Applied Algebra
Notes for AMCS 602

Jean Gallier* & Stephen Shatz**
*Department of Computer and Information Science
e-mail: jean@cis.upenn.edu
**Department of Mathematics

University of Pennsylvania
Philadelphia, PA 19104, USA

August 31, 2012

Contents

Chapter 1

Group Representations

1.1 Group Actions and Homogeneous Spaces

If X is a set (usually, some kind of geometric space, for example, the sphere in $\mathbb{R}^3$, the upper half-plane, etc.), the "symmetries" of X are often captured by the action of a group, G, on X. In fact, if G is a Lie group and the action satisfies some simple properties, the set X can be given a manifold structure which makes it a projection (quotient) of G, a so-called "homogeneous space".

Definition 1.1. Given a set, X, and a group, G, a *left action of G on X* (for short, an *action of G on X*) is a function, $\varphi\colon G \times X \to X$, such that

(1) For all $g, h \in G$ and all $x \in X$,

$$\varphi(g, \varphi(h, x)) = \varphi(gh, x),$$

(2) For all $x \in X$,

$$\varphi(1, x) = x,$$

where $1 \in G$ is the identity element of G.

To alleviate the notation, we usually write $g \cdot x$ or even gx for $\varphi(g, x)$, in which case, the above axioms read:

(1) For all $g, h \in G$ and all $x \in X$,

$$g \cdot (h \cdot x) = gh \cdot x,$$

(2) For all $x \in X$,

$$1 \cdot x = x.$$

The set X is called a *(left) G-set*. The action φ is *faithful* or *effective* iff for every g, if $g \cdot x = x$ for all $x \in X$, then $g = 1$; the action φ is *transitive* iff for any two elements $x, y \in X$, there is some $g \in G$ so that $g \cdot x = y$.

Given an action, $\varphi\colon G \times X \to X$, for every $g \in G$, we have a function, $\varphi_g\colon X \to X$, defined by

$$\varphi_g(x) = g \cdot x, \quad \text{for all } x \in X.$$

Observe that φ_g has $\varphi_{g^{-1}}$ as inverse, since

$$\varphi_{g^{-1}}(\varphi_g(x)) = \varphi_{g^{-1}}(g \cdot x) = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x,$$

and similarly, $\varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}$. Therefore, φ_g is a bijection of X, i.e., a permutation of X. Moreover, we check immediately that

$$\varphi_g \circ \varphi_h = \varphi_{gh},$$

so, the map $g \mapsto \varphi_g$ is a group homomorphism from G to $\mathfrak{S}_X$, the group of permutations of X. With a slight abuse of notation, this group homomorphism $G \longrightarrow \mathfrak{S}_X$ is also denoted φ.

Conversely, it is easy to see that any group homomorphism, $\varphi\colon G \to \mathfrak{S}_X$, yields a group action, $\cdot\colon G \times X \longrightarrow X$, by setting

$$g \cdot x = \varphi(g)(x).$$

Observe that an action, φ, is faithful iff the group homomorphism, $\varphi\colon G \to \mathfrak{S}_X$, is injective. Also, we have $g \cdot x = y$ iff $g^{-1} \cdot y = x$, since $(gh) \cdot x = g \cdot (h \cdot x)$ and $1 \cdot x = x$, for all $g, h \in G$ and all $x \in X$.

Definition 1.2. Given two G-sets, X and Y, a function, $f\colon X \to Y$, is said to be *equivariant*, or a *G-map* iff for all $x \in X$ and all $g \in G$, we have

$$f(g \cdot x) = g \cdot f(x).$$

Remark: We can also define a *right action*, $\cdot\colon X \times G \to X$, of a group G on a set X, as a map satisfying the conditions

(1) For all $g, h \in G$ and all $x \in X$,

$$(x \cdot g) \cdot h = x \cdot gh,$$

(2) For all $x \in X$,

$$x \cdot 1 = x.$$

Every notion defined for left actions is also defined for right actions, in the obvious way.

Here are some examples of (left) group actions.

Example 1: The unit sphere S^2 (more generally, S^{n-1}).

Recall that for any $n \geq 1$, the *(real) unit sphere*, S^{n-1}, is the set of points in $\mathbb{R}^n$ given by

$$S^{n-1} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 = 1\}.$$

In particular, S^2 is the usual sphere in $\mathbb{R}^3$. Since the group $\mathbf{SO}(3) = \mathbf{SO}(3, \mathbb{R})$ consists of (orientation preserving) linear isometries, i.e., *linear* maps that are distance preserving (and of determinant $+1$), and every linear map leaves the origin fixed, we see that any rotation maps S^2 into itself.

Beware that this would be false if we considered the group of *affine* isometries, $\mathbf{SE}(3)$, of $\mathbb{E}^3$. For example, a screw motion does *not* map S^2 into itself, even though it is distance preserving, because the origin is translated.

Thus, we have an action, $\cdot\colon \mathbf{SO}(3) \times S^2 \to S^2$, given by

$$R \cdot x = Rx.$$

The verification that the above is indeed an action is trivial. This action is transitive. This is because, for any two points x, y on the sphere S^2, there is a rotation whose axis is perpendicular to the plane containing x, y and the center, O, of the sphere (this plane is not unique when x and y are antipodal, i.e., on a diameter) mapping x to y.

Similarly, for any $n \geq 1$, we get an action, $\cdot\colon \mathbf{SO}(n) \times S^{n-1} \to S^{n-1}$. It is easy to show that this action is transitive.

Analogously, we can define the *(complex) unit sphere*, Σ^{n-1}, as the set of points in $\mathbb{C}^n$ given by

$$\Sigma^{n-1} = \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid z_1\overline{z}_1 + \cdots + z_n\overline{z}_n = 1\}.$$

If we write $z_j = x_j + iy_j$, with $x_j, y_j \in \mathbb{R}$, then

$$\Sigma^{n-1} = \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{R}^{2n} \mid x_1^2 + \cdots + x_n^2 + y_1^2 + \cdots + y_n^2 = 1\}.$$

Therefore, we can view the complex sphere, Σ^{n-1} (in $\mathbb{C}^n$), as the real sphere, S^{2n-1} (in $\mathbb{R}^{2n}$). By analogy with the real case, we can define an action, $\cdot\colon \mathbf{SU}(n) \times \Sigma^{n-1} \to \Sigma^{n-1}$, of the group, $\mathbf{SU}(n)$, of *linear* maps of $\mathbb{C}^n$ preserving the hermitian inner product (and the origin, as all linear maps do) and this action is transitive.

One should not confuse the unit sphere, Σ^{n-1}, with the hypersurface, $S^{n-1}_{\mathbb{C}}$, given by

$$S^{n-1}_{\mathbb{C}} = \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid z_1^2 + \cdots + z_n^2 = 1\}.$$

For instance, one should check that a line, L, through the origin intersects Σ^{n-1} in a circle, whereas it intersects $S^{n-1}_{\mathbb{C}}$ in exactly two points!

