, $\mathcal{A}$b we now have the two composed functors

$$\mathcal{S}(X) \overset{i}{\hookrightarrow} \mathcal{P}(X) \overset{H^0(\{U_\alpha \to X\}, -)}{\rightsquigarrow} \mathcal{A}\text{b}$$

$$\mathcal{S}(X) \overset{i}{\hookrightarrow} \mathcal{P}(X) \overset{\check{H}^0(X, -)}{\rightsquigarrow} \mathcal{A}\text{b}.$$

Observe that both composed functors are the same functor:

$$F \in \mathcal{S}(X) \rightsquigarrow H^0(X, F) \in \mathcal{A}\text{b}.$$

We need to show that if Q is an injective sheaf, then $i(Q)$ is acyclic for either $H^0(\{U_\alpha \to X\}, -)$ or $\check{H}^0(X, -)$. However, part (3) of Corollary 5.33 says that $i(Q)$ is injective as presheaf and is therefore acyclic. From Grothendieck's Theorem, we obtain the two *Čech Cohomology Spectral Sequences*:

$$H^p(\{U_\alpha \longrightarrow X\}_\alpha, \mathcal{H}^q(F)) \underset{p}{\Longrightarrow} H^\bullet(X, F) \tag{CCI}$$

$$\check{H}^p(X, \mathcal{H}^q(F)) \underset{p}{\Longrightarrow} H^\bullet(X, F) \tag{CCII}$$

Now it turns out that $\mathcal{H}^q(F)^\# = (0)$ for every $q > 0$ and every sheaf, F. (See the exercises.) Also, $\mathcal{H}^q(F)^{(+)} \subseteq \mathcal{H}^q(F)^\#$; so, we find

$$E_2^{0,q} = \check{H}^0(X, \mathcal{H}^q(F)) = \mathcal{H}^q(F)^{(+)} = (0), \quad \text{when} \quad q > 0.$$

If we apply the edge sequence to (CCII), we deduce

Proposition 5.59 *If $(X, \mathcal{O}_X)$ is a ringed space and F is a sheaf of $\mathcal{O}_X$-modules and if we continue to write F when F is considered as a presheaf (instead of $i(F)$), then*

(1) $\check{H}^1(X, F) \longrightarrow H^1(X, F)$ is an isomorphism and

(2) $\check{H}^2(X, F) \longrightarrow H^2(X, F)$ is injective.

(IV) The Local to Global Ext **Spectral Sequence**

Again, let $(X, \mathcal{O}_X)$ be a ringed space and fix a sheaf, A, of $\mathcal{O}_X$-modules on X. Write $\mathcal{S}(X)$ for the (abelian) category of $\mathcal{O}_X$-modules. We can make a functor from $\mathcal{S}(X)$ to itself, denoted $\mathcal{H}om_{\mathcal{O}_X}(A, -)$ *via*

$$\mathcal{H}om_{\mathcal{O}_X}(A, B)(U) = \mathrm{Hom}_{\mathcal{O}_X \restriction U}(A \restriction U, B \restriction U).$$

Here, U is open in X, the functor $\mathcal{H}om_{\mathcal{O}_X}(A,-)$ is usually called the *sheaf Hom*, it is (of course) left exact and its right derived functors (called *sheaf Ext*) are denoted $\mathcal{E}xt^\bullet_{\mathcal{O}_X}(A,-)$.

Therefore, we have the situation of three categories $\mathcal{S}(X)$, $\mathcal{S}(X)$, $\mathcal{A}\mathrm{b}$ and the two functors

$$\mathcal{H}om_{\mathcal{O}_X}(A,-)\colon \mathcal{S}(X) \rightsquigarrow \mathcal{S}(X)$$
$$H^0(X,-) = \Gamma(X,-)\colon \mathcal{S}(X) \rightsquigarrow \mathcal{A}\mathrm{b}$$

whose composition is the functor $\mathrm{Hom}_{\mathcal{O}_X}(A,-)$. In order to apply Grothendieck's Theorem, we must show that *if Q is injective in $\mathcal{S}(X)$, then $\mathcal{H}om_{\mathcal{O}_X}(A,Q)$ is an acyclic sheaf*. This, in turn, follows from

Proposition 5.60 *Suppose that Q is an injective sheaf of $\mathcal{O}_X$-modules. Then $\mathcal{H}om_{\mathcal{O}_X}(A,Q)$ is a flasque $\mathcal{O}_X$-module.*

Proof. If U is open in X, recall we have the presheaf A_U defined by

$$A_U(V) = \begin{cases} A(V) & \text{if } V \subseteq U \\ (0) & \text{if } V \not\subseteq U \end{cases}$$

and this gives rise to the associated sheaf $(A_U)^\sharp$. Now by adjointness,

$$\mathrm{Hom}_{\mathcal{O}_X}((A_U)^\sharp, B) \cong \mathrm{Hom}_{\mathcal{O}_X\text{-presheaves}}(A_U, i(B)).$$

On the right hand side, if V is open and $V \subseteq U$, then an element of $\mathrm{Hom}_{\mathcal{O}_X}(A_U, i(B))$ gives the map $A(V) \longrightarrow B(V)$ (consistent with restrictions). But, if $V \not\subseteq U$, we just get 0. However, this is exactly what we get from $\mathrm{Hom}_{\mathcal{O}_U}(A \restriction U, B \restriction U)$; therefore

$$\mathrm{Hom}_{\mathcal{O}_X}((A_U)^\sharp, B) = \mathrm{Hom}_{\mathcal{O}_X \restriction U}(A \restriction U, B \restriction U).$$

Now take Q to be an injective sheaf, we have to show that

$$\mathrm{Hom}_{\mathcal{O}_X}(A,Q) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X \restriction U}(A \restriction U, Q \restriction U)$$

is surjective for each open U of X. This means we must show that

$$\mathrm{Hom}_{\mathcal{O}_X}(A,Q) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}((A_U)^\sharp, Q)$$

is surjective. But, $0 \longrightarrow (A_U)^\sharp \longrightarrow A$ is exact and Q is injective; so, we are done.

We obtain the *local to global* Ext *spectral sequence*

$$H^p(X, \mathcal{E}xt^q_{\mathcal{O}_X}(A,B)) \underset{p}{\Longrightarrow} \mathrm{Ext}^\bullet_{\mathcal{O}_X}(A,B). \tag{LGExt}$$

Remark: If $j\colon U \hookrightarrow X$ is the inclusion of the open set U in X, then the sheaf we have denoted $(A_U)^\sharp$ above is usually denoted $j_!A$. The functor, $j_!$, is left-exact and so we have a basic sequence of sheaf invariants $R^\bullet j_!$. Of course, we also have $R^\bullet\pi_*$ (for a morphism $\pi\colon Y \to X$) as well as π^*, $j^!$ (adjoint to $j_!$). The *six operations*

$$R^\bullet\pi_*,\ R^\bullet j_!,\ \pi^*,\ j^!,\ R^\bullet\mathcal{H}om,\ \otimes$$

were singled out by A. Grothendieck as the important test cases for the permanence of sheaf properties under morphisms.

(V) "Associativity" Spectral Sequences for Ext **and** Tor

In the proof of Grothendieck's Theorem on the spectral sequence for composed functors, there were two parts. In the first part, we used the essential hypothesis that $F(Q)$ was G-acyclic to compute the cohomology of the total complex (of our double complex) as $R^\bullet(GF(A))$—this is the ending of the spectral sequence. In the second part, which depends only on using a Cartan-Eilenberg resolution and did **not** use the G-acyclicity of $F(Q)$, we computed the spectral sequence $\mathrm{II}_2^{p,q} \Longrightarrow H^\bullet(C)$ and found $R^pG(R^qF(A)) \Longrightarrow H^\bullet(C)$. This second part is always available to us by Proposition 5.58 and we'll make use of it below.

We consider modules over various rings. In order that we have enough flexibility to specialize to varying cases of interest, we begin with three K-algebras, R, S, T and modules A, B, C as follows:

$$(\dagger)\begin{cases} A \text{ is a right } R \text{ and a right } S\text{-module} \\ B \text{ is a left } R\text{-module and a right } T\text{-module} \\ C \text{ is a right } S \text{ and a right } T\text{-module.} \end{cases}$$

Then

$A \otimes_R B$ is a right $S \otimes_K T$-module

and

$\mathrm{Hom}_T(B, C)$ is a right $R \otimes_K S$-module.

Observe that A is then a right $R \otimes_K S$-module *via*

$$a(r \otimes s) = (ar)s$$

because to say A is a right R and a right S-module is to imply

$$(ar)s = (as)r \qquad (\text{all } a \in A, r \in R, s \in S).$$

Also, C is a right $S \otimes_K T$-module. We know in this situation there is an "associativity" isomorphism

$$\mathrm{Hom}_{R\otimes_K S}(A, \mathrm{Hom}_T(B, C)) \cong \mathrm{Hom}_{S\otimes_K T}(A \otimes_R B, C). \qquad (*)$$

If S is K-projective and $P_\bullet \longrightarrow A \longrightarrow 0$ is an $R \otimes_K S$-projective resolution of A, then $P_\bullet \longrightarrow A \longrightarrow 0$ is still an R-projective resolution of A and similarly if $0 \longrightarrow C \longrightarrow Q^\bullet$ is an $S \otimes_K T$-injective resolution, it still is a T-injective resolution of C. Our spectral sequences $\mathrm{II}_2^{p,q}$ then give us two spectral sequences with the same ending (by $(*)$):

$$\begin{aligned} \mathrm{Ext}^p_{R\otimes_K S}(A, \mathrm{Ext}^q_T(B, C)) &\Longrightarrow \mathrm{Ending}^\bullet \\ \mathrm{Ext}^p_{S\otimes_K T}(\mathrm{Tor}^R_q(A, B), C) &\Longrightarrow \mathrm{Ending}^\bullet. \end{aligned}$$

In a similar way, but this time if C is a (left) S and T-module, we get the "associativity" isomorphism

$$A \otimes_{R\otimes_K S} (B \otimes_T C) \cong (A \otimes_R B) \otimes_{S\otimes_K T} C. \qquad (**)$$

Again, we assume S is K-projective and we get two spectral sequences with the same ending (by $(**)$):

$$\begin{aligned} \mathrm{Tor}^{R\otimes_K S}_p(A, \mathrm{Tor}^T_q(B, C)) &\Longrightarrow \widetilde{\mathrm{Ending}}^\bullet \\ \mathrm{Tor}^{S\otimes_K T}_p(\mathrm{Tor}^R_q(A, B), C) &\Longrightarrow \widetilde{\mathrm{Ending}}^\bullet. \end{aligned}$$

However, it is not clear how to compute the endings in these general cases. If we assume more, this can be done. For example, say $\mathrm{Tor}^R_q(A, B) = (0)$ if $q > 0$—this will be true when either A or B is flat over R—then the second Ext sequence and second Tor sequence collapse and we find

$$\begin{aligned} \mathrm{Ext}^p_{R\otimes_K S}(A, \mathrm{Ext}^q_T(B, C)) &\Longrightarrow \mathrm{Ext}^\bullet_{S\otimes_K T}(A \otimes_R B, C) \\ \mathrm{Tor}^{R\otimes_K S}_p(A, \mathrm{Tor}^T_q(B, C)) &\Longrightarrow \mathrm{Tor}_\bullet^{S\otimes_K T}(A \otimes_R B, C). \end{aligned}$$

We have proved all but the last statement of

Proposition 5.61 *Suppose R, S, T are K-algebras with S projective over K and say A is an R and S right module, C is an S and T right (resp. left) module and B is a left R and right T-module. Then there are spectral sequences with the same ending*

$$\begin{aligned} \operatorname{Ext}^p_{R\otimes_K S}(A, \operatorname{Ext}^q_T(B,C)) &\implies \text{Ending}^\bullet \\ \operatorname{Ext}^p_{S\otimes_K T}(\operatorname{Tor}^R_q(A,B), C) &\implies \text{Ending}^\bullet \end{aligned}$$

(resp.

$$\begin{aligned} \operatorname{Tor}_p^{R\otimes_K S}(A, \operatorname{Tor}^T_q(B,C)) &\implies \widetilde{\text{Ending}}^\bullet \\ \operatorname{Tor}_p^{S\otimes_K T}(\operatorname{Tor}^R_q(A,B), C) &\implies \widetilde{\text{Ending}}^\bullet \text{)} \end{aligned}$$

If $\operatorname{Tor}^R_q(A,B) = (0)$ *when* $q > 0$ *(e.g. if A or B is R-flat) then*

$$\operatorname{Ext}^p_{R\otimes_K S}(A, \operatorname{Ext}^q_T(B,C)) \Longrightarrow \operatorname{Ext}^\bullet_{S\otimes_K T}(A \otimes_R B, C) \tag{Ext}$$

and

$$\operatorname{Tor}_p^{R\otimes_K S}(A, \operatorname{Tor}^T_q(B,C)) \Longrightarrow \operatorname{Tor}^{S\otimes_K T}_\bullet(A \otimes_R B, C)). \tag{Tor}$$

Lastly, if B is T-projective (more generally $\operatorname{Ext}^q_T(B,C)$ *vanishes if $q > 0$ and* $\operatorname{Tor}^T_q(B,C)$ *vanishes if $q > 0$), then we have the* Ext *and* Tor *associativity formulae*

$$\operatorname{Ext}^p_{R\otimes_K S}(A, \operatorname{Hom}_T(B,C)) \cong \operatorname{Ext}^p_{S\otimes_K T}(A \otimes_R B, C)$$

and

$$\operatorname{Tor}_p^{R\otimes_K S}(A, B \otimes_T C) \cong \operatorname{Tor}_p^{S\otimes_K T}(A \otimes_R B, C).$$

Proof. The last statement is trivial as our spectral sequences (Ext), (Tor) collapse.

Upon specializing the K-algebras R, S, T and the modules A, B, C, we can obtain several corollaries of interest. For example, let $S = R^{\mathrm{op}}$ and $A = R$. Then $\operatorname{Ext}^p_{R\otimes R^{\mathrm{op}}}(R, -) = H^p(R, -)$ in Hochschild's sense (by Section 5.3) and if R is K-projective the spectral sequences involving Ext yield

Corollary 5.62 *If R is K-projective then there is a spectral sequence*

$$H^p(R, \operatorname{Ext}^q_T(B,C)) \Longrightarrow \operatorname{Ext}^\bullet_{R^{\mathrm{op}}\otimes_K T}(B,C)$$

provided B is a left R and right T-module and C is also a left R and right T-module.