Example 2: The upper half-plane.

The *upper half-plane*, H, is the open subset of $\mathbb{R}^2$ consisting of all points, $(x, y) \in \mathbb{R}^2$, with $y > 0$. It is convenient to identify H with the set of complex numbers, $z \in \mathbb{C}$, such that $\Im z > 0$. Then, we can define an action, $\cdot\colon \mathbf{SL}(2, \mathbb{R}) \times H \to H$, of the group $\mathbf{SL}(2, \mathbb{R})$ on H, as follows: For any $z \in H$, for any $A \in \mathbf{SL}(2, \mathbb{R})$,

$$A \cdot z = \frac{az + b}{cz + d},$$

where

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $ad - bc = 1$. It is easily verified that $A \cdot z$ is indeed always well defined and in H when $z \in H$. This action is transitive (check this).

Maps of the form

$$z \mapsto \frac{az + b}{cz + d},$$

where $z \in \mathbb{C}$ and $ad - bc = 1$, are called *Möbius transformations*. Here, $a, b, c, d \in \mathbb{R}$, but in general, we allow $a, b, c, d \in \mathbb{C}$. Actually, these transformations are not necessarily defined everywhere on $\mathbb{C}$, for example, for $z = -d/c$ if $c \neq 0$. To fix this problem, we add a "point at infinity", ∞, to $\mathbb{C}$ and define Möbius transformations as functions $\mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{C} \cup \{\infty\}$. If $c = 0$, the Möbius transformation sends ∞ to itself, otherwise, $-d/c \mapsto \infty$ and $\infty \mapsto a/c$. The space $\mathbb{C} \cup \{\infty\}$ can be viewed as the plane, $\mathbb{R}^2$, extended with a point at infinity. Using a stereographic projection from the sphere S^2 to the plane, (say from the north pole to the equatorial plane), we see that there is a bijection between the sphere, S^2, and $\mathbb{C} \cup \{\infty\}$. More precisely, the *stereographic projection* of the sphere S^2 from the north pole, $N = (0, 0, 1)$, to the plane $z = 0$ (extended with the point at infinity, ∞) is given by

$$(x, y, z) \in S^2 - \{(0, 0, 1)\} \mapsto \left(\frac{x}{1 - z}, \frac{y}{1 - z}\right) = \frac{x + iy}{1 - z} \in \mathbb{C}, \quad \text{with} \quad (0, 0, 1) \mapsto \infty.$$

The inverse stereographic projection is given by

$$(x, y) \mapsto \left(\frac{2x}{x^2 + y^2 + 1}, \frac{2y}{x^2 + y^2 + 1}, \frac{x^2 + y^2 - 1}{x^2 + y^2 + 1}\right), \quad \text{with} \quad \infty \mapsto (0, 0, 1).$$

Intuitively, the inverse stereographic projection "wraps" the equatorial plane around the sphere. The space $\mathbb{C} \cup \{\infty\}$ is known as the *Riemann sphere*. We will see shortly that $\mathbb{C} \cup \{\infty\} \cong S^2$ is also the complex projective line, $\mathbb{CP}^1$. In summary, Möbius transformations are bijections of the Riemann sphere. It is easy to check that these transformations form a group under composition for all $a, b, c, d \in \mathbb{C}$, with $ad - bc = 1$. This is the *Möbius group*, denoted $\mathbf{M\ddot{o}b}^+$. The Möbius transformations corresponding to the case $a, b, c, d \in \mathbb{R}$, with $ad - bc = 1$ form a subgroup of $\mathbf{M\ddot{o}b}^+$ denoted $\mathbf{M\ddot{o}b}^+_{\mathbb{R}}$. The map from $\mathbf{SL}(2, \mathbb{C})$ to $\mathbf{M\ddot{o}b}^+$ that sends $A \in \mathbf{SL}(2, \mathbb{C})$ to the corresponding Möbius transformation is a surjective group homomorphism and one checks easily that its kernel is $\{-I, I\}$ (where I is the 2×2 identity matrix). Therefore, the Möbius group $\mathbf{M\ddot{o}b}^+$ is isomorphic to the quotient group $\mathbf{SL}(2, \mathbb{C})/\{-I, I\}$, denoted $\mathbf{PSL}(2, \mathbb{C})$. This latter group turns out to be the group of projective transformations of the projective space $\mathbb{CP}^1$. The same reasoning shows that the subgroup $\mathbf{M\ddot{o}b}^+_{\mathbb{R}}$ is isomorphic to $\mathbf{SL}(2, \mathbb{R})/\{-I, I\}$, denoted $\mathbf{PSL}(2, \mathbb{R})$.

The group $\mathbf{SL}(2, \mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\} \cong S^2$ the same way that $\mathbf{SL}(2, \mathbb{R})$ acts on H, namely: For any $A \in \mathbf{SL}(2, \mathbb{C})$, for any $z \in \mathbb{C} \cup \{\infty\}$,

$$A \cdot z = \frac{az + b}{cz + d},$$

where

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{with} \quad ad - bc = 1.$$

This action is clearly transitive.

Example 3: The set of $n \times n$ symmetric, positive, definite matrices, $\mathbf{SPD}(n)$.

The group $\mathbf{GL}(n) = \mathbf{GL}(n, \mathbb{R})$ acts on $\mathbf{SPD}(n)$ as follows: For all $A \in \mathbf{GL}(n)$ and all $S \in \mathbf{SPD}(n)$,

$$A \cdot S = ASA^\top.$$

It is easily checked that $ASA^\top$ is in $\mathbf{SPD}(n)$ if S is in $\mathbf{SPD}(n)$. This action is transitive because every SPD matrix, S, can be written as $S = AA^\top$, for some invertible matrix, A (prove this as an exercise).

Example 4: The projective spaces $\mathbb{RP}^n$ and $\mathbb{CP}^n$.