Note that this is reminiscent of the local-global Ext spectral sequence. Note further that if B is also T-*projective*, we deduce an isomorphism

$$H^p(R, \operatorname{Hom}_T(B,C)) \cong \operatorname{Ext}^p_{R^{\mathrm{op}}\otimes T}(B,C).$$

Next, let $A = B = R = K$ in the Ext-sequences. If S is K-projective the second Ext sequence collapses and gives $\operatorname{Ext}^p_{S\otimes_K T}(K,C) \cong \text{Ending}^p$. The first spectral sequence then yields

Corollary 5.63 *Say S is K-projective and S and T possess augmentations to K, then we have the spectral sequence*

$$\operatorname{Ext}^p_S(K, \operatorname{Ext}^q_T(K,C)) \Longrightarrow \operatorname{Ext}^\bullet_{S\otimes_K T}(K,C),$$

where C is a right S and right T-module.

Here is another corollary:

Corollary 5.64 *Say S and T are K-algebras with S being K-projective. Assume C is a two-sided $S \otimes_K T$-module, then there is a spectral sequence*

$$H^p(S, H^q(T, C)) \Longrightarrow H^\bullet(S \otimes_K T, C).$$

Proof. For this use K, S^e, T^e in place of R, S, T. Now S^e is K-projective as S is so. Further replace A, B, C by (S, T, C)—this is O.K. because C is indeed both a right S^e and right T^e-module by hypothesis. The second Ext sequence collapses; so,

$$\mathrm{Ext}^p_{(S\otimes_K T)^e}(S \otimes_K T, C) \cong \mathrm{Ending}^p.$$

But, the left-side is just $H^p(S \otimes_K T, C)$ by definition. Now the $E_2^{p,q}$ term of our first Ext sequence is

$$\mathrm{Ext}^p_{S^e}(S, \mathrm{Ext}^q_{T^e}(T, C))$$

that is, it equals $H^p(S, H^q(T, C))$; so our proposition concludes the proof.

Clearly, there are analogous results for homology. Here are the conclusions, the exact hypotheses and the proofs will be left as (DX).

$$\begin{aligned} H_p(T, \mathrm{Tor}^R_q(A, B)) &\Longrightarrow \mathrm{Tor}^{R\otimes_K T^{\mathrm{op}}}_\bullet(A, B) \\ \mathrm{Tor}^S_p(\mathrm{Tor}^R_q(A, K), K) &\Longrightarrow \mathrm{Tor}^{R\otimes_K S}_\bullet(A, K) \\ H_p(S, H_q(R, A)) &\Longrightarrow H_\bullet(R \otimes_K S, A). \end{aligned}$$

5.5 The Koszul Complex and Applications

In our previous work on the Hochschild cohomology of algebras, we studied the standard or bar complex, but we saw that it was inefficient in several cases of interest. As mentioned there, we have another, much better complex—the *Koszul complex*—which will serve for varied applications and which we turn to now.

Let A be a ring and M a module over this ring. For simplicity, we'll assume A is commutative as the main applications occur in this case. But, all can be done wih appropriate care in the general case. The Koszul complex is defined with respect to any given sequence $(f_1, \ldots, f_r)$ of elements of A. We write

$$\overrightarrow{f} = (f_1, \ldots, f_r).$$

Form the graded exterior power $\bigwedge^\bullet A^r$. We make $\bigwedge^\bullet A^r$ into a complex according to the following prescription: Since

$$\bigwedge^\bullet A^r = \coprod_{k=0}^{r} \bigwedge^k A^r,$$

it is a graded module, and we just have to define differentiation. Let $(e_1, \ldots, e_r)$ be the canonical basis of A^r, and set

$$de_j = f_j \in \bigwedge^0 A^r = A,$$

then extend d to be an antiderivation. That is, extend d *via*

$$d(\alpha \wedge \beta) = d\alpha \wedge \beta + (-1)^{\deg\alpha} \alpha \wedge d\beta.$$

For example,

$$d(e_i \wedge e_j) = f_i e_j - f_j e_i,$$

and

$$\begin{aligned} d(e_i \wedge e_j \wedge e_k) &= d(e_i \wedge e_j) \wedge e_k + (e_i \wedge e_j) \wedge de_k \\ &= (f_i e_j - f_j e_i) \wedge e_k + f_k (e_i \wedge e_j) \\ &= f_i \widehat{e_i} \wedge e_j \wedge e_k - f_j e_i \wedge \widehat{e_j} \wedge e_k + f_k e_i \wedge e_j \wedge \widehat{e_k}, \end{aligned}$$

where, as usual, the hat above a symbol means that this symbol is omitted. By an easy induction, we get the formula:

$$d(e_{i_1} \wedge \cdots \wedge e_{i_t}) = \sum_{j=1}^{t} (-1)^{j-1} f_{i_j} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_j}} \wedge \cdots \wedge e_{i_t}.$$

We denote this complex by $K_\bullet(\overrightarrow{f})$, i.e., it is the graded module $\bigwedge^\bullet A^r$ with the antiderivation d that we just defined. This is the *Koszul complex*.

Given an A-module M, we can make two Koszul complexes for the module M, namely:

$$\begin{aligned} K_\bullet(\overrightarrow{f}, M) &= K_\bullet(\overrightarrow{f}) \otimes_A M, \\ K^\bullet(\overrightarrow{f}, M) &= \mathrm{Hom}_A(K_\bullet(\overrightarrow{f}), M). \end{aligned}$$

We can take the homology and the cohomology respectively of these complexes, and we get the modules

$$H_\bullet(\overrightarrow{f}, M) \quad \text{and} \quad H^\bullet(\overrightarrow{f}, M).$$

For the cohomology complex, we need the explicit form of δ. Now,

$$K^t(\overrightarrow{f}, M) = \mathrm{Hom}_A(\bigwedge^t A^r, M),$$

and the family of elements of the form

$$e_{i_1} \wedge \cdots \wedge e_{i_t} \quad \text{with } 1 \leq i_1 < i_2 < \ldots < i_t \leq r,$$

is a basis of $\bigwedge^t A^r$; thus, $\mathrm{Hom}_A(\bigwedge^t A^r, M)$ is isomorphic to the set of alternating functions, g, from the set of sequences $(i_1, \ldots, i_t)$ of length t in $\{1, \ldots, r\}$ to M. Hence, the coboundary δ is given (on elements $g \in \mathrm{Hom}_A(\bigwedge^t A^r, M)$) by

$$(\delta g)(i_1, \ldots i_{t+1}) = \sum_{j=1}^{t+1} (-1)^{j-1} f_{i_j} g(i_1, \ldots, \widehat{i_j}, \ldots, i_{t+1}).$$

We have $H^0(\overrightarrow{f}, M) = Z^0(\overrightarrow{f}, M) = \mathrm{Ker}\, \delta$. (Note that $K^0(\overrightarrow{f}, M) = M$, *via* the map $g \mapsto g(1)$.) Then,

$$\delta g(e_i) = f_i g(1) = f_i m,$$

so $\delta f = 0$ implies that $f_i m = 0$ for all i. We find that

$$H^0(\overrightarrow{f}, M) = \{m \in M \mid \mathfrak{A} m = 0\}, \tag{5.1}$$

where $\mathfrak{A}$ is the ideal generated by $\{f_1, \ldots, f_r\}$. Also, it is clear that

$$H^t(\overrightarrow{f}, M) = 0 \quad \text{if } t < 0 \text{ or } t > r. \tag{5.2}$$

Let us compute the top cohomology group $H^r(\overrightarrow{f}, M)$. We have

$$Z^r(\overrightarrow{f}, M) = K^r(\overrightarrow{f}, M) = \mathrm{Hom}_A(\bigwedge^r A^r, M) = M,$$

via the map $g \mapsto g(e_1 \wedge \cdots \wedge e_r)$. Now, $\mathrm{Im}\, \delta_{r-1} = B^r(\overrightarrow{f}, M)$, but what is $B^r(\overrightarrow{f}, M)$? If $g \in K^{r-1}(\overrightarrow{f}, M)$ is an alternating function on $i_1, \ldots, i_{r-1}$, then

$$\delta_{r-1} g(1, \ldots, r) = (\delta_{r-1} g)(e_1 \wedge \cdots \wedge e_r) = \sum_{j=1}^{r} (-1)^{j-1} f_j g(1, \ldots, \widehat{j}, \ldots, r).$$

Therefore,

$$B^r = f_1 M + \cdots + f_r M,$$

and we find that

$$H^r(\overrightarrow{f}, M) = M/(f_1 M + \cdots + f_r M) = M/\mathfrak{A} M.$$

It is important to connect the Koszul homology (whose boundary map is

$$\partial(e_{i_1} \wedge \cdots \wedge e_{i_t} \otimes m) = \sum_{j=1}^{t} (-1)^{j-1} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_j}} \wedge \cdots e_{i_t} \otimes f_{i_j} m)$$

and cohomology *via* the notion of *Koszul duality*. This is the following: Consider $K_t(\overrightarrow{f}, M)$; an element of $K_t(\overrightarrow{f}, M)$ has the form

$$h = \sum e_{i_1} \wedge \cdots \wedge e_{i_t} \otimes z_{i_1 \ldots i_t}, \quad \text{where } 1 \leq i_1 < i_2 < \ldots < i_t \leq r.$$

We define a map (the duality map)

$$\Theta\colon K_t(\overrightarrow{f}, M) \longrightarrow K^{r-t}(\overrightarrow{f}, M)$$

as follows: Pick $j_1 < j_2 < \cdots < j_{r-t}$, and set

$$\Theta(h)(j_1, \ldots, j_{r-t}) = \epsilon z_{i_1 \ldots i_t},$$

where

(α) $i_1, \ldots, i_t$ is the set of complementary indices of $j_1, \ldots, j_{r-t}$ taken in ascending order,

(β) ϵ is the sign of the permutation

$$(1, 2, \ldots, r) \mapsto (i_1, \ldots, i_t, j_1, \ldots, j_{r-t}),$$

where both $i_1, \ldots, i_t$ and $j_1, \ldots, j_{r-t}$ are in ascending order.

We find (DX) that

$$\Theta(\partial h) = \delta\Theta(h),$$

where ∂ is the homology boundary map described above. So, the isomorphism, Θ, induces an isomorphism

$$H_t(\overrightarrow{f}, M) \cong H^{r-t}(\overrightarrow{f}, M) \quad \text{for all } t \geq 0,$$

which is called *Koszul duality*. This notion of Koszul duality does not look like a duality, but we can make it look so. For this, write $Q(A)$ for "the" injective hull of A as A-module and set $M^D = \mathrm{Hom}_A(M, Q(A))$. The cofunctor $M \rightsquigarrow M^D$ is exact; we'll refer to M^D as the dual of M. Now the associativity isomorphism

$$\mathrm{Hom}_A(M \otimes_A N, Z) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, Z))$$

shows that $(K_t(\overrightarrow{f}, M))^D$ is isomorphic to $K^t(\overrightarrow{f}, M^D)$. Moreover, it is easy to see that

$$\begin{array}{ccc} (K_t(\overrightarrow{f}, M))^D & \xrightarrow{\cong} & K^t(\overrightarrow{f}, M^D) \\ \uparrow{\scriptstyle \partial_t^D} & & \uparrow{\scriptstyle \delta^{t-1}} \\ (K_{t-1}(\overrightarrow{f}, M))^D & \xrightarrow{\cong} & K^{t-1}(\overrightarrow{f}, M^D) \end{array}$$

is a commutative diagram. So, it follows (by the exactness of $M \rightsquigarrow M^D$) (DX) that our isomorphisms yield isomorphisms

$$H_t(\overrightarrow{f}, M)^D \cong H^t(\overrightarrow{f}, M^D), \quad \text{for all } t \geq 0. \tag{5.3}$$

Put these together with the above notion of Koszul duality and obtain the *duality isomorphisms*

$$\begin{aligned} H^t(\overrightarrow{f}, M^D) &\cong H^{r-t}(\overrightarrow{f}, M)^D \\ H_t(\overrightarrow{f}, M^D) &\cong H_{r-t}(\overrightarrow{f}, M)^D, \quad \text{for all } t \geq 0. \end{aligned}$$

Gathering together what we have proved above, we find the following

Proposition 5.65 *If A is a (commutative) ring, M is an A-module, and $\overrightarrow{f} = (f_1, \ldots, f_r)$ an ordered set of r elements from A, then for the Koszul homology and cohomology of M we have*

(0) $H_t(\overrightarrow{f}, M) = H^t(\overrightarrow{f}, M) = (0)$ *if* $t < 0$ *or* $t > r$,

(1) (Koszul duality) There is an isomorphism

$$H_t(\overrightarrow{f}, M) \cong H^{r-t}(\overrightarrow{f}, M), \quad \text{all } t \geq 0,$$

(2)

$$\begin{aligned} H_0(\overrightarrow{f}, M) &= H^r(\overrightarrow{f}, M) = M/\mathfrak{A}M, \\ H^0(\overrightarrow{f}, M) &= H_r(\overrightarrow{f}, M) = \{m \mid \mathfrak{A}m = 0\}, \end{aligned}$$

where $\mathfrak{A}$ *is the ideal generated by* $f_1, \ldots, f_r$.

Write $M^D = \mathrm{Hom}_A(M, Q(A))$ *with* $Q(A)$ *the injective hull of* A, *then*

(3) $H_t(\overrightarrow{f}, M)^D \cong H^t(\overrightarrow{f}, M^D)$

and Koszul duality becomes

$$\begin{aligned} H^t(\overrightarrow{f}, M^D) &\cong H^{r-t}(\overrightarrow{f}, M)^D, \\ H_t(\overrightarrow{f}, M^D) &\cong H_{r-t}(\overrightarrow{f}, M)^D, \quad \text{for all } t \geq 0. \end{aligned}$$

We need one more definition to exhibit the main algebraic property of the Koszul complex.

Definition 5.12 The sequence $\overrightarrow{f} = (f_1, \ldots, f_r)$ is *regular* for M or M*-regular* if for every i, with $1 \leq i \leq r$, the map

$$z \mapsto f_i z$$

is an injection of $M/(f_1 M + \cdots + f_{i-1} M)$ to itself.

By its very definition, the notion of M-regularity appears to depend on the order of the elements $f_1, \ldots, f_r$. This is indeed the case as the following classical example [39] shows: Let A be $\mathbb{C}[X, Y, Z]$ and $f_1 = X(Y-1)$; $f_2 = Y$; $f_3 = Z(Y-1)$. Then unique factorization in A shows that f_1, f_2, f_3 is A-regular, but f_1, f_3, f_2 is certainly not A-regular as $f_3 X$ is zero in $A/f_1 A$ but X is not zero there. In the special case that A is graded, M is a graded module and the f_j are homogeneous elements of A, the order of an M-sequence does not matter.

If $\mathfrak{A}$ is a given ideal of A and $f_1, \ldots, f_r \in \mathfrak{A}$ (the f_j are not necessarily generators of $\mathfrak{A}$), and if $f_1, \ldots, f_r$ is an M-regular sequence but no for other element $g \in \mathfrak{A}$ is $f_1, \ldots, f_r, g$ an M-regular sequence, then $f_1, \ldots, f_r$ is a *maximal* M*-regular sequence from* $\mathfrak{A}$. It turns out that *the number of elements in a maximal* M*-regular sequence from* $\mathfrak{A}$ *is independent of the choice of such a sequence*; this number is called the $\mathfrak{A}$*-depth* of M and denoted $\mathrm{depth}_{\mathfrak{A}} M$. (When A is a local ring and $\mathfrak{A} = \mathfrak{M}$ is its maximal ideal, one writes $\mathrm{depth}\, M$ and omits any reference to $\mathfrak{M}$.)

Here is the main property of the Koszul complex *vis a vis* M-regularity (and, hence, depth):

Proposition 5.66 *(Koszul) Suppose* M *is an* A*-module and* $\overrightarrow{f}$ *is an* M*-regular sequence of length* r. *Then the Koszul complexes* $K_\bullet(\overrightarrow{f}, M)$ *and* $K^\bullet(\overrightarrow{f}, M)$ *are acyclic and consequently*

$$H_i(\overrightarrow{f}, M) = (0) \quad \text{if} \quad i \neq 0 \quad \text{and} \quad H^i(\overrightarrow{f}, M) = (0) \quad \text{if} \quad i \neq r.$$

Proof. The two Koszul complexes

$$K_\bullet(\overrightarrow{f}, M)\colon M \xrightarrow{\partial_r} \bigwedge^{r-1} A^r \otimes_A M \xrightarrow{\partial} \cdots \xrightarrow{\partial} A^r \otimes_A M \xrightarrow{\partial_1} M$$

$$K^\bullet(\overrightarrow{f}, M)\colon M \xrightarrow{\delta^0} \mathrm{Hom}_A(A^r, M) \xrightarrow{\delta} \cdots \xrightarrow{\delta} \mathrm{Hom}_A(\bigwedge^{r-1} A^r, M) \xrightarrow{\delta^{r-1}} M$$

will be exact sequences when $H_1(\overrightarrow{f}, M) = \cdots = H_{r-1}(\overrightarrow{f}, M) = (0)$ and when $H^1(\overrightarrow{f}, M) = \cdots = H^{r-1}(\overrightarrow{f}, M) = (0)$; so the vanishing statement of the conclusion appears stronger than acyclicity. But, under our hypothesis the modules

$$H_r(\overrightarrow{f}, M) = H^0(\overrightarrow{f}, M) = \{m \mid \mathfrak{A}m = (0)\}$$

automatically vanish since f_1 is a non-zero divisor on M.

We will prove the vanishing statements and, of course, by Koszul duality all we need prove is that $H_t(\overrightarrow{f}, M) = (0)$ for all $t > 0$. There are several ways of proving this; all use induction on r, the length of the M-sequence. We choose a method involving the tensor product of complexes.

If $C_\bullet$ and $D_\bullet$ are left complexes, we make their tensor product $C_\bullet \otimes D_\bullet$ by setting

$$(C_\bullet \otimes D_\bullet)_t = \coprod_{i+j=t} C_i \otimes D_j$$

and defining differentiation by

$$d(\alpha \otimes \beta) = d_C(\alpha) \otimes \beta + (-1)^{\deg \alpha} \alpha \otimes d_D(\beta).$$

Then, $(C_\bullet \otimes D_\bullet)_\bullet$ is a complex. Consider for example the Koszul complex for the single element $f \in A$. Namely,

$$K_\bullet(f)_t = \begin{cases} A & \text{if } t = 0 \text{ or } 1 \\ (0) & \text{if } t > 1 \end{cases}$$

a two term complex. Its differentiation is given by $d(e) = f$, where $e\,(= 1)$ is a base for A as A-module; in other words, d is just multiplication by f. With this notation, we have

$$K_\bullet(\overrightarrow{f}) = K_\bullet(f_1) \otimes \cdots \otimes K_\bullet(f_r).$$

Now the vanishing statements are true and trivial for $r = 0$ or 1. So, write $\overrightarrow{f'} = (f_1, \ldots, f_{r-1})$ and set $L_\bullet = K_\bullet(\overrightarrow{f'}, M)$. Since $\overrightarrow{f'}$ is M-regular we see that

$$H_t(\overrightarrow{f'}, M) = H_t(L_\bullet) = (0), \quad \text{for all } t > 0,$$

by the induction hypothesis. Further, set $M_\bullet = K_\bullet(f_r, M)$. Then $K_\bullet(\overrightarrow{f}, M) = (L_\bullet \otimes M_\bullet)_\bullet$, and this will enable our induction.

I claim that we have the exact sequence

$$\cdots \longrightarrow H_0(H_t(L_\bullet) \otimes M_\bullet) \longrightarrow H_t(L_\bullet \otimes M_\bullet) \longrightarrow H_1(H_{t-1}(L_\bullet) \otimes M_\bullet) \longrightarrow \cdots \tag{5.4}$$

for every $t \geq 0$. Suppose this claim is proved, take $t \geq 2$ (so that $t - 1 \geq 1$) and get

$$H_t(L_\bullet) = H_{t-1}(L_\bullet) = (0)$$

by the induction hypothesis. The exact sequence (5.4) tells us that $H_t(\overrightarrow{f}, M) = H_t(L_\bullet \otimes M_\bullet) = (0)$ when $t \geq 2$. If $t = 1$, we know that $H_1(L_\bullet)$ vanishes, so (5.4) gives us the exact sequence

$$0 \longrightarrow H_1(\overrightarrow{f}, M) \longrightarrow H_1(H_0(L_\bullet) \otimes M_\bullet).$$

But $H_1(-) = H^0(-)$ by Koszul duality for $M_\bullet$ and the latter is the kernel of multiplication by f_r on $(-)$. However, in this case $(-)$ is $H_0(L_\bullet) = M/(f_1M + \cdots + f_{r-1}M)$; the kernel of multiplication by f_r on this last module is zero because $f_1, \ldots, f_r$ is M-regular. We conclude $H_1(H_0(L_\bullet) \otimes M_\bullet)$ is zero, finishing our induction.

There remains only the proof of exact sequence (5.4). It, in turn, follows from a general homological lemma:

Lemma 5.67 *Suppose M is a two-term complex of A-modules, zero in degree $\neq 0, 1$ and for which M_0 and M_1 are free A-modules. If $L_\bullet$ is any complex of A-modules, we have the exact sequence*

$$\cdots \longrightarrow H_0(H_t(L_\bullet) \otimes M_\bullet) \longrightarrow H_t(L_\bullet \otimes M_\bullet) \longrightarrow H_1(H_{t-1}(L_\bullet) \otimes M_\bullet) \longrightarrow \cdots \tag{5.4}$$

for all $t \geq 0$.

Proof. Once again, we have more than one proof available. We'll sketch the first and give the second in detail. The modules comprising $M_\bullet$ are A-free, so there is a "Künneth Formula" spectral sequence

$$E^2_{p,q} = H_p(H_q(L_\bullet) \otimes_A M_\bullet) \Longrightarrow H_\bullet(L_\bullet \otimes_A M_\bullet).$$

(For example, see Corollary 5.64 and its homology analog.) But, as $M_\bullet$ is a two-term complex, $E^2_{p,q} = (0)$ if $p \neq 0, 1$ and we obtain the zipper sequence (**??**) of our lemma.

More explicitly (our second proof), we make two one-term complexes, M_i, in which M_i has its one term in degree i ($i = 0, 1$). Each differentiation in these complexes is to be the trivial map. We form the tensor product complexes $L_\bullet \otimes M_i$ and recall that

$$\begin{cases} (L_\bullet \otimes M_0)_p = L_p \otimes M_0 \\ d(\alpha \otimes \beta) = d_L(\alpha) \otimes \beta \\ H_p(L_\bullet \otimes M_0) = H_p(L_\bullet) \otimes M_0 \end{cases}$$

and

$$\begin{cases} (L_\bullet \otimes M_1)_p = L_{p-1} \otimes M_1 \\ d(\alpha \otimes \beta) = d_L(\alpha) \otimes \beta \\ H_p(L_\bullet \otimes M_1) = H_{p-1}(L_\bullet) \otimes M_1. \end{cases}$$

Then, we obtain an exact sequence of complexes

$$0 \longrightarrow L_\bullet \otimes M_0 \longrightarrow L_\bullet \otimes M_\bullet \longrightarrow L_\bullet \otimes M_1 \longrightarrow 0$$

and its corresponding long exact homology sequence

$$\cdots H_{p+1}(L_\bullet \otimes M_1) \xrightarrow{\partial} H_p(L_\bullet \otimes M_0) \longrightarrow H_p(L_\bullet \otimes M_\bullet) \longrightarrow H_p(L_\bullet \otimes M_1) \longrightarrow \cdots .$$

But, ∂ is just $1 \otimes d_{M_\bullet}$ and so the above homology sequence is exactly (**??**). □

The main applications we shall make of the Koszul complex concern the notion of "dimension"—and even here most applications will be to commutative rings. We begin by defining the various notions of dimension. Suppose R is a ring (not necessarily commutative) and M is an R-module.

Definition 5.13 The module M has *projective dimension* (resp. *injective dimension*) $\leq n$ if and only if it possesses a projective (resp. injective) resolution $P_\bullet \longrightarrow M \longrightarrow 0$ (resp. $0 \longrightarrow M \longrightarrow Q^\bullet$) for which $P_t = 0$ (resp. $Q^t = 0$) when $t > n$. The infimum of the integers n for which M has projective (resp. injective) dimension $\leq n$ is called the *projective dimension* (resp. *injective dimension*) *of* M.

Remark: Of course, if no n exists so that proj dim $M \leq n$, then we write proj dim $M = \infty$ and similarly for injective dimension. A module is projective (resp. injective) iff it has proj (resp. inj) dim $= 0$. It is convenient to set proj (or inj) dim (0) equal to $-\infty$. If M is a right R-module, it is an R^{op}-module and so it has proj (and inj) dimension as R^{op}-module. Therefore, it makes sense to include R in the notation and we'll write $\dim_R M$ for the projective or injective dimension of M (as R-module) when no confusion can arise.

By this time, the following propositions, characterizing the various dimensions, are all routine to prove. So, we'll omit all the proofs leaving them as (DX's).

Proposition 5.68 *If R is a ring and M is an R-module, then the following are equivalent conditions:*

(1) M has projective dimension $\leq n$ (here, $n \geq 0$)

(2) $\mathrm{Ext}^{n+1}_R(M, -) = (0)$

(3) $\mathrm{Ext}^n_R(M, -)$ *is a right exact functor*

(4) If $0 \longrightarrow X_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ *is an acyclic resolution of M and if $P_0, \ldots, P_{n-1}$ are R-projective, then X_n is also R-projective*

Also, the following four conditions are mutually equivalent:

(1′) M has injective dimension $\leq n$ (here, $n \geq 0$)

(2′) $\mathrm{Ext}^{n+1}_R(-, M) = (0)$

(3′) $\mathrm{Ext}^n_R(-, M)$ *is a right exact functor*

(4′) If $0 \longrightarrow M \longrightarrow Q^0 \longrightarrow \cdots \longrightarrow Q^{n-1} \longrightarrow X^n \longrightarrow 0$ *is an acyclic resolution of M and if $Q^0, \ldots, Q^{n-1}$ are R-injective, then X^n is also R-injective.*

If we use the long exact sequence of (co)homology, we get a corollary of the above:

Corollary 5.69 *Say* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *is an exact sequence of R-modules.*

(1) If $\dim_R M'$ *and* $\dim_R M'' \leq n$ *(either both projective or both injective dimension), then* $\dim_R M \leq n$

(2) Suppose M is projective, then either

(a) $\dim_R M'' = 0$ *(i.e., M'' is projective), in which case M' is also projective; or*

(b) $\dim_R M'' \geq 1$*, in which case* $\dim_R M' = \dim_R M'' - 1$.

To get an invariant of the underlying ring, R, we ask for those n for which $\mathrm{projdim}_R M \leq n$ (resp. $\mathrm{injdim}_R M \leq n$) for *all* R-modules M. For such an n, we write $\mathrm{gldim}\, R \leq n$ and say the *global dimension of R is less than or equal to n*. (It will turn out that we can check this using either projdim for all M or injdim for all M; so, no confusion can arise.) Of course, the infimum of all n so that $\mathrm{gldim}\, R \leq n$ is called the *global dimension of R*. When we use right R-modules, we are using R^{op}-modules and so are computing $\mathrm{gldim}\, R^{\mathrm{op}}$.

Notice that $\operatorname{gldim} R$ is an invariant computed from the category of R-modules. So, *if R and S are rings and if there is an equivalence of categories R-mod $\approx$ S-mod, then* $\operatorname{gldim} R = \operatorname{gldim} S$. Rings for which R-mod $\approx$ S-mod are called *Morita equivalent rings*. For commutative rings, it turns out that Morita equivalence is just isomorphism; this is not true for non-commutative rings. Indeed, if R is a ring and $M_n(R)$ denotes, as usual, the ring of $n \times n$ matrices over R, then $R \approx M_n(R)$. Moreover, this is almost the full story. Also, if $R \approx S$, then $R^{\mathrm{op}} \approx S^{\mathrm{op}}$. Now for a field, K, we clearly have $\operatorname{gldim} K = 0$; so, we find $\operatorname{gldim} M_n(K) = 0$, as well. If A is a commutative ring and G is a group, then the map $\sigma \mapsto \sigma^{-1}$ gives an isomorphism of $A[G]$ onto $A[G]^{\mathrm{op}}$. Hence, $\operatorname{gldim} A[G] = \operatorname{gldim} A[G]^{\mathrm{op}}$.

Proposition 5.70 *Let R be a ring and let n be a non-negative integer. Then the following statements are equivalent:*

(1) Every R-module, M, has $\operatorname{projdim}_R \leq n$.

(2) Every R-module, M, has $\operatorname{injdim}_R \leq n$.

(3) $\operatorname{gldim} R \leq n$.

(4) $\operatorname{Ext}^t_R(-,-) = (0)$ *for all* $t > n$.

(5) $\operatorname{Ext}^{n+1}_R(-,-) = (0)$.

(6) $\operatorname{Ext}^n_R(-,-)$ *is right-exact.*

A ring R is called *semi-simple* if and only if every submodule, N, of each R-module, M, possesses an R-complement. (We say M is *completely reducible.*) That is, iff given $N \subseteq M$, there is a submodule $\widetilde{N} \subseteq M$ so that the natural map $N \coprod \widetilde{N} \longrightarrow M$ is an isomorphism (of R-modules). Of course each field, K, or division ring, D, is semi-simple. But, again, semi-simplicity is a property of the category R-mod; so $M_n(K)$ and $M_n(D)$ are also semi-simple. It is a theorem of Maschke that if K is a field, G is a finite group, and $(\operatorname{ch}(K), \#(G)) = 1$, then the group algebra, $K[G]$, is semi-simple. See Problem 134 for this result. Again, there are many equivalent ways to characterize semi-simplicity:

Proposition 5.71 *For any ring, R, the following statements are equivalent:*

(1) R is semi-simple.

(2) R^{op} is semi-simple.

(3) R, as R-module, is a coproduct of simple R-modules.