The *(real) projective space*, $\mathbb{RP}^n$, is the set of all lines through the origin in $\mathbb{R}^{n+1}$, i.e., the set of one-dimensional subspaces of $\mathbb{R}^{n+1}$ (where $n \geq 0$). Since a one-dimensional subspace, $L \subseteq \mathbb{R}^{n+1}$, is spanned by any nonzero vector, $u \in L$, we can view $\mathbb{RP}^n$ as the set of equivalence classes of nonzero vectors in $\mathbb{R}^{n+1} - \{0\}$ modulo the equivalence relation,

$$u \sim v \quad \text{iff} \quad v = \lambda u, \quad \text{for some} \quad \lambda \in \mathbb{R},\ \lambda \neq 0.$$

In terms of this definition, there is a projection, $pr\colon (\mathbb{R}^{n+1} - \{0\}) \to \mathbb{RP}^n$, given by $pr(u) = [u]_\sim$, the equivalence class of u modulo $\sim$. Write $[u]$ for the line defined by the nonzero vector, u. Since every line, L, in $\mathbb{R}^{n+1}$ intersects the sphere S^n in two antipodal points, we can view $\mathbb{RP}^n$ as the quotient of the sphere S^n by identification of antipodal points. We write

$$S^n/\{I, -I\} \cong \mathbb{RP}^n.$$

We define an action of $\mathbf{SO}(n+1)$ on $\mathbb{RP}^n$ as follows: For any line, $L = [u]$, for any $R \in \mathbf{SO}(n+1)$,

$$R \cdot L = [Ru].$$

Since R is linear, the line $[Ru]$ is well defined, i.e., does not depend on the choice of $u \in L$. It is clear that this action is transitive.

The *(complex) projective space*, $\mathbb{CP}^n$, is defined analogously as the set of all lines through the origin in $\mathbb{C}^{n+1}$, i.e., the set of one-dimensional subspaces of $\mathbb{C}^{n+1}$ (where $n \geq 0$). This time, we can view $\mathbb{CP}^n$ as the set of equivalence classes of vectors in $\mathbb{C}^{n+1} - \{0\}$ modulo the equivalence relation,

$$u \sim v \quad \text{iff} \quad v = \lambda u, \quad \text{for some} \quad \lambda \ \neq 0 \in \mathbb{C}.$$

We have the projection, $pr\colon \mathbb{C}^{n+1} - \{0\} \to \mathbb{CP}^n$, given by $pr(u) = [u]_\sim$, the equivalence class of u modulo $\sim$. Again, write $[u]$ for the line defined by the nonzero vector, u.

Recall that $\Sigma^n \subseteq \mathbb{C}^{n+1}$, the unit sphere in $\mathbb{C}^{n+1}$, is defined by

$$\Sigma^n = \{(z_1, \ldots, z_{n+1}) \in \mathbb{C}^{n+1} \mid z_1\overline{z}_1 + \cdots + z_{n+1}\overline{z}_{n+1} = 1\}.$$

For any line, $L = [u]$, where $u \in \mathbb{C}^{n+1}$ is a nonzero vector, writing $u = (u_1, \ldots, u_{n+1})$, a point $z \in \mathbb{C}^{n+1}$ belongs to L iff $z = \lambda(u_1, \ldots, u_{n+1})$, for some $\lambda \in \mathbb{C}$. Therefore, the intersection, $L \cap \Sigma^n$, of the line L and the sphere Σ^n is given by

$$L \cap \Sigma^n = \{\lambda(u_1, \ldots, u_{n+1}) \in \mathbb{C}^{n+1} \mid \lambda \in \mathbb{C},\ \lambda\overline{\lambda}(u_1\overline{u}_1 + \cdots + u_{n+1}\overline{u}_{n+1}) = 1\},$$

i.e.,

$$L \cap \Sigma^n = \left\{ \lambda(u_1, \ldots, u_{n+1}) \in \mathbb{C}^{n+1} \;\middle|\; \lambda \in \mathbb{C},\ |\lambda| = \frac{1}{\sqrt{|u_1|^2 + \cdots + |u_{n+1}|^2}} \right\}.$$

Thus, we see that there is a bijection between $L \cap \Sigma^n$ and the circle, S^1, i.e., geometrically, $L \cap \Sigma^n$ is a circle. Moreover, since any line, L, through the origin is determined by just one other point, we see that for any two lines L_1 and L_2 through the origin,

$$L_1 \neq L_2 \quad \text{iff} \quad (L_1 \cap \Sigma^n) \cap (L_2 \cap \Sigma^n) = \emptyset.$$

However, Σ^n is the sphere S^{2n+1} in $\mathbb{R}^{2n+2}$. It follows that $\mathbb{CP}^n$ is the quotient of S^{2n+1} by the equivalence relation, $\sim$, defined such that

$$y \sim z \quad \text{iff} \quad y, z \in L \cap \Sigma^n, \quad \text{for some line, } L, \text{ through the origin.}$$

Therefore, we can write

$$S^{2n+1}/S^1 \cong \mathbb{CP}^n.$$

Observe that $\mathbb{CP}^n$ can also be viewed as the orbit space of the action, $\cdot\colon S^1 \times S^{2n+1} \to S^{2n+1}$, given by

$$\lambda \cdot (z_1, \ldots, z_{n+1}) = (\lambda z_1, \ldots, \lambda z_{n+1}),$$

where $S^1 = \mathbf{U}(1)$ (the group of complex numbers of modulus 1) and S^{2n+1} is identified with Σ^n. The case $n = 1$ is particularly interesting, as it turns out that

$$S^3/S^1 \cong S^2.$$

This is the famous *Hopf fibration*. To show this, proceed as follows: As

$$S^3 \cong \Sigma^1 = \{(z, z') \in \mathbb{C}^2 \mid |z|^2 + |z'|^2 = 1\},$$

define a map, $\mathrm{HF}\colon S^3 \to S^2$, by

$$\mathrm{HF}((z, z')) = (2z\overline{z'}, |z|^2 - |z'|^2).$$

We leave as a homework exercise to prove that this map has range S^2 and that

$$\mathrm{HF}((z_1, z_1')) = \mathrm{HF}((z_2, z_2')) \quad \text{iff} \quad (z_1, z_1') = \lambda(z_2, z_2'), \quad \text{for some } \lambda \text{ with } |\lambda| = 1.$$

In other words, for any point, $p \in S^2$, the inverse image, $\mathrm{HF}^{-1}(p)$ (also called *fibre* over p), is a circle on S^3. Consequently, S^3 can be viewed as the union of a family of disjoint circles. This is the *Hopf fibration*. It is possible to visualize the Hopf fibration using the stereographic projection from S^3 onto $\mathbb{R}^3$. This is a beautiful and puzzling picture. For example, see Berger [1]. Therefore, HF induces a bijection from $\mathbb{CP}^1$ to S^2, and it is a homeomorphism.

We define an action of $\mathbf{SU}(n+1)$ on $\mathbb{CP}^n$ as follows: For any line, $L = [u]$, for any $R \in \mathbf{SU}(n+1)$,

$$R \cdot L = [Ru].$$

Again, this action is well defined and it is transitive.

Example 5: Affine spaces.

If E is any (real) vector space and X is any set, a transitive and faithful action, $\cdot : E \times X \to X$, of the additive group of E on X makes X into an *affine space*. The intuition is that the members of E are translations.