(4) R, as R-module, is completely reducible.

(5) Each (left) ideal of R is an injective module.

(6) Every R-module is completely reducible.

(7) In R-mod, every exact sequence splits.

(8) Every R-module is projective.

(9) Every R-module is injective.

(10) $\operatorname{gldim} R = 0$.

The proofs of these equivalences will be left as the material of Problem 145. Note that dimension is defined using $\mathrm{Ext}^\bullet_R(-,-)$ and $\mathrm{Tor}^R_\bullet$ is not mentioned. There are two reasons for this. First, while Hom, Ext, projective and injective are properties of abelian categories, tensor and Tor are generally not. Second, the vanishing of Tor characterizes flatness which is a weaker property than projectivity. However, for commutative rings, the notions of dimension and global dimension are frequently reduced by localization to the case of local rings. For noetherian local rings, we already know flatness and freeness are equivalent for f.g. modules; so over noetherian local rings the vanishing of Tor is connected with dimension (at least on the category of f.g. modules). In the general case, when we use Tor, we call the resulting invariant the Tor-*dimension*. It's easy to see that when R is a PID we have $\mathrm{gldim}\, R \leq 1$.

For our main applications of the Koszul complex, we return to the situation of a pair (R, Q) in which R is a ring and $\epsilon\colon R \to Q$ is a *surjective* R-module map. Such a pair is an *augmented ring*, the map ϵ is the augmentation (as discussed in Section 5.3) and Q is the *augmentation module*. As usual, write I for the augmentation ideal (just a left ideal, in general): $I = \mathrm{Ker}\, \epsilon$. Then the exact sequence

$$0 \longrightarrow I \longrightarrow R \xrightarrow{\epsilon} Q \longrightarrow 0$$

and Corollary 5.69 above show:

Either Q is projective (so that I is projective) or $1 + \dim_R I = \dim_R Q$.

Note that if R is commutative then I is a 2-sided ideal and Q becomes a ring if we set $\epsilon(r)\cdot\epsilon(p) = r\cdot\epsilon(p)$; i.e., if we make ϵ a ring homomorphism. The map ϵ is then a section in case R is a Q-algebra. Here is the main result on which our computations will be based.

Theorem 5.72 *Assume (R, Q) is an augmented ring and suppose I is finitely generated (as R-ideal) by elements $f_1, \ldots, f_r$* **which commute with each other**. *If $f_1, \ldots, f_r$ form an R-regular sequence, then $\dim_R Q = r$ (if $Q \neq (0)$). In particular,* $\mathrm{gldim}\, R \geq r$.

Proof. Write A for the commutative ring $\mathbb{Z}[T_1, \ldots, T_r]$, then as the $f_1, \ldots, f_r$ commute with each other, R becomes an A-module if we make T_j operate *via* $\rho T_j = \rho f_j$ for all $\rho \in R$. We form the Koszul complex $K_\bullet(\overrightarrow{T})$ for A and then form $R \otimes_A K_\bullet(\overrightarrow{T})$. The latter is clearly the Koszul complex $K_\bullet(\overrightarrow{f}, R)$ and as $(f_1, \ldots, f_r)$ is an R-regular sequence, $K_\bullet(\overrightarrow{f}, R)$ is acyclic. Thus, we obtain the exact sequence

$$0 \longrightarrow R \xrightarrow{\partial_r} \bigwedge^{r-1}(R^r) \xrightarrow{\partial_{r-1}} \cdots \xrightarrow{\partial_2} \bigwedge^{1}(R^r) \xrightarrow{\partial_1} R \longrightarrow Q \longrightarrow 0 \qquad (*)$$

because we know the image of ∂_1 is the (left) ideal generated by $f_1, \ldots, f_r$; that is, $\mathrm{Im}\, \partial_1 = I$. Now $(*)$ is visibly an R-projective resolution of Q and so $\dim_R Q \leq r$.

Since $(*)$ is an R-projective resolution of Q, we can use it to compute $\mathrm{Ext}^\bullet_R(Q, -)$. In particular, we can compute $\mathrm{Ext}^\bullet_R(Q, Q)$—this is the cohomology of the complex $\mathrm{Hom}_R((*), Q)$. But, the latter complex is just $K^\bullet(\overrightarrow{f}, Q)$. We find

$$\mathrm{Ext}^r_R(Q, Q) = H^r(\overrightarrow{f}, Q) = Q$$

and so $\dim_R Q = r$ provided $Q \neq (0)$. □

Corollary 5.73 *If K is a ring (not necessarily commutative) and R is the graded ring $K[T_1, \ldots, T_r]$, then $\dim_R K = r$. If K is a field or division ring and R is the local ring of formal power series $K[[T_1, \ldots, T_r]]$, then $\dim_R K = r$. (This is also true if K is any ring though R may not be local.) Lastly, if K is a field complete with respect to a valuation and R is the local ring of converging power series $K\{T_1, \ldots, T_r\}$, then $\dim_R K = r$. In all these cases,* $\mathrm{gldim}\, R \geq r$.

Proof. In each case, the variables $T_1, \ldots, T_r$ play the role of the $f_1, \ldots, f_r$ of our theorem; all hypotheses are satisfied. □

Notice that for $A\,(= \mathbb{Z}[T_1, \ldots, T_r])$, the Koszul resolution

$$0 \longrightarrow A \longrightarrow \bigwedge^{r-1}(A^r) \longrightarrow \cdots \bigwedge^{1}(A^r) \longrightarrow A \longrightarrow \mathbb{Z} \longrightarrow 0 \qquad (**)$$

can be used to compute $\mathrm{Tor}^A_\bullet(-, \mathbb{Z})$ as well as $\mathrm{Ext}^\bullet_A(\mathbb{Z}, -)$. So for M, any A-module,

$$\mathrm{Tor}^A_p(M, \mathbb{Z}) = H_p(\overrightarrow{T}, M) \quad \text{and} \quad \mathrm{Ext}^p_A(\mathbb{Z}, M) = H^p(\overrightarrow{T}, M).$$

By Koszul duality,

$$\mathrm{Tor}^A_p(M, \mathbb{Z}) \cong \mathrm{Ext}^{r-p}_A(\mathbb{Z}, M).$$

Further, the acyclicity of $M \otimes_A K_\bullet(\overrightarrow{T})$ is equivalent with $\mathrm{Tor}^A_p(M, \mathbb{Z}) = (0)$ when $p > 0$.

Now, recall that, for a ring R possessing a section $R \xrightarrow{\epsilon} K$ (here, R is a K-algebra), we defined the homology and cohomology "bar" groups by

$$\begin{aligned} \overline{H}_n(R, M) &= \mathrm{Tor}^R_n(M, K) \qquad (M \text{ an } R^{\mathrm{op}}\text{-module}) \\ \overline{H}^n(R, M) &= \mathrm{Ext}^n_R(K, M) \qquad (M \text{ an } R\text{-module}). \end{aligned}$$

In the cases

(1) $R = K[T_1, \ldots, T_r]$

(2) $R = K[[T_1, \ldots, T_r]]$

(3) $R = K\{T_1, \ldots, T_r\}$ $\quad (K$ has a topology),

our discussion above shows that

$$\overline{H}_n(R, M) = H_n(\overrightarrow{T}, M) \quad \text{and} \quad \overline{H}^n(R, M) = H^n(\overrightarrow{T}, M).$$

So, by the Hochschild (co)homology comparison theorem (Theorem 5.29), we see that *the Hochschild groups* $H_n(R, \epsilon_*(M))$ *and* $H^n(R, \epsilon_*^{\mathrm{op}}(M))$ *can be computed by the Koszul complexes* $K_\bullet(\overrightarrow{T}, M)$ *and* $K^\bullet(\overrightarrow{T}, M)$ *in cases (1)–(3) above*. This is what we alluded to at the end of the discussion following Theorem 5.29.

We now face the problem of the global dimension of a ring R. We assume R is not only an augmented ring (with augmentation module, Q, and ideal, I) but in fact *that I is a two-sided ideal so that Q is a ring and $\epsilon\colon R \to Q$ is a ring homomorphism*. Experience shows that for certain types of rings some subclasses of modules have more importance than others. For example, if R is a graded ring, the graded modules are the important ones for these are the ones giving rise to sheaves over the geometric object corresponding to R (a generalized projective algebraic variety) and the cohomology groups of these sheaves are geometric invariants of the object in question. Again, if R is a (noetherian) local ring, the finitely generated modules are the important ones as we saw in Chapter 3. It makes sense therefore to compute the global dimension of R with respect to the class of "important" R-modules, that is to define

$$\mathcal{I}\text{-gldim}\, R = \inf\{m \mid \mathcal{I}\text{-gldim}_R \leq m\},$$

where $\mathcal{I}\text{-gldim}_R \leq m$ iff for every *important* module, M, we have $\dim_R M \leq m$; (here, $\mathcal{I}$–stands for "important").

Eilenberg ([9]) abstracted the essential properties of the graded and finitely generated modules to give an axiomatic treatment of the notion of the class of "important" modules. As may be expected, the factor

ring, Q, plays a decisive role. Here is the abstract treatment together with the verification that for graded (resp. local) rings, the graded (resp. finitely generated) modules satisfy the axioms.

(A) Call an R^{op}-module, M, *pertinent* provided $M \otimes_R Q \neq (0)$ when $M \neq (0)$; also (0) is to be pertinent.

If R is a graded ring, say $R = \coprod_{j\geq 0} R_j$, then we set $I = R^{(+)} = \coprod_{j>0} R_j$ and $Q = R_0$. *When M is a graded R^{op}-module with* **grading bounded below** *then M is pertinent.* For we have $M = \coprod_{n\geq B} M_n$; so, $MI = \coprod_{n\geq B+1} M_n \neq M$. But $M \otimes_R Q = M/MI$. When R is a local ring, we set $I = \mathfrak{M}_R$ (its maximal ideal) and then $Q = \kappa(R)$–the residue field. Of course, *all f.g. R^{op}-modules are pertinent* by Nakayama's Lemma.

If S is a subset of a module, M, write $F(S)$ for the free R (or R^{op})-module generated by S. Of course, there's a natural map $F(S) \longrightarrow M$ and we get an exact sequence

$$0 \longrightarrow \mathrm{Ker}\,(S) \longrightarrow F(S) \longrightarrow M \longrightarrow \mathrm{cok}(S) \longrightarrow 0.$$

(B) The subset, S, of M is *good* provided $0 \in S$ and for each $T \subseteq S$, in the exact sequence

$$0 \longrightarrow \mathrm{Ker}\,(T) \longrightarrow F(T) \longrightarrow M \longrightarrow \mathrm{cok}(T) \longrightarrow 0,$$

the terms $\mathrm{Ker}\,(T)$ and $\mathrm{cok}(T)$ are pertinent.

Notice right away that free modules are pertinent; so, if S is good and we take $\{0\} = T$, then, as the map $F(\{0\}) \longrightarrow M$ is the zero map, we find $M = \mathrm{cok}(\{0\})$ and therefore M is pertinent. That is, any module possessing a good subset is automatically pertinent. Conversely, if M is pertinent, then clearly $S = \{0\}$ is a good subset; so, we've proved

Proposition 5.74 *If R is an augmented ring and I is two-sided, the following are equivalent conditions on an R^{op}-module, M:*

(a) M possesses a good subset

(b) M is pertinent

(c) $\{0\}$ is a good subset of M.

In the case that R is a graded ring, *we shall restrict all attention to modules whose homogeneous elements (if any) have degrees bounded below. In this case, any set $S \subseteq M$ consisting of* 0 *and homogeneous elements is good.* For suppose $T \subseteq S$, then we grade $F(T)$ by the requirement that $F(T) \longrightarrow M$ be a map of degree zero (remember; M is graded and, further, observe if $0 \in T$ it goes to 0 in M and causes no trouble). But then, $\mathrm{Ker}\,(T)$ and $\mathrm{cok}(T)$ are automatically graded (with grading bounded below) and so are pertinent. If R^{op} is a noetherian local ring and M is a finitely generated R^{op}-module, then *any finite set containing* 0 *is good*. For if S is finite, then any $T \subseteq S$ is also finite and so all of $F(T)$, M, $\mathrm{cok}(T)$ are f.g. But since R^{op} is noetherian, $\mathrm{Ker}\,(T)$ is also f.g.

(C) A family, $\mathcal{F}$, of R^{op}-modules is *a class of important modules* provided

(1) If $M \in \mathcal{F}$ it has a good set S which generates M, and

(2) In the exact sequence

$$0 \longrightarrow \mathrm{Ker}\,(S) \longrightarrow F(S) \longrightarrow M \longrightarrow 0$$

resulting from (1), we have $\mathrm{Ker}\,(S) \in \mathcal{F}$.

For graded rings, R, *the graded modules (whose degrees are bounded below) form an important family*. This is easy since such modules are always generated by their homogeneous (= good) elements and $\mathrm{Ker}\,(S)$ is clearly graded and has degrees bounded below. In the case that R is noetherian local, *the family of all f.g. modules is important*. Again, this is easy as such modules are generated by finite (= good) sets and $\mathrm{Ker}\,(S)$ is again f.g. because R is noetherian.

In what follows, one should keep in mind the two motivating examples and the specific translations of the abstract concepts: pertinent modules, good sets of elements, the class of important modules.

Abstract R	**R graded**	**R noetherian local**
pertinent module	graded module with degrees bounded below	finitely generated module
good subset of a module	subset of homogeneous elements of a module	finite subset of module
class of important modules	class of graded modules with degrees bounded below	class of finitely generated modules

Since we have abstracted the local case, it is no surprise that we have a "generalized Nakayama's Lemma":

Proposition 5.75 *(Generalized Nakayama's Lemma) If (R, Q) is an augmented ring with I a two-sided ideal, then for any good subset, S, of an R^{op}-module, M, whenever the image of $S - \{0\}$ in $M \otimes_R Q$ generates $M \otimes_R Q$ as Q^{op}-module the set $S - \{0\}$ generates M. Moreover, if $\mathrm{Tor}_1^R(M, Q) = (0)$, and the image of $S - \{0\}$ freely generates $M \otimes_R Q$ as Q^{op}-module, then $S - \{0\}$ freely generates M as R^{op}-module.*

Proof. The proof is practically identical to the usual case (write S instead of $S - \{0\}$): We have the exact sequence

$$0 \longrightarrow \mathrm{Ker}\,(S) \longrightarrow F(S) \xrightarrow{\varphi} M \longrightarrow \mathrm{cok}(S) \longrightarrow 0,$$

and we tensor with Q. We obtain the exact sequence

$$F(S) \otimes_R Q \xrightarrow{\overline{\varphi}} M \otimes_R Q \longrightarrow \mathrm{cok}(S) \otimes_R Q \longrightarrow 0$$

and we've assumed $\overline{\varphi}$ is surjective. Thus $\mathrm{cok}(S) \otimes_R Q = (0)$, yet $\mathrm{cok}(S)$ is pertinent; so $\mathrm{cok}(S) = (0)$. Next, our original sequence has become

$$0 \longrightarrow \mathrm{Ker}\,(S) \longrightarrow F(S) \longrightarrow M \longrightarrow 0,$$

so we can tensor with Q again to obtain

$$\mathrm{Tor}_1^R(M, Q) \longrightarrow \mathrm{Ker}\,(S) \otimes_R Q \longrightarrow F(S) \otimes_R Q \xrightarrow{\overline{\varphi}} M \otimes_R Q \longrightarrow 0.$$

Since, in the second part, we've assume $\overline{\varphi}$ is an isomorphism and $\mathrm{Tor}_1^R(M, Q) = (0)$, we get $\mathrm{Ker}\,(S) \otimes_R Q = (0)$. But, $\mathrm{Ker}\,(S)$ is also pertinent and so $\mathrm{Ker}\,(S) = (0)$. □

If we specialize Q, we get the following:

Corollary 5.76 *With (R, Q) as in the generalized Nakayama's Lemma and assuming Q is a (skew) field,*[8] *we have the following equivalent conditions for an R^{op}-module, M, which is generated by a good set:*

(1) M is free over R^{op}

(2) M is R^{op}-flat

(3) $\mathrm{Tor}_n^R(M, Q) = (0)$ if $n > 0$

(4) $\mathrm{Tor}_1^R(M, Q) = (0)$.

Moreover, under these equivalent conditions, every good generating set for M contains an R^{op}-basis for M.

Proof. (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) are trivial or are tautologies.

(4) $\Longrightarrow$ (1). The image, $\overline{S}$, of our good generating set generates $M \otimes_R Q$. But, Q is a (skew) field; so $\overline{S}$ contains a basis and this has the form $\overline{T}$ for some $T \subseteq S$. Then $T \cup \{0\}$ is good and (4) with generalized Nakayama shows T is an R^{op}-basis for M. This gives (1) and even proves the last asssertion. □

Finally, we have the abstract $\mathcal{I}$-gldim theorem, in which $\mathcal{I}$ is a class of important modules.

[8] A skew field is a division ring.

Theorem 5.77 *($\mathcal{I}$-Global Dimension Theorem) If (R, Q) is an augmented ring in which $\mathrm{Ker}\,(R \xrightarrow{\epsilon} Q)$ is a two-sided ideal, if Q is a (skew) field and if $\mathcal{I}$ is an important class of R^{op}-modules, then*

$$\mathcal{I}\text{-gldim}\, R^{\mathrm{op}} \leq \dim_R Q \qquad (\textit{proj. dim}).$$

Proof. Of course, w.m.a. $\dim_R Q < \infty$ else there is nothing to prove; so, write $n = \dim_R Q$. The proof is now practically forced, namely pick an important R^{op}-module, M, then by assumption there is a good generating set, S_0, in M and an exact sequence

$$0 \longrightarrow \mathrm{Ker}\,(S_0) \longrightarrow F(S_0) \longrightarrow M \longrightarrow 0.$$

Also, $\mathrm{Ker}\,(S_0)$ is important so, there's a good generating set, S_1, in $\mathrm{Ker}\,(S_0)$ and an exact sequence

$$0 \longrightarrow \mathrm{Ker}\,(S_1) \longrightarrow F(S_1) \longrightarrow \mathrm{Ker}\,(S_0) \longrightarrow 0$$

in which $\mathrm{Ker}\,(S_1)$ is again important. We repeat and obtain the chain of exact sequences

$$\left.\begin{array}{c} 0 \longrightarrow \mathrm{Ker}\,(S_0) \longrightarrow F(S_0) \longrightarrow M \longrightarrow 0 \\ 0 \longrightarrow \mathrm{Ker}\,(S_1) \longrightarrow F(S_1) \longrightarrow \mathrm{Ker}\,(S_0) \longrightarrow 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ 0 \longrightarrow \mathrm{Ker}\,(S_t) \longrightarrow F(S_t) \longrightarrow \mathrm{Ker}\,(S_{t-1}) \longrightarrow 0 \end{array}\right\} \qquad (\dagger)$$

for all t. Upon splicing these sequences, we get the exact sequence

$$0 \longrightarrow \mathrm{Ker}\,(S_t) \longrightarrow F(S_t) \longrightarrow F(S_{t-1}) \longrightarrow \cdots \longrightarrow F(S_1) \longrightarrow F(S_0) \longrightarrow M \longrightarrow 0. \qquad (\dagger\dagger)$$

Now in the sequence

$$0 \longrightarrow \mathrm{Ker}\,(S_t) \longrightarrow F(S_t) \longrightarrow \mathrm{Ker}\,(S_{t-1}) \longrightarrow 0$$

($t \geq 0$ and $\mathrm{Ker}\,(S_{-1}) = M$), we compute Tor and find

$$\cdots \longrightarrow \mathrm{Tor}^R_{r+1}(F(S_t), Q) \longrightarrow \mathrm{Tor}^R_{r+1}(\mathrm{Ker}\,(S_{t-1}), Q) \longrightarrow \mathrm{Tor}^R_r(\mathrm{Ker}\,(S_t), Q) \longrightarrow \mathrm{Tor}^R_r(F(S_t), Q) \longrightarrow \cdots$$

for all $r \geq 1$ and $t \geq 0$; hence the isomorphisms

$$\mathrm{Tor}^R_{r+1}(\mathrm{Ker}\,(S_{t-1}), Q) \cong \mathrm{Tor}^R_r(\mathrm{Ker}\,(S_t), Q).$$

Take $r = 1$ and $t = n - 1$, then

$$\mathrm{Tor}^R_2(\mathrm{Ker}\,(S_{n-2}), Q) \cong \mathrm{Tor}^R_1(\mathrm{Ker}\,(S_{n-1}), Q)$$

and similarly

$$\mathrm{Tor}^R_3(\mathrm{Ker}\,(S_{n-3}), Q) \cong \mathrm{Tor}^R_2(\mathrm{Ker}\,(S_{n-2}), Q),$$

etc. We find

$$\mathrm{Tor}^R_{n+1}(\mathrm{Ker}\,(S_{-1}), Q) \cong \mathrm{Tor}^R_1(\mathrm{Ker}\,(S_{n-1}), Q). \qquad (\dagger\dagger\dagger)$$

But, $\dim_R Q = n$ and so $\mathrm{Tor}^R_{n+1}(-, Q) = (0)$; thus,

$$\mathrm{Tor}^R_1(\mathrm{Ker}\,(S_{n-1}), Q) = (0).$$

Now $\mathrm{Ker}\,(S_{n-1})$ is important and the corollary to Generalized Nakayama shows that $\mathrm{Ker}\,(S_{n-1})$ is R^{op}-free. Thus,

$$0 \longrightarrow \mathrm{Ker}\,(S_{n-1}) \longrightarrow F(S_{n-1}) \longrightarrow \cdots \longrightarrow \mathrm{Ker}\,(S_1) \longrightarrow F(S_0) \longrightarrow M \longrightarrow 0$$

is a free resolution (length n) of M and this proves $\dim_{R^{\mathrm{op}}}(M) \leq n$. But, M is arbitrary and we're done. □

Notice that the above argument is completely formal except at the very last stage where we used the vanishing of $\mathrm{Tor}^R_{n+1}(-, Q)$. But, this vanishing holds if $\mathrm{Tor}^R\text{-dim}(Q) \leq n$ and therefore we've actually proved the following stronger version of the $\mathcal{I}$-global dimension theorem:

Corollary 5.78 *Under the hypotheses of the $\mathcal{I}$-global dimension theorem, we have the strong $\mathcal{I}$-global dimension inequality*

$$\mathcal{I}\text{-gldim}(R^{\mathrm{op}}) \leq \mathrm{Tor}^R\text{-dim}(Q).$$

To recapitulate and set these ideas firmly in mind, here are the two special, motivating cases:

Theorem 5.79 *(Syzygy[9] Theorem) Assume of the ring R that either*

(I) R is graded; $R = Q \amalg R_1 \amalg R_2 \amalg \cdots$, and Q is a (skew) field,

or

(II) R is local with R^{op} noetherian and $Q = \kappa(R)$ is a (skew) field.

Then, when $\mathcal{I}$ is, in case (I), the class of graded R^{op}-modules with degrees bounded below, or in case (II), the class of finitely generated R^{op}-modules, we have

$$\mathcal{I}\text{-gldim}(R^{\mathrm{op}}) \leq \mathrm{Tor}^R\text{-dim}(Q).$$

Moreover, either Q is projective or else if $\mathfrak{A}$ is any R^{op}-ideal (which in case (I) is homogeneous), then we have

$$1 + \dim_{R^{\mathrm{op}}}(\mathfrak{A}) \leq \dim_R(Q).$$

In case (I) of the Syzygy Theorem, note that Q is an R^{op}-module, too and that $\mathcal{I}$ can be taken to be the class of graded (with degrees bounded below) R-modules. Therefore, $\dim_{R^{\mathrm{op}}}(Q) \leq \mathrm{Tor}^R\text{-dim}(Q) \leq \dim_R(Q)$. Interchanging R and R^{op} as we may, we deduce

Corollary 5.80 *In case (I) of the Syzygy Theorem, we have*

(a) $\dim_R(Q) = \dim_{R^{\mathrm{op}}}(Q) = \mathrm{Tor}^R\text{-dim}(Q) = \mathrm{Tor}^{R^{\mathrm{op}}}\text{-dim}(Q)$,

(b) $\mathcal{I}\text{-gldim}(R) \leq \mathrm{Tor}^R\text{-dim}(Q)$,

(c) $1 + \dim_R(\mathfrak{A}) \leq \dim_R(Q)$ *if Q is not projective.*

Similarly, in case (II) of the Syzygy Theorem, provided we assume R noetherian, $\mathcal{I}$ is again the family of f.g. R-modules when we interchange R and R^{op}. There results

Corollary 5.81 *If R is local with both R and R^{op} noetherian, then*

(a) $\dim_R(\kappa(R)) = \dim_{R^{\mathrm{op}}}(\kappa(R)) = \mathrm{Tor}^R\text{-dim}(\kappa(R)) = \mathrm{Tor}^{R^{\mathrm{op}}}\text{-dim}(\kappa(R))$,

(b) $\mathcal{I}\text{-gldim}(R) \leq \mathrm{Tor}^R\text{-dim}(\kappa(R))$,

(c) $1 + \dim_R(\mathfrak{A}) \leq \mathrm{Tor}^R\text{-dim}(\kappa(R))$.

Finally, there are the cases that appeared first in the literature:

Corollary 5.82 *If K is a (skew) field and*

(I) (Hilbert Syzygy Theorem) $R = K[T_1, \ldots, T_n]$ and M is a graded R-module with degrees bounded from below or $\mathfrak{A}$ is a homogeneous R-ideal then

$$\dim_R M \leq n \quad \textit{and} \quad \dim_R \mathfrak{A} \leq n - 1.$$

[9]The Greek (later Latin) derived word "syzygy" means a coupling, pairing, relationship. Thus, for the exact sequence $0 \longrightarrow \mathrm{Ker}\,(S) \longrightarrow F(S) \longrightarrow M \longrightarrow 0$, the generators of $\mathrm{Ker}\,(S)$ are relations among the generators of M and generate all such relations. For $0 \longrightarrow \mathrm{Ker}\,(S_1) \longrightarrow F(S_1) \longrightarrow \mathrm{Ker}\,(S) \longrightarrow 0$, generators of $\mathrm{Ker}\,(S_1)$ are relations among the relations and so on. Each of $\mathrm{Ker}\,(S_j)$ is a *syzygy module*.

or

(II) $R = K[[T_1, \ldots, T_n]]$ *(resp.* $R = K\{T_1, \ldots, T_n\}$ *when* K *has a non-discrete (valuation) topology) and* M *is a f.g.* R*-module while* $\mathfrak{A}$ *is an* R*-ideal, then*

$$\dim_R M \leq n \quad \textit{and} \quad \dim_R \mathfrak{A} \leq n - 1.$$

To prove these, we use the above and Theorem 5.72.

Remarks:

(1) Note that Q appears as the "worst" module, i.e., the one with the largest homological dimension. In the case of a commutative local ring, R, if $\mathfrak{M}$ is generated by an R-regular sequence (R is then called a *regular local ring*) of length n, we see that $\mathcal{I}$-gldim$(R) = n$ and $Q = \kappa(R)$ achieves this maximum dimension. The finiteness of global dimension turns out to be characteristic of regular local rings (Serre [46]).

(2) One might think of interchanging R and R^{op} in the general global dimension theorem. But this is not generally possible because the class of important modules usually does not behave well under this interchange. The trouble comes from the self-referential nature of $\mathcal{I}$. The R-module Q is an R^{op}-module, pertinence will cause no difficulty, nor will good subsets cause difficulty (in general). But, we need Ker (S) to be important in the sequence

$$0 \longrightarrow \mathrm{Ker}\,(S) \longrightarrow F(S) \longrightarrow M \longrightarrow 0$$

if M is to be important, so we cannot get our hands on how to characterize importance "externally" in the general case.

For the global dimension of R (that is, when $\mathcal{I} = R$-mod itself) we must restrict attention to more special rings than arbitrary augmented rings. Fix a *commutative* ring K and assume R is a K-algebra as in the Hochschild Theory of Section 5.3. An obvious kind of cohomological dimension is then the smallest n so that $H^{n+1}(R, M) = (0)$ for all $R^e\,(= R \otimes_K R^{\mathrm{op}})$-modules, M; where the cohomology is Hochschild cohomology. But, this is not a new notion because, by definition,

$$H^r(R, M) = \mathrm{Ext}^r_{R^e}(R, M).$$

Hence, the Hochschild cohomological dimension is exactly $\mathrm{projdim}_{R^e}(R)$. Let us agree to write $\dim_{R^e}(R)$ instead of $\mathrm{projdim}_{R^e}(R)$. It's important to know the behavior of $\dim_{R^e}(R)$ under base extension of K as well as under various natural operations on the K-algebra R. Here are the relevant results.

Proposition 5.83 *Suppose* R *is projective over* K *and let* L *be a commutative base extension of* K*. Then*

$$\dim_{(L \otimes_K R)^e}(L \otimes_K R) \leq \dim_{R^e}(R).$$

If L *is faithfully flat over* K*, equality holds.*

Remark: To explain the (perhaps) puzzling inequality of our proposition, notice that the dimension of R is as a K-algebra while that of $L \otimes_K R$ is as an L-algebra as befits base extension. So we might have written $\dim_{R^e}(R; K)$, *etc.* and then the inequality might not have been so puzzling–but, one must try to rein in excess notation.

Proof. A proof can be based on the method of maps of pairs as given in Section 5.3, but it is just as simple and somewhat instructive to use the associativity spectral sequence and associativity formula for Ext (cf.