Those familiar with affine spaces as in Gallier [6] (Chapter 2) or Berger [1] will point out that if X is an affine space, then, not only is the action of E on X transitive, but more is true: For any two points, $a, b \in E$, there is a *unique* vector, $u \in E$, such that $u \cdot a = b$. By the way, the action of E on X is usually considered to be a right action and is written additively, so $u \cdot a$ is written $a + u$ (the result of translating a by u). Thus, it would seem that we have to require more of our action. However, this is not necessary because E (under addition) is *abelian*. More precisely, we have the proposition

Proposition 1.1. *If G is an abelian group acting on a set X and the action $\cdot : G \times X \to X$ is transitive and faithful, then for any two elements $x, y \in X$, there is a unique $g \in G$ so that $g \cdot x = y$ (the action is simply transitive).*

Proof. Since our action is transitive, there is at least some $g \in G$ so that $g \cdot x = y$. Assume that we have $g_1, g_2 \in G$ with

$$g_1 \cdot x = g_2 \cdot x = y.$$

We shall prove that, actually,

$$g_1 \cdot z = g_2 \cdot z, \quad \text{for all } z \in X.$$

As our action is faithful we must have $g_1 = g_2$, and this proves our proposition.

Pick any $z \in X$. As our action is transitive, there is some $h \in G$ so that $z = h \cdot x$. Then, we have

$$\begin{aligned}
g_1 \cdot z &= g_1 \cdot (h \cdot x) \\
&= (g_1 h) \cdot x \\
&= (h g_1) \cdot x \qquad \text{(since } G \text{ is abelian)} \\
&= h \cdot (g_1 \cdot x) \\
&= h \cdot (g_2 \cdot x) \qquad \text{(since } \quad g_1 \cdot x = g_2 \cdot x) \\
&= (h g_2) \cdot x \\
&= (g_2 h) \cdot x \qquad \text{(since } G \text{ is abelian)} \\
&= g_2 \cdot (h \cdot x) \\
&= g_2 \cdot z.
\end{aligned}$$

Therefore, $g_1 \cdot z = g_2 \cdot z$, for all $z \in X$, as claimed. □

More examples will be considered later.

The subset of group elements that leave some given element $x \in X$ fixed plays an important role.

Definition 1.3. Given an action, $\cdot : G \times X \to X$, of a group G on a set X, for any $x \in X$, the group G_x (also denoted $\mathrm{Stab}_G(x)$), called the *stabilizer* of x or *isotropy group at* x is given by

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

We have to verify that G_x is indeed a subgroup of G, but this is easy. Indeed, if $g \cdot x = x$ and $h \cdot x = x$, then we also have $h^{-1} \cdot x = x$ and so, we get $gh^{-1} \cdot x = x$, proving that G_x is a subgroup of G. In general, G_x is **not** a normal subgroup.

Observe that

$$G_{g \cdot x} = g G_x g^{-1},$$

for all $g \in G$ and all $x \in X$.

Indeed,

$$\begin{aligned}
G_{g \cdot x} &= \{h \in G \mid h \cdot (g \cdot x) = g \cdot x\} \\
&= \{h \in G \mid hg \cdot x = g \cdot x\} \\
&= \{h \in G \mid g^{-1} h g \cdot x = x\} \\
&= g G_x g^{-1}.
\end{aligned}$$

Therefore, the stabilizers of x and $g \cdot x$ are conjugate of each other.

When the action of G on X is transitive, for any fixed $x \in G$, the set X is a quotient (as set, not as group) of G by G_x. Indeed, we can define the map, $\pi_x \colon G \to X$, by

$$\pi_x(g) = g \cdot x, \quad \text{for all } g \in G.$$

Observe that

$$\pi_x(gG_x) = (gG_x) \cdot x = g \cdot (G_x \cdot x) = g \cdot x = \pi_x(g).$$

This shows that $\pi_x \colon G \to X$ induces a quotient map, $\overline{\pi}_x \colon G/G_x \to X$, from the set, G/G_x, of (left) cosets of G_x to X, defined by

$$\overline{\pi}_x(gG_x) = g \cdot x.$$

Since

$$\pi_x(g) = \pi_x(h) \quad \text{iff} \quad g \cdot x = h \cdot x \quad \text{iff} \quad g^{-1}h \cdot x = x \quad \text{iff} \quad g^{-1}h \in G_x \quad \text{iff} \quad gG_x = hG_x,$$

we deduce that $\overline{\pi}_x \colon G/G_x \to X$ is injective. However, since our action is transitive, for every $y \in X$, there is some $g \in G$ so that $g \cdot x = y$ and so, $\overline{\pi}_x(gG_x) = g \cdot x = y$, i.e., the map $\overline{\pi}_x$ is also surjective. Therefore, the map $\overline{\pi}_x \colon G/G_x \to X$ is a bijection (of sets, not groups). The map $\pi_x \colon G \to X$ is also surjective. Let us record this important fact as

Proposition 1.2. *If $\cdot \colon G \times X \to X$ is a transitive action of a group G on a set X, for every fixed $x \in X$, the surjection, $\pi \colon G \to X$, given by*

$$\pi(g) = g \cdot x$$

induces a bijection

$$\overline{\pi} \colon G/G_x \to X,$$

where G_x is the stabilizer of x.

The map $\pi \colon G \to X$ (corresponding to a fixed $x \in X$) is sometimes called a *projection* of G onto X. Proposition 1.2 shows that for every $y \in X$, the subset, $\pi^{-1}(y)$, of G (called the *fibre above* y) is equal to some coset, gG_x, of G and thus, is in bijection with the group G_x itself. We can think of G as a moving family of fibres, G_x, parametrized by X. This point of view of viewing a space as a moving family of simpler spaces is typical in (algebraic) geometry, and underlies the notion of (principal) fibre bundle.

Note that if the action $\cdot \colon G \times X \to X$ is transitive, then the stabilizers G_x and G_y of any two elements $x, y \in X$ are isomorphic, as they as conjugates. Thus, in this case, it is enough to compute one of these stabilizers for a "convenient" x.

As the situation of Proposition 1.2 is of particular interest, we make the following definition:

Definition 1.4. A set, X, is said to be a *homogeneous space* if there is a transitive action, $\cdot \colon G \times X \to X$, of some group, G, on X.

We see that all the spaces of Example 1–5 are homogeneous spaces. Another example that will play an important role when we deal with Lie groups is the situation where we have a group, G, a subgroup, H, of G (not necessarily normal) and where $X = G/H$, the set of left cosets of G modulo H. The group G acts on G/H by left multiplication:

$$a \cdot (gH) = (ag)H,$$

where $a, g \in G$. This action is clearly transitive and one checks that the stabilizer of gH is gHg^{-1}. If G is a topological group and H is a closed subgroup of G it turns out that G/H is Hausdorff (Recall that a topological space, X, is *Hausdorff* iff for any two distinct points $x \neq y \in X$, there exists two disjoint open subsets, U and V, with $x \in U$ and $y \in V$.) If G is a Lie group, we obtain a manifold.