Proposition 5.61). To this end, we make the following substitutions for the objects, K, R, S, T, A, B, C of that Proposition:

$$K \longrightarrow K,\ R \longrightarrow K,\ S \longrightarrow R^e,\ T \longrightarrow L,$$
$$A \longrightarrow R,\ B \longrightarrow L,\ C \longrightarrow M \quad \text{(an arbitrary } (L \otimes_K R)^e\text{-module)}.$$

Since R is projective over K, the abstract hypothesis: A (our R) is R (our K)-flat is valid and moreover B (our L) is T (again our L)-projective. Hence, the Ext associativity gives

$$\operatorname{Ext}^p_{R^e}(R, M) \cong \operatorname{Ext}^p_{(L\otimes_K R)^e}(L \otimes_K R, M)$$

because $S \otimes_K T$ is equal to $(L \otimes_K R)^e$. Now M is an L and an R^e-module; so, if $p > \dim_{R^e}(R)$ the left side vanishes and therefore so does the right side. But, M is arbitrary and the inequality follows. (One could also use Corollary 5.64).

We have an inequality simply because we cannot say that an arbitrary R^e-module is also an L-module. Now suppose L is faithfully flat as K-algebra, then L splits as K-*module* into $K\,(= K \cdot 1) \amalg V$ so that we have a K-morphism $\pi\colon L \to K$. The composition $K \overset{i}{\hookrightarrow} L \xrightarrow{\pi} K$ is the identity. If M is any R^e-module, then $L \otimes_K M$ is an R^e and an L-module and we may apply our above Ext associativity to $L \otimes_K M$. We find the isomorphism

$$\operatorname{Ext}^p_{R^e}(R, L \otimes_K M) \cong \operatorname{Ext}^p_{(L\otimes_K R)^e}(L \otimes_K R, L \otimes_K M). \tag{$*$}$$

However, the composition

$$M = K \otimes_K M \xhookrightarrow{i\otimes 1} L \otimes_K M \xrightarrow{\pi\otimes 1} K \otimes_K M = M$$

is the identity; so, applied to $(*)$ it gives

$$\operatorname{Ext}^p_{R^e}(R, M) \longrightarrow \operatorname{Ext}^p_{R^e}(R, L \otimes_K M) \longrightarrow \operatorname{Ext}^p_{R^e}(R, M) \tag{$**$}$$

whose composition is again the identity. If $p > \dim_{(L\otimes_K R)^e}(L \otimes_K R)$ the middle group is (0) and so $(**)$ shows $\operatorname{Ext}^p_{R^e}(R, M) = (0)$. M is arbitrary, therefore $\dim_{R^e}(R) \le \dim_{(L\otimes_K R)^e}(L \otimes_K R)$. □

Of course, faithful flatness is always true if K is a field; so, we find

Corollary 5.84 *If K is a field and R is a K-algebra, then for any commutative K-algebra, L, we have*

$$\dim_{R^e}(R) = \dim_{(L\otimes_K R)^e}(L \otimes_K R).$$

In particular, the notion of dimension is "geometric", i.e., it is independent of the field extension.

If we're given a pair of K-algebras, say R and S, then we get two new K-algebras $R \prod S$ and $R \otimes_K S$. Now, consider $R \prod S$. It has the two projections pr_1 and pr_2 to R and S and so we get the two functors pr_1^* and pr_2^* from R-mod (resp. S-mod) to $R \prod S$ – mod. If M is an $R \prod S$-module, then we get two further functors

$$pr_{1*}\colon R \prod S - \text{mod} \rightsquigarrow R\text{-mod}$$
$$pr_{2*}\colon R \prod S - \text{mod} \rightsquigarrow S\text{-mod}$$

via $M \rightsquigarrow (1,0)M$ (resp. $(0,1)M$). Observe that $pr_i^*(pr_{i*}M)$ is naturally an $R \prod S$-submodule of M, therefore we have two functors

$$F\colon R\text{-mod} \prod S\text{-mod} \rightsquigarrow R \prod S - \text{mod}$$

via

$$F(M, \widetilde{M}) = pr_1^* M \amalg pr_2^* \widetilde{M} \quad (\text{in } R \prod S - \text{mod})$$

and

$$G\colon R \prod S - \text{mod} \rightsquigarrow R\text{-mod} \prod S\text{-mod}$$

via

$$G(M) = (pr_{1_*} M, pr_{2_*} M);$$

the above shows that F *and* G *establish an equivalence of categories*

$$R \prod S - \text{mod} \approx R\text{-mod} \prod S\text{-mod}.$$

If $T = R \prod S$, then $T^e = R^e \prod S^e$; so, applying the above, we get the category equivalence

$$T^e\text{-mod} = R^e \prod S^e - \text{mod} \approx R^e\text{-mod} \prod S^e\text{-mod}.$$

Then, obvious arguments show that

$$H^p(R \prod S, M) \cong H^p(R, pr_{1_*} M) \amalg H^p(S, pr_{2_*} M)$$

(where, M is an $(R \prod S)^e$-module). This proves the first statement of

Proposition 5.85 *Suppose R and S are K-algebras and R is K-projective then*

$$\dim_{(R \prod S)^e}(R \prod S) = \max(\dim_{R^e}(R), \dim_{S^e}(S))$$

and

$$\dim_{(R \otimes S)^e}(R \otimes S) \leq \dim_{R^e}(R) + \dim_{S^e}(S).$$

Proof. For the second statement, we have the spectral sequence (of Corollary 5.64)

$$H^p(R, H^q(S, M)) \Longrightarrow H^\bullet(R \otimes_K S, M).$$

Exactly the same arguments as used in the Tower Theorem (Theorem 5.2) for the Hochschild-Serre spectral sequence finish the proof. □

Remark: The K-projectivity of R is only used to prove the inequality for $R \otimes_K S$.

We can go further using our spectral sequences.

Theorem 5.86 *Suppose R is a K-projective K-algebra, then*

$$\text{gldim}\, R^e \leq \dim_{R^e}(R) + \text{gldim}(R).$$

Further,

$$\text{gldim}(R) \leq \dim_{R^e}(R) + \text{gldim}\, K$$

and

$$\text{gldim}(R^{\text{op}}) \leq \dim_{R^e}(R) + \text{gldim}\, K.$$

Proof. We apply the spectral sequence

$$E_2^{p,q} = H^p(R, \mathrm{Ext}_T^q(B,C)) \Longrightarrow \mathrm{Ext}^\bullet_{R^{\mathrm{op}} \otimes_K T}(B,C)$$

of Corollary 5.62. Here, B and C are left R and right T-modules (and, in the $\mathrm{Ext}^\bullet$ of the ending, they are viewed as right $R^{\mathrm{op}} \otimes_K T$-modules, or left $R \otimes_K T^{\mathrm{op}}$-modules). We set $T = R$ and see that

$$\mathrm{Ext}_R^q(B,C) = (0) \quad \text{when} \quad q > \mathrm{gldim}(R).$$

But,

$$H^p(R,-) = \mathrm{Ext}^p_{R^e}(R,-)$$

and so

$$H^p(R,-) = (0) \quad \text{when} \quad p > \dim_{R^e}(R).$$

Therefore, $E_2^{p,q} = (0)$ when $p + q > \dim_{R^e}(R) + \mathrm{gldim}(R)$. Once again, exactly as in the Tower Theorem, we conclude $\mathrm{Ext}^n_{R \otimes_K R^{\mathrm{op}}}(B,C)$ vanishes for $n > \dim_{R^e}(R) + \mathrm{gldim}(R)$. This proves the first inequality.

For the second and third inequalities, we merely set $T = K$. Then, $\mathrm{Ext}_K^q(B,C)$ vanishes for all $q > \mathrm{gldim}(K)$ and $H^p(R,-)$ vanishes for all $p > \dim_{R^e}(R) = \dim_{R^e}(R^{\mathrm{op}})$. Our spectral sequence argument now yields the two desired inequalities. □

Corollary 5.87 *If R is a projective K-algebra and R is semi-simple as K-algebra, then*

$$\mathrm{gldim}(R^e) = \dim_{R^e}(R).$$

If R is arbitrary but K is a semi-simple ring, then

$$\mathrm{gldim}(R) \leq \dim_{R^e}(R)$$

and

$$\mathrm{gldim}(R^{\mathrm{op}}) \leq \dim_{R^e}(R).$$

Proof. In the first inequality, $\mathrm{gldim}(R) = 0$, so

$$\mathrm{gldim}(R^e) \leq \dim_{R^e}(R).$$

The opposite inequality is always true by definition.

If now K is semi-simple, R is automatically K-projective; so, our other inequalities (of the theorem) finish the proof as $\mathrm{gldim}(K) = 0$. □

Corollary 5.88 *If K is semi-simple and R is a K-algebra, then R^e is semi-simple if and only if R is a projective R^e-module (i.e., $\dim_{R^e}(R) = 0$).*

Proof. Suppose $\dim_{R^e}(R) = (0)$. Then, by Corollary 5.87 above, $\mathrm{gldim}(R) = 0$, i.e., R is itself a semi-simple ring. But then we apply the corollary one more time and deduce $\mathrm{gldim}(R^e) = 0$. Conversely, if $\mathrm{gldim}(R^e) = 0$, then $\dim_{R^e}(R) = 0$. □

Corollary 5.89 *If K is semi-simple and if R^e is semi-simple, then R is semi-simple (as K-algebra).*

Proof. As $\mathrm{gldim}(R^e) = 0$ and K is semi-simple, we get $\dim_{R^e}(R) = 0$. But, $\mathrm{gldim}(R) \leq \dim_{R^e}(R)$; so, we are done. □

We can now put together the Koszul complex and the material above to prove

Theorem 5.90 *(Global Dimension Theorem) Suppose K is a commutative ring and write $R = K[T_1, \ldots, T_n]$. Then,*

$$\dim_{R^e}(R) = \dim_R(K) = n.$$

We have the inequality

$$n \leq \operatorname{gldim} R \leq n + \operatorname{gldim} K,$$

and so if K is a semi-simple ring (e.g., a field), then

$$\operatorname{gldim} R = n.$$

Proof. By the main application of the Koszul complex to dimension (Theorem 5.72) we have $\dim_R(K) = n$ and so $\operatorname{gldim} R \geq n$. Here, K is an R-module *via* sending all T_j to 0. But if $\widetilde{\epsilon}$ is *any* K-algebra map $R \longrightarrow K$, we can perform the automorphism $T_j \mapsto T_j - \widetilde{\epsilon}(T_j)$ and this takes $\widetilde{\epsilon}$ to the usual augmentation in which all $T_j \longrightarrow 0$. Therefore, we still have $\dim_R K = n$ (and $\operatorname{gldim} R \geq n$) when viewing K as R-module *via* $\widetilde{\epsilon}$.

Now $R^{\mathrm{op}} = R$; so, $R^e = R \otimes_K R$, and thus

$$R^e = K[T_1, \ldots, T_n, Z_1, \ldots Z_n] = R[Z_1, \ldots, Z_n].$$

(Remember that T_j stands for $T_j \otimes 1$ and Z_j for $1 \otimes T_j$). The standard augmentation $\eta\colon R^e \to R$ is given by $\rho \otimes \widetilde{\rho} \mapsto \rho\widetilde{\rho}$ and it gives a map

$$R^e = R[Z_1, \ldots, Z_n] \longrightarrow R,$$

in which Z_j goes to $T_j \in R$. The Z_j's commute and we can apply Theorem 5.72 again to get

$$\dim_{R^e}(R) = n.$$

Finally, Theorem 5.86 shows that

$$\operatorname{gldim}(R) \leq n + \operatorname{gldim} K.$$

□

Remark: The global dimension theorem is a substantial improvement of Hilbert's Syzygy Theorem. For one thing we need not have K a field (but, in the semi-simple case this is inessential) and, more importantly, we need not restrict to graded modules. Also, the role of the global dimension of K becomes clear.

5.6 Concluding Remarks

The apparatus of (co)homological methods and constructions and, more importantly, their manifold applications to questions and situations in algebra and geometry has been the constant theme of this chapter. Indeed, upon looking back to all earlier chapters from the first appearance of group cohomology as a computational tool to help with group extensions through the use of sequences of modules and Galois cohomology in field theory to the theory of derived functors and spectral sequences to obtain new, subtle invariants in algebra and geometry, we see a unified ever deepening pattern in this theme. The theme and pattern are a major development of the last sixty years of the twentieth century—a century in which mathematics flowered as never before. Neither theme nor pattern gives a hint of stopping and we have penetrated just to middling ground. So read on and work on.

5.7 Supplementary Readings

The classic reference on homological algebra is Cartan and Eilenberg [9]. One may also consult Mac Lane [36], Rotman [44], Weibel [48], Hilton and Stammback [24], Bourbaki [5], Godement [18] and Grothendieck [20]. For recent developments and many more references, see Gelfand and Manin's excellent books [16, 17]. For a global perspective on the role of homological algebra in mathematics, see Dieudonné [10].

Bibliography

[1] Emil Artin. *Galois Theory*. Dover, second edition, 1964.

[2] Michael Artin. *Algebra*. Prentice Hall, first edition, 1991.

[3] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison Wesley, third edition, 1969.

[4] Nicolas Bourbaki. *Algèbre, Chapitres 1-3*. Eléments de Mathématiques. Hermann, 1970.

[5] Nicolas Bourbaki. *Algèbre, Chapitre 10*. Eléments de Mathématiques. Masson, 1980.

[6] Nicolas Bourbaki. *Algèbre, Chapitres 4-7*. Eléments de Mathématiques. Masson, 1981.

[7] Nicolas Bourbaki. *Algèbre Commutative, Chapitres 8-9*. Eléments de Mathématiques. Masson, 1983.

[8] Nicolas Bourbaki. *Elements of Mathematics. Commutative Algebra, Chapters 1-7*. Springer–Verlag, 1989.

[9] Henri Cartan and Samuel Eilenberg. *Homological Algebra*. Princeton Math. Series, No. 19. Princeton University Press, 1956.

[10] Jean Dieudonné. *Panorama des matématiques pures. Le choix bourbachique*. Gauthiers-Villars, second edition, 1979.

[11] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, second edition, 1999.

[12] Albert Einstein. Zur Elektrodynamik bewegter Körper. *Annalen der Physik*, 17:891–921, 1905.

[13] David Eisenbud. *Commutative Algebra With A View Toward Algebraic Geometry*. GTM No. 150. Springer–Verlag, first edition, 1995.

[14] Jean-Pierre Escofier. *Galois Theory*. GTM No. 204. Springer Verlag, first edition, 2001.

[15] Peter Freyd. *Abelian Categories. An Introduction to the theory of functors*. Harper and Row, first edition, 1964.

[16] Sergei I. Gelfand and Yuri I. Manin. *Homological Algebra*. Springer, first edition, 1999.

[17] Sergei I. Gelfand and Yuri I. Manin. *Methods of Homological Algebra*. Springer, second edition, 2003.

[18] Roger Godement. *Topologie Algébrique et Théorie des Faisceaux*. Hermann, first edition, 1958. Second Printing, 1998.

[19] Daniel Gorenstein. *Finite Groups*. Harper and Row, first edition, 1968.

[20] Alexander Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Mathematical Journal*, 9:119–221, 1957.

[21] Alexander Grothendieck and Jean Dieudonné. Eléments de Géométrie Algébrique, IV: Etude Locale des Schémas et des Morphismes de Schémas (Première Partie). *Inst. Hautes Etudes Sci. Publ. Math.*, 20:1–259, 1964.

[22] Marshall Hall. *Theory of Groups*. AMS Chelsea, second edition, 1976.

[23] David Hilbert. Die Theorie der algebraischen Zahlkörper. *Jahresberich der DMV*, 4:175–546, 1897.

[24] Peter J. Hilton and Urs Stammbach. *A Course in Homological Algebra*. GTM No. 4. Springer, second edition, 1996.

[25] G. Hochschild. On the cohomology groups of an associative algebra. *Ann. of Math. (2)*, 46:58–67, 1945.

[26] G. Hochschild. On the cohomology theory for associative algebras. *Ann. of Math. (2)*, 47:568–579, 1946.

[27] Thomas W. Hungerford. *Algebra*. GTM No. 73. Springer Verlag, first edition, 1980.

[28] Nathan Jacobson. *Basic Algebra II*. Freeman, first edition, 1980.

[29] Nathan Jacobson. *Basic Algebra I*. Freeman, second edition, 1985.

[30] Daniel M. Kan. Adjoint functors. *Trans. Amer. Math. Soc.*, 87:294–329, 1958.

[31] Irving Kaplansky. *Fields and Rings*. The University of Chicago Press, second edition, 1972.

[32] Jean Pierre Lafon. *Les Formalismes Fondamentaux de l' Algèbre Commutative*. Hermann, first edition, 1974.

[33] Jean Pierre Lafon. *Algèbre Commutative. Languages Géométrique et Algébrique*. Hermann, first edition, 1977.

[34] Serge Lang. *Algebra*. Addison Wesley, third edition, 1993.

[35] Saunders Mac Lane. *Categories for the Working Mathematician*. GTM No. 5. Springer–Verlag, first edition, 1971.

[36] Saunders Mac Lane. *Homology*. Grundlehren der Math. Wiss., Vol. 114. Springer–Verlag, third edition, 1975.

[37] Saunders Mac Lane and Garrett Birkhoff. *Algebra*. Macmillan, first edition, 1967.

[38] M.-P. Malliavin. *Algèbre Commutative. Applications en Géométrie et Théorie des Nombres*. Masson, first edition, 1985.

[39] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, first edition, 1989.

[40] Barry Mitchell. The full embedding theorem. *Amer. J. Math.*, 86:619–637, 1964.

[41] Patrick Morandi. *Field and Galois Theory*. GTM No. 167. Springer Verlag, first edition, 1997.

[42] John S. Rose. *A Course on Group Theory*. Cambridge University Press, first edition, 1978.

[43] Joseph J. Rotman. *The Theory of Groups, An Introduction*. Allyn and Bacon, second edition, 1973.

[44] Joseph J. Rotman. *An Introduction to Homological Algebra*. Academic Press, first edition, 1979.

[45] Jean-Pierre Serre. *Corps Locaux*. Hermann, third edition, 1980.

[46] Jean-Pierre Serre. *Local Algebra*. Springer Monographs in Mathematics. Springer, first edition, 2000.

[47] B.L. Van Der Waerden. *Algebra, Vol. 1.* Ungar, seventh edition, 1973.

[48] Charles A. Weibel. *Introduction to Homological Algebra.* Studies in Advanced Mathematics, Vol. 38. Cambridge University Press, first edition, 1994.

[49] Ernst Witt. Zyklisch Körper und Algebren der Charakteristik p vom Grade p^m. *J. Reine Angew. Math.*, 176:126–140, 1937.

[50] Oscar Zariski and Pierre Samuel. *Commutative Algebra, Vol I.* GTM No. 28. Springer Verlag, first edition, 1975.

[51] Oscar Zariski and Pierre Samuel. *Commutative Algebra, Vol II.* GTM No. 29. Springer Verlag, first edition, 1975.

[52] Hans J. Zassenhaus. *The Theory of Groups.* Dover, second edition, 1958.

Index

M-regular sequence, 381
$\mathcal{I}$-Global Dimension Theorem, 390
(Co)homological Functors, 327
(N), 2
(co)homology of algebras, 331

enveloping algebra, 332

$\mathfrak{a}$-adic completion of A, 29
$\mathfrak{a}$-adic topology, 29
abelian category, 24
AC, 298
ACC for module, *see* ascending chain condition for module
acyclic complex, 310
acyclic resolution of modules, 128
additive functor, 125
additive group functor, 96
additive Hilbert 90, 294
$\mathfrak{A}$-adic topology, 237
adjoint functors, 339
admissible monomial, 113
admissible word, 105
affine group, 84
Akizuki's structure theorem, 195, 240
    false for noncomm. rings, 196
Akizuki, Y., 194
algebraic closure, 298
algebraic closure of field, 247
algebraic element over commutative ring, 115
algebraic geometry, 199
algebraically closed, 298
algebraically closed field, 247
algebraically dependent set over commutative ring, 115
algebraically independent set over commutative ring, 115
alternating R-algebra, 154
amalgamated product of groups, 106
annihilator of submodule, 116
arrow of category, *see* morphism of category
Artin ordering, 156
Artin Schreier
    Theorem I, 292, 293
    Theorem II, 292
Artin's irreducibility criterion, 294–296
Artin's theorem, 44, 261, 263, 265, 268, 271
Artin's theorem of the primitive element, 270
Artin, E., 294
Artin–Rees theorem, 238, 239
artinian module, 116
ascending chain condition for module, 116
associated primes of module, 228
atoms, 55
augmentation, 338
augmentation ideal, 334, 338
augmentation module, 386
augmented ring, 386
k-automorphism of field extension, 262
axiom of choice, 66, 185

backward image functor, 175
Baer embedding theorem, 20, 133, 135
    Godement's proof, 133
Baer radical of group, 2
Baer representation theorem, 131, 133
Baer's theorem, 3
Baer, R., 135
bar resolution, 334
base extension of module to algebra, 169
Basic Existence Theorem, 298
bounded complex, 310
    above, 310
    below, 310
Brauer, R., 52
bundle homomorphism of vector bundles, 18
Burnside basis theorem, 2, 72, 74
Burnside dimension, 74
Burnside's Lemma, 55
Burnside, W., 65, 88
butterfly lemma, *see* Zassenhaus' butterfly lemma

Cameron-Cohen Inequality, 55
canonical flasque resolution, 351

canonical map to localization, 174
canonical site, 32
Cartan–Eilenberg injective resolution of complex, 368
casus irreducibilis of cubic, 45
category, 95
  examples, 95
category co-over object, 101
category over object, 101
Cauchy, A., 61
Cayley graph, 7
Cayley transform, 53
Cayley–Hamilton theorem, 237
center of group, 69
central group extension, 82
centralizer of group element, 59
chain, 66
chain detour lemma, 241, 242
chain map, 310
d-chain on manifold, 153
character, 354
character of representation, 260
characteristic class of extension of module by module, 329
characteristic of ring, 11
characteristic subgroup of group, 71
Chevalley, 214
Chinese Remainder Theorem, 192, 195
  classical, 192
classification of groups of order pq, 85
closed set in Spec, 181
n-th coboundary group of group, 86
n-th coboundary map, group cohomology, 86
coboundary of 1-cochain on group, 79
n-th cochain group of group, 86
cochain map, 310
1-cochain on group, 79
2-cochain on group, 78
n-th cocycle group of group, 86
2-cocycle on group, 78
cofinal subset of index set, *see* final subset of index set
cofunctor, 96
cogredient tensor of rank a, 147
Cohen's lemma, 184, 185
Cohen, I. S., 184
Cohen-Seidenberg, 207
  I: Lying over Theorem, 207
  II: Going-up Theorem, 208
  III: Going-Down Theorem, 209
  III: Going-down Theorem, 210
cohomological complex, 310
cohomological spectral sequence, 356
cohomologous 2-cocycles on group, 79
cohomology
  long exact sequence, 277
  of a cyclic group, 280
  of presheaves, 344
  of sheaves, 344
cohomology cofunctor, 97
cohomology group of R with coefficient in M, 334
0-th cohomology group of group
  calculation, 86
n-th cohomology group of group, 86
cohomology of groups, 371
comaximal ideals, 192
comma category, *see* category over *or* co-over object
commutator group of group, 72
commutator of group elements, 69
compatible filtration and coboundary map, 355
compatible filtration and grading, 355
complementary index of spectral sequence, 356
completely reducible module, 385
S-component of submodule, 235
composition factors of composition series, 66
composition of morphisms between objects of category, 95
composition series for group, 66
compositum of two fields, 271
conductor, 221
  of the integral closure, 221
conjugacy class of group element, 59
H-conjugacy class of group element, 59
k-conjugate fields, 257
conjugation group action, 59
connecting homomorphism, 277
connecting homomorphism in LES for (co)homology, 319
connecting homomorphism in snake lemma, 137
constant presheaf with values in object, 24
continuous functor vector spaces $\to$ vector spaces, 17
contracted ideal, 176
contraction of tensors, 147
contragredient tensor of rank b, 147
convolution product in polynomial ring, 110
coprimary module, 223
coproduct in category, 102
  examples, 103–106
    $\mathcal{G}$r, 105
    $\mathcal{M}$od, 103
    $\mathcal{S}$ets, 103
coproduct of family of groups, 8
cotangent bundle of manifold, 153

cotangent space to manifold at point, 152
counting lemma, 60
covering family, 25
covering of object of category, 32
covering surjection, *see* minimal surjection
crossed homomorphism, 54, *see* twisted homomorphism
cup-product, group cohomology, 5

décalage, 328
DCC for module, *see* descending chain condition for module
Dedekind domain, 229
  examples, 229
Dedekind ring, 129
Dedekind's theorem, 260–262
Dedekind, R., 229
degenerate spectral sequence, 364
degree of field extension, 244
degree of filtration, 355
∂-functor, 321
δ-functor, 321
derivation of algebra with values in algebra, 245
  examples, 245
derived functor, 317
j-th derived group of group, 73
derived length of group, 74
derived series of group, 74
descending chain condition for module, 116
descent, 170, 338
descent of property in extension, 170
determinant of linear map, 154
dimension shifting, 328
direct image of sheaf, 198
direct limit, *see* right limit
direct mapping family, *see* right mapping family
directed set, 156
  examples, 156
discrete valuation on ring, 39
discrete valuation ring, 39
divisible abelian group, 8
divisible module, 132
dual category, 96
dual module, 354
DVR, *see* discrete valuation ring

E. Noether, 216
E. Noether: finiteness Theorem, 220
Eckmann, B., 135
Eilenberg, 54
Eilenberg, S., 87, 323
Eisenbud, 218
elementary d-chain in manifold, 153
elementary abelian p-group, 72
elementary symmetric functions, 209
empty word, 105
end of spectral sequence, 356
epimorphism of vector bundles, 18
equivalent categories, 98
equivalent group extensions, 75
essential injection, 130
essential primes of submodule in module, 228
essential submodule, *see* large submodule
essential surjection, *see* minimal surjection
étale algebra over comm. ring, 252
Euler function, 121
exact functor, 125
  examples, 125
exact sequence of groups, 75
exact sequence of vector bundles, 19
$\mathrm{Ext}^n_{\mathcal{A}}(\cdot, B)$, 318
extended ideal, 176
extension lemma, 256–259
  General, 284
extension property for injective modules, 131
exterior algebra of module, 150
j-th exterior power of module, 150

f.f., *see* faithfully flat module
f.g., *see* finitely generated module
f.p., *see* finitely presented module
Fact I
  cohomology of groups, 277
Fact II
  cohomology of groups, 277
faithful module, 188
faithfully flat module, 155
Feit, W., 65, 88
Fermat prime, 3
Fermat's little theorem, 254
fibre, 214
fibred coproduct over object, 102
  examples, 103–106
    $\mathcal{G}$r, 106
    $\mathcal{M}$od, 104
    $\mathcal{S}$ets, 104
fibred product over object, 102
  examples, 103–106
    $\mathcal{M}$od, 104
    $\mathcal{S}$ets, 104
filtered complex, 355
filtration index of spectral sequence, 356

final subset of index set, 160
finite atom, 55
finitely generated (f.g) module
    need not be f.p., 120
finitely generated algebra, 115
finitely generated group, 3
finitely generated ideal (FGI) test, 165
finitely generated module, 115
finitely presented module, 116
finiteness Theorems, 220
first homomorphism theorem, 182
first uniqueness theorem for primary decomp., 228, 230, 231
Fitting's lemma, 223
five lemma, 136, 143, 167, 190, 323
fixed field of family of characters, 261
flat module over ring, 155
flat op-module over ring, 155
forgetful functor, 96
forward image functor, 175
fraction field of comm. ring, 176
fraction ring of comm. ring, *see* localization of comm. ring
fractional ideal, 37
fractional linear transformation, 6
Frattini argument, 90
Frattini subgroup, 71
free group on set, 106
free module on set, 115
free product of groups, 106
free resolution of module, 128
Frobenius, G., 65
full subcategory, 96
functor, 96
    examples, 96–97
    may have right adjoint, no left adjoint, 100
fundamental theorem of Galois Theory, 264, 271
    general case, 286

Galois cohomology groups, 280
Galois equivalent field extensions, 263
Galois group
    with Krull topology, 285
Galois group of field extension, 262
Galois group of polynomial, 262
Galois, E., 69
Γ-Riccati equation, 11
Gauss, K., 45
Generalized Nakayama's Lemma, 389
generation of group by set, 107
generation of submodule by set, *see* submodule generated by set
geometry, 199
germ of function, 12
global dimension (of a ring), 384
Global Dimension Theorem, 396
Godement, 133
Godement resolution, 351
good free module, 147
good subset, 388
graded ring, 149
Grothendieck, 220, 369
    Spectral sequence of composed functors, 369
Ω-group, 92
    examples, 92
p-group, 61
group action (left), 57
    examples, 59
group cohomology, 277
group extension, 75
    examples, 82–85
group ring, 330

half-exact functor, 125
Hamel basis, 67, 68
    application to $\mathbb{R}/\mathbb{Q}$, 68
Hausdorff maximal principle, 66
height of prime ideal, 180
Hensel, K., 238
Henselization, 54
Herbrand's Lemma, 54
Herstein's lemma, 236
    proof using Artin–Rees, 239
Hilbert basis theorem
    Noether's argument, 122
    original, 123
Hilbert Syzygy Theorem, 391
Hilbert Theorem 90
    cohomological version, 280
    original form, 282
Hochschild, 334
    cohomology groups, 334
    homology groups, 334
Hochschild groups, 387
holomorphic geometry, 199
homogeneous ideal, 149
homogeneous space for group, 275
homological complex, 310
homology functor, 97
homology group of R with coefficients in M, 334
homology groups of G with coefficients in A, 331

homothety
example, 223
homotopy, 314
homotopy functor, 97
homotopy invariance, 314
Hurewicz map, 97

immediate equivalence, 104
important module, 387
indecomposable module, 11
independent characters, 260
independent transcendentals over commutative ring, *see* algebraically independent set over commutative ring
index of filtration, 355
inductive limit, *see* right limit
inductive mapping family, *see* right mapping family
inductive poset, 66
injective dimension, 384
injective hull of module, 135
injective module, 126
inner twisted homomorphism, *see* principal twisted homomorphism
inseparable field extension, 248
integral, 203
basis, 215
closure, 204
dependence, 203
dependence, transitivity of, 204
morphism, 203
over (Definition), 203
integral element over domain, 12
integrally closed, 204
integrally closed domain, 12
integrally closed domain in algebra, 12
integrally closed ring, 204
inverse limit, *see* left limit
inverse mapping family, *see* left mapping family
invertible module, 201
irreducible element of ring, 36
irreducible set, 234
isolated associated prime ideals of module, 228
isolated essential prime ideals of submodule in module, 228
isolated primary components of module, 228
isolated primary components of submodule in module, 228
isolated prime ideal of ideal, 183
isomorphic categories, 98
isomorphic normal flags, 92
isomorphism between objects of category, 96