Even if G and X are topological spaces and the action, $\cdot\colon G \times X \to X$, is continuous, the space G/G_x under the quotient topology is, in general, **not** homeomorphic to X.

We will give later sufficient conditions that insure that X is indeed a topological space or even a manifold. In particular, X will be a manifold when G is a Lie group.

In general, an action $\cdot\colon G \times X \to X$ is not transitive on X, but for every $x \in X$, it is transitive on the set

$$O(x) = G \cdot x = \{g \cdot x \mid g \in G\}.$$

Such a set is called the *orbit* of x. The orbits are the equivalence classes of the following equivalence relation:

Definition 1.5. Given an action, $\cdot\colon G \times X \to X$, of some group, G, on X, the equivalence relation, $\sim$, on X is defined so that, for all $x, y \in X$,

$$x \sim y \quad \text{iff} \quad y = g \cdot x, \quad \text{for some } g \in G.$$

For every $x \in X$, the equivalence class of x is the *orbit of* x, denoted $O(x)$ or $\mathrm{Orb}_G(x)$, with

$$O(x) = \{g \cdot x \mid g \in G\}.$$

The set of orbits is denoted X/G.

The orbit space, X/G, is obtained from X by an identification (or merging) process: For every orbit, all points in that orbit are merged into a single point. For example, if $X = S^2$ and G is the group consisting of the restrictions of the two linear maps I and $-I$ of $\mathbb{R}^3$ to S^2 (where $-I(x, y, z) = (-x, -y, -z)$), then

$$X/G = S^2/\{I, -I\} \cong \mathbb{RP}^2.$$

Many manifolds can be obtained in this fashion, including the torus, the Klein bottle, the Möbius band, etc.

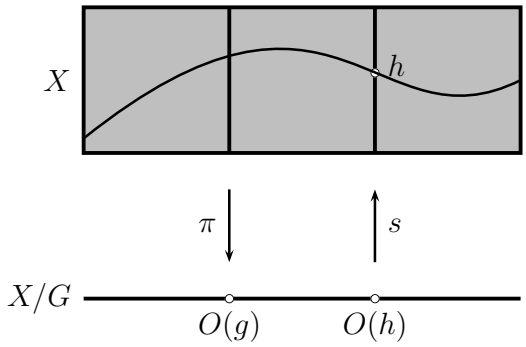


Figure 1.1: The set X as a fibre bundle, and a section

The space X can be viewed as a family of fibres (a fibre bundle) over the set of orbits X/G, each fibre being an orbit $O(g)$. If $\pi\colon X \to X/G$ is the projection function, then for every orbit $a = O(g)$ considered as a point of X/G, the fibre $\pi^{-1}(a) = O(g)$ is the whole orbit of g; see Figure 1.1. A *section* of X is a way of picking some element in each orbit, namely a function $s\colon X/G \to X$ such that $\pi \circ s = \mathrm{id}$.

Since the action of G is transitive on $O(x)$, by Proposition 1.2, we see that for every $x \in X$, we have a bijection

$$O(x) \cong G/G_x.$$

As a corollary, if both X and G are finite, for any set, $A \subseteq X$, of representatives from every orbit, we have the *orbit formula*:

$$|X| = \sum_{a \in A} [G\colon G_x] = \sum_{a \in A} |G|/|G_x|.$$

Even if a group action, $\cdot\colon G \times X \to X$, is not transitive, when X is a manifold, we can consider the set of orbits, X/G, and if the action of G on X satisfies certain conditions, X/G is actually a manifold. Manifolds arising in this fashion are often called *orbifolds*. In summary, we see that manifolds arise in at least two ways from a group action:

(1) As homogeneous spaces, G/G_x, if the action is transitive.

(2) As orbifolds, X/G.

Of course, in both cases, the action must satisfy some additional properties.

Let us now determine some stabilizers for the actions of Examples 1–4, and for more examples of homogeneous spaces.

(a) Consider the action, $\cdot\colon \mathbf{SO}(n) \times S^{n-1} \to S^{n-1}$, of $\mathbf{SO}(n)$ on the sphere S^{n-1} $(n \geq 1)$ defined in Example 1. Since this action is transitive, we can determine the stabilizer of any

convenient element of S^{n-1}, say $e_1 = (1, 0, \ldots, 0)$. In order for any $R \in \mathbf{SO}(n)$ to leave e_1 fixed, the first column of R must be e_1, so R is an orthogonal matrix of the form

$$R = \begin{pmatrix} 1 & U \\ 0 & S \end{pmatrix}, \quad \text{with} \quad \det(S) = 1.$$

As the rows of R must be unit vector, we see that $U = 0$ and $S \in \mathbf{SO}(n-1)$. Therefore, the stabilizer of e_1 is isomorphic to $\mathbf{SO}(n-1)$, and we deduce the bijection

$$\mathbf{SO}(n)/\mathbf{SO}(n-1) \cong S^{n-1}.$$

Strictly speaking, $\mathbf{SO}(n-1)$ is not a subgroup of $\mathbf{SO}(n)$ and in all rigor, we should consider the subgroup, $\widetilde{\mathbf{SO}}(n-1)$, of $\mathbf{SO}(n)$ consisting of all matrices of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & S \end{pmatrix}, \quad \text{with} \quad \det(S) = 1$$

and write

$$\mathbf{SO}(n)/\widetilde{\mathbf{SO}}(n-1) \cong S^{n-1}.$$

However, it is common practice to identify $\mathbf{SO}(n-1)$ with $\widetilde{\mathbf{SO}}(n-1)$.

When $n = 2$, as $\mathbf{SO}(1) = \{1\}$, we find that $\mathbf{SO}(2) \cong S^1$, a circle, a fact that we already knew. When $n = 3$, we find that $\mathbf{SO}(3)/\mathbf{SO}(2) \cong S^2$. This says that $\mathbf{SO}(3)$ is somehow the result of glueing circles to the surface of a sphere (in $\mathbb{R}^3$), in such a way that these circles do not intersect. This is hard to visualize!

A similar argument for the complex unit sphere, Σ^{n-1}, shows that

$$\mathbf{SU}(n)/\mathbf{SU}(n-1) \cong \Sigma^{n-1} \cong S^{2n-1}.$$

Again, we identify $\mathbf{SU}(n-1)$ with a subgroup of $\mathbf{SU}(n)$, as in the real case. In particular, when $n = 2$, as $\mathbf{SU}(1) = \{1\}$, we find that

$$\mathbf{SU}(2) \cong S^3,$$

i.e., the group $\mathbf{SU}(2)$ is topologically the sphere S^3! Actually, this is not surprising if we remember that $\mathbf{SU}(2)$ is in fact the group of unit quaternions.

(b) We saw in Example 2 that the action, $\cdot\colon \mathbf{SL}(2,\mathbb{R}) \times H \to H$, of the group $\mathbf{SL}(2,\mathbb{R})$ on the upper half plane is transitive. Let us find out what the stabilizer of $z = i$ is. We should have

$$\frac{ai + b}{ci + d} = i,$$

that is, $ai + b = -c + di$, i.e.,

$$(d - a)i = b + c.$$

Since a, b, c, d are real, we must have $d = a$ and $b = -c$. Moreover, $ad - bc = 1$, so we get $a^2 + b^2 = 1$. We conclude that a matrix in $\mathbf{SL}(2, \mathbb{R})$ fixes i iff it is of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad \text{with} \quad a^2 + b^2 = 1.$$

Clearly, these are the rotation matrices in $\mathbf{SO}(2)$ and so, the stabilizer of i is $\mathbf{SO}(2)$. We conclude that

$$\mathbf{SL}(2, \mathbb{R})/\mathbf{SO}(2) \cong H.$$

This time, we can view $\mathbf{SL}(2, \mathbb{R})$ as the result of gluing circles to the upper half plane. This is not so easy to visualize. There is a better way to visualize the topology of $\mathbf{SL}(2, \mathbb{R})$ by making it act on the open disk, D.

Now, consider the action of $\mathbf{SL}(2, \mathbb{C})$ on $\mathbb{C} \cup \{\infty\} \cong S^2$. As it is transitive, let us find the stabilizer of $z = 0$. We must have

$$\frac{b}{d} = 0,$$

and as $ad - bc = 1$, we must have $b = 0$ and $ad = 1$. Thus, the stabilizer of 0 is the subgroup, $\mathbf{SL}(2, \mathbb{C})_0$, of $\mathbf{SL}(2, \mathbb{C})$ consisting of all matrices of the form

$$\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}, \quad \text{where} \quad a \in \mathbb{C} - \{0\} \quad \text{and} \quad c \in \mathbb{C}.$$

We get

$$\mathbf{SL}(2, \mathbb{C})/\mathbf{SL}(2, \mathbb{C})_0 \cong \mathbb{C} \cup \{\infty\} \cong S^2,$$

but this is not very illuminating.

(c) In Example 3, we considered the action, $\cdot\colon \mathbf{GL}(n) \times \mathbf{SPD}(n) \to \mathbf{SPD}(n)$, of $\mathbf{GL}(n)$ on $\mathbf{SPD}(n)$, the set of symmetric positive definite matrices. As this action is transitive, let us find the stabilizer of I. For any $A \in \mathbf{GL}(n)$, the matrix A stabilizes I iff

$$AIA^\top = AA^\top = I.$$

Therefore, the stabilizer of I is $\mathbf{O}(n)$ and we find that

$$\mathbf{GL}(n)/\mathbf{O}(n) = \mathbf{SPD}(n).$$

Observe that if $\mathbf{GL}^+(n)$ denotes the subgroup of $\mathbf{GL}(n)$ consisting of all matrices with a strictly positive determinant, then we have an action $\cdot\colon \mathbf{GL}^+(n) \times \mathbf{SPD}(n) \to \mathbf{SPD}(n)$ of $\mathbf{GL}^+(n)$ on $\mathbf{SPD}(n)$. This action is transtive and we find that the stabilizer of I is $\mathbf{SO}(n)$; consequently, we get

$$\mathbf{GL}^+(n)/\mathbf{SO}(n) = \mathbf{SPD}(n).$$

(d) In Example 4, we considered the action, $\cdot\colon \mathbf{SO}(n+1) \times \mathbb{RP}^n \to \mathbb{RP}^n$, of $\mathbf{SO}(n+1)$ on the (real) projective space, $\mathbb{RP}^n$. As this action is transitive, let us find the stabilizer of

the line, $L = [e_1]$, where $e_1 = (1, 0, \ldots, 0)$. For any $R \in \mathbf{SO}(n+1)$, the line L is fixed iff either $R(e_1) = e_1$ or $R(e_1) = -e_1$, since e_1 and $-e_1$ define the same line. As R is orthogonal with $\det(R) = 1$, this means that R is of the form

$$R = \begin{pmatrix} \alpha & 0 \\ 0 & S \end{pmatrix}, \quad \text{with} \quad \alpha = \pm 1 \quad \text{and} \quad \det(S) = \alpha.$$

But, S must be orthogonal, so we conclude $S \in \mathbf{O}(n)$. Therefore, the stabilizer of $L = [e_1]$ is isomorphic to the group $\mathbf{O}(n)$ and we find that

$$\mathbf{SO}(n+1)/\mathbf{O}(n) \cong \mathbb{RP}^n.$$

Strictly speaking, $\mathbf{O}(n)$ is not a subgroup of $\mathbf{SO}(n+1)$, so the above equation does not make sense. We should write

$$\mathbf{SO}(n+1)/\widetilde{\mathbf{O}}(n) \cong \mathbb{RP}^n,$$

where $\widetilde{\mathbf{O}}(n)$ is the subgroup of $\mathbf{SO}(n+1)$ consisting of all matrices of the form

$$\begin{pmatrix} \alpha & 0 \\ 0 & S \end{pmatrix}, \quad \text{with} \quad S \in \mathbf{O}(n),\ \alpha = \pm 1 \quad \text{and} \quad \det(S) = \alpha.$$

However, the common practice is to write $\mathbf{O}(n)$ instead of $\widetilde{\mathbf{O}}(n)$.

We should mention that $\mathbb{RP}^3$ and $\mathbf{SO}(3)$ are homeomorphic spaces. This is shown using the quaternions, for example, see Gallier [6], Chapter 8.

A similar argument applies to the action, $\cdot\colon \mathbf{SU}(n+1) \times \mathbb{CP}^n \to \mathbb{CP}^n$, of $\mathbf{SU}(n+1)$ on the (complex) projective space, $\mathbb{CP}^n$. We find that

$$\mathbf{SU}(n+1)/\mathbf{U}(n) \cong \mathbb{CP}^n.$$

Again, the above is a bit sloppy as $\mathbf{U}(n)$ is not a subgroup of $\mathbf{SU}(n+1)$. To be rigorous, we should use the subgroup, $\widetilde{\mathbf{U}}(n)$, consisting of all matrices of the form

$$\begin{pmatrix} \alpha & 0 \\ 0 & S \end{pmatrix}, \quad \text{with} \quad S \in \mathbf{U}(n),\ |\alpha| = 1 \quad \text{and} \quad \det(S) = \overline{\alpha}.$$

The common practice is to write $\mathbf{U}(n)$ instead of $\widetilde{\mathbf{U}}(n)$. In particular, when $n = 1$, we find that

$$\mathbf{SU}(2)/\mathbf{U}(1) \cong \mathbb{CP}^1.$$

But, we know that $\mathbf{SU}(2) \cong S^3$ and, clearly, $\mathbf{U}(1) \cong S^1$. So, again, we find that $S^3/S^1 \cong \mathbb{CP}^1$ (but we know, more, namely, $S^3/S^1 \cong S^2 \cong \mathbb{CP}^1$.)