Jacobian criterion for multiplicity, 245, 248
Jacobson radical, 131, 182
Jacobson radical of group, 2
Jordan's Theorem, 55
Jordan–Hölder theorem, 92, 121

Kaplansky, 55
Kaplansky's Theorem, 56
Koszul complex, 378
duality isomorphisms, 380
Koszul duality, 379, 380
Kronecker's theorem of the primitive element, 270–272
Krull
Galois theory, 284
Krull dimension of comm. ring, 180
examples, 180–181
dim = 0, 180
dim = 1, 180
dim = n, 181
Krull height theorem, 241
converse, 242
Krull intersection theorem, 236, 237, 240
original, 237
Krull principal ideal theorem, 239, 241, 242
Krull topology, 285
Krull, W., 239
Kummer, 289
Pairing theorem, 290
Kummer theory, *see* prime cyclic Kummer theory
Kummer's theorem, 295, *see* prime cyclic Kummer theory
Kummer, E., 229

Lagrange's cubic resolvent, 45
Lagrange's theorem
converse false, 60
large submodule, 130
Lasker-Noether decomposition theorem, 226, 228
Lasker's original, 227
Noether's original, 227
LCS of group, *see* lower central series of group
left acyclic resolution, 310
left adjoint functor, 100
left derived functors of cofunctor, 317
left derived functors of functor, 317
left limit, 157
examples, 160–162
left mapping family, 156
examples, 157
left-exact cofunctor, 125

left-exact functor, 125
lemma (L), 357–360
lemma(L), 359
length of chain of prime ideals, 180
length of module, 121
level of spectral sequence, 356
lifting property for projective modules, 127
line bundle, *see* invertible module
linear representation of group, 59
local embedding lemma, 62, 63
local flatness criterion, 186
local property, 186
local ring, 10, 179
local ringed space, 198
    examples, 198
localization of comm. ring, 174
    examples, 175
localization of comm. ring at prime ideal, 179
    represents germs of 'some kind', 191–192
localizing subcategory, 121
locally P, *see* local property
locally (P) group, 4
locally standard LRS, 199
locally trivial vector space family, 16
locally-free $\mathcal{O}_X$-module, 200
long (co)homology sequence lemma, 319
long exact (co)homology sequence lemma, 320
loop space of space, 108
    functor is right-adjoint to suspension functor, 108
lower central series of group, 89
lower star, 339
LRS, *see* local ringed space

Mac Lane, 216
Mac Lane I, 252, 267, 304
    interpretation, 253
Mac Lane II, 252, 254
    interpretation, 253
Mac Lane's theorem, 307
Mac Lane, S., 87
Main theorem on separability, 252
    counter example when K/k is not finite, 255
map of pairs, 339
Maschke's Theorem, 48, 385
maximal M-regular sequence, 381
maximal condition for module, 116
maximal idempotent of ring, 11
maximal spectrum of comm. ring, 181
minimal condition for module, 116
minimal injection, *see* essential injection
minimal polynomial, 209
minimal polynomial of algebraic elt., 248
minimal surjection, 130
module
    Map(B, G), 278
    divisible, 352
G-module, 59
Ω-module, 92
module of relative Kähler differentials, 250
    examples, 250–252
monomial, 111, 113
monomorphism of vector bundles, 18
Moore's theorem, 274
Moore, E.H., 274
Moore–Smith property, *see* directed set
Morita equivalence, 385
morphism of category, 95
morphism of functors, *see* natural transformation of functors
morphisms between objects of category, 95
multiplicative group functor, 97
multiplicative subset in comm. ring, 173
    examples, 173
multiplicity of root of polyn., 244

(N), 70, 72, 73, 90
Nagata, 215, 218, 220
    rings, 220
    rings (Definition), 220
Nagata, M., 194
Nakayama's lemma, 187, 189, 202, 233, 240
    classical, 187
natural irrationalities, 272
natural irrationalities theorem, 42, 271, 295
    interpretation, 272
    original, 272
natural transformation of functors, 97
    examples, 97
        on Vect(k), 98
Newton's Identities, 214
Nielson, J., 107
nilpotence class of group, 90
nilpotent group, 90
nilradical of comm. ring, 181
Noether Normalization Lemma, 216
Noether's proposition, 225, 226
Noether, E., 225
Noetherian induction, 194, 226
noetherian module, 116
    subring of noetherian ring need not be noetherian, 120
non-generator in group, 71

nonrepetitious normal flag, 92
norm, 209, 280
  of an extension, 281
G-norm, 84
norm map
  definition, 279
normal basis theorem, 47, 272, 281
  algebraic interpretation, 274–275
  geometric interpretation, 275–276
normal chain, *see* normal flag
normal closure of field extension, 259
normal domain, *see* integrally closed domain
normal field extension, 257
  counter-example to transitivity, 258
  non sequiturs, 258
normal flag, 92
normal ring, 204
normal series, *see* normal flag
Ω-normal subgroup, 92
normality, 204
  Noetherian domain, 206
normalized 2-cochain on group, 82
normalizer of set in group, 62
number field, 37, 229

object of category, 95
open set in Spec, 181
opposite category, *see* dual category
orbit space, 58
orbit under group action, 58
orthogonal idempotents, 200

partial order on set, 66
partially ordered set, *see* poset
Pass, 205
perfect field, 248, 305, 307
  examples, 248
pertinent module, 388
PHS for group, *see* principal homogeneous space for group
Picard group of comm. ring, 202
polynomial solvable by auxiliary chain of equations, 43
Pontrjagin dual, 290, 292, 293
poset, 66
power lemma, 231, 236
  generalization, *see* Herstein's lemma
premorphism, 309
presentation of group, 107
presentation of module, 124
presheaf, 344
presheaf of germs, 24
presheaf on topological space with values in category, 24
primary ideal, 223
$\mathfrak{p}$-primary submodule, 224
primary submodule in module, 224
prime avoidance lemma, 184, 241
prime element of ring, 36
prime ideal, 179
Prime Number Theorem, 54
prime spectrum of comm. ring, 181
  almost never Hausdorff, 183
primitive element, 270
primitive element theorem, *see* Artin's such *or* Kronecker's such
primitive root of unity, 289
principal homogeneous space for group, 275
principal idempotent of ring, *see* maximal idempotent of ring
principal twisted homomorphism, 86
product in category, 102
  examples, 103–106
    $\mathcal{G}$r, 105
    $\mathcal{M}$od, 103
    $\mathcal{S}$ets, 103
profinite group, 163
profinite groups, 372
projective cover, 130
  counter-example, 130
projective dimension, 384
projective limit, *see* left limit
projective mapping family, *see* left mapping family
projective module, 126
  product of such need not be such, 20
projective resolution of module, 128
proper map, 41
property (N), *see* (N)
pseudo-metric topology, 237
pull-back of forms, 153
pullback functor for vector space families, 16
purely inseparable degree of field extension, 255
purely inseparable elt. over field, 249
purely transcendental, 304

quasi-coherent $\mathcal{O}_X$-module, 200
quasi-compact space, 183

radical of ideal, 182
rank of quasi-coherent $\mathcal{O}_X$-module, 200
rank of vector bundle, 16
rank one group, 4

rational function field, 176
C^k real geometry, 199
reduced primary decomposition, 226
reduced ring, 182
refinement of normal flag by normal flag, 92
regular element of comm. ring, 177
regular filtration, 356
regular local ring, 392
regular sequence, 381
related fields, 256
relative radical of submodule in module, 223
representable functor, 99
    examples, 99
    uniqueness of representing pair, 99
K-representation of group, 260
residual quotient of submodule by set, *see* transporter of set to submodule
resolution, 310
    injective, 310
    projective, 310
restriction of vector space family, 16
right acyclic resolution, 310
right adjoint functor, 100
right derived functors of cofunctor, 317
right derived functors of functor, 317
right limit, 157
    examples, 160–162
right mapping family, 156
    examples, 157
right-exact cofunctor, 125
right-exact functor, 125
ring of formal power series over field, 29
ring of integers in number field, 229
ringed space, 372
Rudakov, A., 13

S-saturation of submodule, 178
Schanuel's lemma, 14, 124
Schmidt, F.K., 307
Schopf, A., 135
Schreier refinement theorem, 92, 93
Schreier, O., 107
second cohomology group of group, 79
second homomorphism theorem, 70, 91, 122, 135, 232
second uniqueness theorem for primary decomp., 228
section, 338
section of vector bundle over vector bundle, 16
semi-local ring, 36
semi-simple ring, 385
separable closure of field in extension, 255
separable degree of field extension, 255
separable element over field
    provisional defn., 248
separable extension, 214
separable field extension, 304, 306
    provisional defn., 248
separable irreducible polynomial
    provisional defn., 248
separable polynomial
    provisional defn., 248
separably generated field extension, 304, 306
separating transcendence base, 304
Serre, 55
sheaf, 344
    Čech cohomology, 347
    cohomology, 346
    direct image, 345
    flasque, 347
sheaf Hom, 373
sheaf of discontinuous sections, 351
sheaf of local rings, 197
sheaf of sets, 25
sheafification #, 344
short exact sequence of groups, 75
Sierpinski, 54
simple group, 64
simple module, 121
site, 32
skew field, 389
SMA, I, *see* sufficiently many automorphisms, I
SMA, II, *see* sufficiently many automorphisms, II
small commutative diagram, 316
small normal subgroup, 2
small radical of group, 2
small submodule, 130
smooth algebra over comm. ring, 252
snake lemma, 137, 143, 168, 189, 319
solvable group, 74
    Galois' sense, 69
space of 1-forms on manifold at point, *see* cotangent space to manifold at point
spectral sequence
    Čech cohomology, 373
    Associativity for EXt and Tor, 374
    Ext, 376
    Hochschild-Serre, 371
    Leray, 372
    Local to global Ext, 373
    Tor, 376
Spectral sequences, 355
spectral topology, *see* Zariski topology
split exact sequence, 126

split group extension, 82
splitting field arising from successive solution of chain of equations, 43
splitting field for polyn., 256
splitting of exact sequence, 126
stabilizer under group action, 58
stalk of a (pre)sheaf, 344
stalk of presheaf at point, 197
standard model
examples, 199
standard resolution, 334, 343
Steinitz, E., 298
Axioms for Σ, 301
Exchange Lemma, 301
Existence of a transcendence basis, 301
Existence of an algebraic closure, 299
General Exchange Lemma, 302
stripping functor, *see* forgetful functor
strongly convergent spectral sequence, 360
sub-bundle of vector bundle, 18
subcategory, 95
examples, 96
subextension of field extension, 259
Ω-subgroup, 92
submodule generated by set, 115
sufficiently many automorphisms, I, 258, 263, 265
sufficiently many automorphisms, II, 259, 266, 268
sum of submodules, 115
superfluous submodule, *see* small submodule
support of module, 185
suspension of space, 108
functor is left-adjoint to loop space functor, 108
Sylow classification theorem, *see* Sylow theorem II
Sylow existence theorem, *see* Sylow theorem I
p-Sylow subgroup, 61
of group of order pq, 64
of group of order pqr, 64
Sylow theorem I, 60, 62
original, 61
Sylow theorem II, 62, 64, 90
Sylow theorem III, 64, 70
modified, 90, 91
Sylow, L., 60
symbolic power of prime ideal, 239
symmetric algebra of module, 150
j-th symmetric power of module, 150
Syzygy, 391
Theorem, 391

tangent bundle of manifold, 153
tangent space to manifold at point, 152
Taylor's theorem, 272
tensor algebra of module, 149
tensor field, 147
tensor product of two modules over ring, 140
computations, 142–147
Thompson, J., 65, 88
tilde construction from module, 196
topological ring, 31
topologically nilpotent element in topological ring, 31
$\mathrm{Tor}_n^{\mathcal{A}}(\cdot, B)$, 318
Tor dimension, 386
n-torsion element of group, 4
torsion free group element, 4
total complex, 367
total differential, 367
total fraction ring, 204
total fraction ring of comm. ring, 176
total grading index of spectral sequence, 356
Tower Theorem, 372
trace, 209, 280
of an extension, 281
transcendence basis, 299
transcendence degree, 215, 304
transcendental element over commutative ring, 115
transcendental extensions, 298
translation group action, 59
transporter of set to submodule, 116
trivial group action, 59
twisted homomorphism, 86
two-sided ideal, 115
Tychonov's theorem, 163
type of group extension, 76

UCS of group, *see* upper central series of group
uniqueness I for δ-functors, 322
uniqueness II for δ-functors, 323, 328
uniqueness III for δ-functors, 324
universal δ-functor, 321
isomorphism at $n = 0$ lifts, 321
universal ∂-functor, 321
universal mapping property
left limits, 158
localization, 178
polynomial rings, 110
products, 102
right limits, 158, 162, 163
tensor products, 163
universal, effective epimorphism, 32
universally Japanese rings, 220
upper central series of group, 89
upper star, 339

Urysohn's lemma, 183

van Kampen's theorem, 106
variety defined by ideal, 181
vector bundle, 16
vector space family over topological space, 16

weakly convergent spectral sequence, 360
Wederburn, 48
weight function on domain, 36
well ordered chain, 66
Wielandt, H., 60
Witt, 293
    ring of Witt vectors, 293
words over alphabet, 105
wreath product, 84

Yoneda, 48
Yoneda's embedding lemma, 99, 113, 141, 253
    interpretation, 99

Zariski topology, 181, 213
Zassenhaus' butterfly lemma, 93, 94
Zassenhaus, H., 93
Zermelo well ordering principle, 66
Zorn's lemma, 66, 67, 132, 135, 179, 182, 185, 253