(e) We now consider a generalization of projective spaces (real and complex). First, consider the real case. Given any $n \geq 1$, for any k, with $0 \leq k \leq n$, let $G(k, n)$ be the

set of all linear k-dimensional subspaces of $\mathbb{R}^n$ (also called *k-planes*). Any k-dimensional subspace, U, of $\mathbb{R}$ is spanned by k linearly independent vectors, $u_1, \ldots, u_k$, in $\mathbb{R}^n$; write $U = \mathrm{span}(u_1, \ldots, u_k)$. We can define an action, $\cdot\colon \mathbf{O}(n) \times G(k,n) \to G(k,n)$, as follows: For any $R \in \mathbf{O}(n)$, for any $U = \mathrm{span}(u_1, \ldots, u_k)$, let

$$R \cdot U = \mathrm{span}(Ru_1, \ldots, Ru_k).$$

We have to check that the above is well defined. If $U = \mathrm{span}(v_1, \ldots, v_k)$ for any other k linearly independent vectors, $v_1, \ldots, v_k$, we have

$$v_i = \sum_{j=1}^{k} a_{ij} u_j, \quad 1 \leq i \leq k,$$

for some $a_{ij} \in \mathbb{R}$, and so,

$$Rv_i = \sum_{j=1}^{k} a_{ij} Ru_j, \quad 1 \leq i \leq k,$$

which shows that

$$\mathrm{span}(Ru_1, \ldots, Ru_k) = \mathrm{span}(Rv_1, \ldots, Rv_k),$$

i.e., the above action is well defined. This action is transitive. This is because if U and V are any two k-planes, we may assume that $U = \mathrm{span}(u_1, \ldots, u_k)$ and $V = \mathrm{span}(v_1, \ldots, v_k)$, where the u_i's form an orthonormal family and similarly for the v_i's. Then, we can extend these families to orthonormal bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ or $\mathbb{R}^n$, and w.r.t. the orthonormal basis $(u_1, \ldots, u_n)$, the matrix of the linear map sending u_i to v_i is orthogonal. Thus, it is enough to find the stabilizer of any k-plane. Pick $U = \mathrm{span}(e_1, \ldots, e_k)$, where $(e_1, \ldots, e_n)$ is the canonical basis of $\mathbb{R}^n$ (i.e., $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, with the 1 in the ith position). Now, any $R \in \mathbf{O}(n)$ stabilizes U iff R maps $e_1, \ldots, e_k$ to k linearly independent vectors in the subspace $U = \mathrm{span}(e_1, \ldots, e_k)$, i.e., R is of the form

$$R = \begin{pmatrix} S & 0 \\ 0 & T \end{pmatrix},$$

where S is $k \times k$ and T is $(n-k) \times (n-k)$. Moreover, as R is orthogonal, S and T must be orthogonal, i.e., $S \in \mathbf{O}(k)$ and $T \in \mathbf{O}(n-k)$. We deduce that the stabilizer of U is isomorphic to $\mathbf{O}(k) \times \mathbf{O}(n-k)$ and we find that

$$\mathbf{O}(n)/(\mathbf{O}(k) \times \mathbf{O}(n-k)) \cong G(k,n).$$

It turns out that this makes $G(k,n)$ into a smooth manifold of dimension $k(n-k)$ called a *Grassmannian*.

The restriction of the action of $\mathbf{O}(n)$ on $G(k,n)$ to $\mathbf{SO}(n)$ yields an action, $\cdot\colon \mathbf{SO}(n) \times G(k,n) \to G(k,n)$, of $\mathbf{SO}(n)$ on $G(k,n)$. Then, it is easy to see that the stabilizer of the

subspace U is isomorphic to the subgroup, $S(\mathbf{O}(k) \times \mathbf{O}(n-k))$, of $\mathbf{SO}(n)$ consisting of the rotations of the form

$$R = \begin{pmatrix} S & 0 \\ 0 & T \end{pmatrix},$$

with $S \in \mathbf{O}(k)$, $T \in \mathbf{O}(n-k)$ and $\det(S)\det(T) = 1$. Thus, we also have

$$\mathbf{SO}(n)/S(\mathbf{O}(k) \times \mathbf{O}(n-k)) \cong G(k,n).$$

If we recall the projection $pr\colon \mathbb{R}^{n+1} - \{0\} \to \mathbb{RP}^n$, by definition, a *k-plane* in $\mathbb{RP}^n$ is the image under pr of any $(k+1)$-plane in $\mathbb{R}^{n+1}$. So, for example, a line in $\mathbb{RP}^n$ is the image of a 2-plane in $\mathbb{R}^{n+1}$, and a hyperplane in $\mathbb{RP}^n$ is the image of a hyperplane in $\mathbb{R}^{n+1}$. The advantage of this point of view is that the k-planes in $\mathbb{RP}^n$ are arbitrary, i.e., they do not have to go through "the origin" (which does not make sense, anyway!). Then, we see that we can interpret the Grassmannian, $G(k+1, n+1)$, as a space of "parameters" for the k-planes in $\mathbb{RP}^n$. For example, $G(2, n+1)$ parametrizes the lines in $\mathbb{RP}^n$. In this viewpoint, $G(k+1, n+1)$ is usually denoted $\mathbb{G}(k,n)$.

It can be proved (using some exterior algebra) that $G(k,n)$ can be embedded in $\mathbb{RP}^{\binom{n}{k}-1}$. Much more is true. For example, $G(k,n)$ is a projective variety, which means that it can be defined as a subset of $\mathbb{RP}^{\binom{n}{k}-1}$ equal to the zero locus of a set of homogeneous equations. There is even a set of quadratic equations, known as the *Plücker equations*, defining $G(k,n)$. In particular, when $n = 4$ and $k = 2$, we have $G(2,4) \subseteq \mathbb{RP}^5$ and $G(2,4)$ is defined by a single equation of degree 2. The Grassmannian $G(2,4) = \mathbb{G}(1,3)$ is known as the *Klein quadric*. This hypersurface in $\mathbb{RP}^5$ parametrizes the lines in $\mathbb{RP}^3$.

Complex Grassmannians are defined in a similar way, by replacing $\mathbb{R}$ by $\mathbb{C}$ and $\mathbf{O}(n)$ by $\mathbf{U}(n)$ throughout. The complex Grassmannian, $G_{\mathbb{C}}(k,n)$, is a complex manifold as well as a real manifold and we have

$$\mathbf{U}(n)/(\mathbf{U}(k) \times \mathbf{U}(n-k)) \cong G_{\mathbb{C}}(k,n).$$

As in the case of the real Grassmannians, the action of $\mathbf{U}(n)$ on $G_{\mathbb{C}}(k,n)$ yields an action of $\mathbf{SU}(n)$ on $G_{\mathbb{C}}(k,n)$ and we get

$$\mathbf{SU}(n)/S(\mathbf{U}(k) \times \mathbf{U}(n-k)) \cong G_{\mathbb{C}}(k,n),$$

where $S(\mathbf{U}(k) \times \mathbf{U}(n-k))$ is the subgroup of $\mathbf{SU}(n)$ consisting of all matrices, $R \in \mathbf{SU}(n)$, of the form

$$R = \begin{pmatrix} S & 0 \\ 0 & T \end{pmatrix},$$

with $S \in \mathbf{U}(k)$, $T \in \mathbf{U}(n-k)$ and $\det(S)\det(T) = 1$.

(f) Consider the action of $G = \mathbf{GL}(2,\mathbb{C})$ on $\mathbb{C}^2$ given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix}.$$

This action is not transitive. The stabilizer of any point of $\mathbb{C}^2$ is given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix},$$

that is

$$\begin{aligned} (\alpha - 1)x + \beta y &= 0 \\ \gamma x + (\delta - 1)y &= 0. \end{aligned}$$

If $x = y = 0$, then the stabilizer G_0 is all of G. Otherwise, we must have

$$\det \begin{pmatrix} \alpha - 1 & \beta \\ \gamma & \delta - 1 \end{pmatrix} = 0.$$

If $x = 0$ and $y \neq 0$, then we must have $\delta = 1, \beta = 0$. In this case,

$$\operatorname{stab} \begin{pmatrix} 0 \\ y \end{pmatrix} = \left\{ \begin{pmatrix} \alpha & 0 \\ \gamma & 1 \end{pmatrix} \mid \alpha \neq 0 \right\}.$$

If $x \neq 0$ and $y = 0$, then we must have $\alpha = 1, \gamma = 0$. In this case,

$$\operatorname{stab} \begin{pmatrix} x \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & \beta \\ 0 & \delta \end{pmatrix} \mid \delta \neq 0 \right\}.$$

If $x, y \neq 0$, then

$$\operatorname{stab} \begin{pmatrix} x \\ y \end{pmatrix} = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \beta = -\frac{(\alpha - 1)x}{y}, \gamma = -\frac{(\delta - 1)y}{x}, \alpha + \delta - 1 \neq 0 \right\}.$$

Note that the condition $(\alpha - 1)(\delta - 1) - \beta\gamma = 0$ holds trivially.

(g) Let

$$G = \left\{ \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \mid \xi \in \mathbb{R} \right\}$$

and consider the linear action of G on $\mathbb{R}^2$, that is

$$\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + \xi y \\ y \end{pmatrix}.$$

The elements of G are shear transformations. The stabilizer of a point is given by

$$\begin{aligned} x + \xi y &= x \\ y &= y, \end{aligned}$$

that is,

$$\xi y = 0.$$

If $y = 0$, then

$$\text{stab}\begin{pmatrix} x \\ 0 \end{pmatrix} = G$$

and every point of the real line is an orbit, else

$$\text{stab}\begin{pmatrix} x \\ y \end{pmatrix} = \{I\}$$

and the orbit of $\begin{pmatrix} x \\ y \end{pmatrix}$ is the line through $(0, y)$.

(e) Our last example is the group of symmetries of an equilateral triangle whose centroid is taken as the origin; see Figure 1.2.

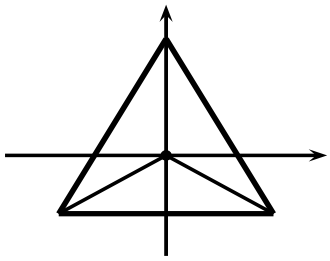


Figure 1.2: Symmetries of an equilateral triangle

We have the rotation by $2\pi/3$, denoted σ, and the reflection about the y-axis, denoted τ. It is easy to check that

$$\begin{aligned} \tau\sigma^2 &= \sigma\tau \\ \sigma^3 &= I \\ \tau^2 &= I. \end{aligned}$$

The group generated by σ and τ and satisfying the above equations is the group of rigid motions of the triangle. This group is isomorphic to the permutation group of 3 elements, $\mathfrak{S}_3$. Obviously, this group acts on the triangle. We can define other actions of this group, for example on $\mathbb{R}^3$, *via*

$$\begin{aligned} e_1 &\mapsto e_{\sigma(1)} \\ e_2 &\mapsto e_{\sigma(2)} \\ e_3 &\mapsto e_{\sigma(3)}, \end{aligned}$$

for every $\sigma \in \mathfrak{S}_3$, where (e_1, e_2, e_3) is the canonical basis of $\mathbb{R}^3$.

1.2 Haar Integral and Maschke's Theorem

Let G be a group, let V be a vector space over $\mathbb{C}$, and write

$$\mathrm{Fcn}(G,\mathbb{C}) \quad \text{resp.} \quad \mathrm{Fcn}(G,V),$$

for the set of all functions from G to $\mathbb{C}$, resp. from G to V.

When G is a *locally compact* topological group, Haar proved (1931):

Theorem 1.3. *There is a notion of integral on G, so that for every continuous function f with compact support, the integral $\int_G f(\sigma)d\sigma \in \mathbb{C}$ is invariant under left translation, which means that*

$$\int_G f(\tau\sigma)d\sigma = \int_G f(\sigma)d\sigma, \quad \textit{for all} \quad \tau \in G. \tag{$*$}$$

This integral is unique up a to multiplicative constant.

Examples.

(1) $G = \mathbb{R}$ under addition. In this case

$$\int_{\mathbb{R}} f(x)dx$$

is the ordinary integral $\int_{-\infty}^{\infty} f(x)dx$. For any $y \in G = \mathbb{R}$, we have

$$\int_{-\infty}^{\infty} f(y+x)dx = \int_{-\infty}^{\infty} f(x)dx.$$

(2) $G = \mathbb{R}^*_{>0}$ (the positive reals under multiplication).

We need to find an integral of the form

$$\int_0^{\infty} f(x)w(x)dx$$

satisfying the identity

$$\int_0^{\infty} f(yx)w(x)dx = \int_0^{\infty} f(u)w(u)du.$$

If we let $u = yx$, then $du = ydx$, and we should have

$$\int_0^{\infty} f(yx)w(x)dx = \int_0^{\infty} f(u)w\left(\frac{u}{y}\right)\frac{du}{y} = \int_0^{\infty} f(u)w(u)du.$$

Thus, the following equation should hold:

$$\frac{1}{y}w\left(\frac{u}{y}\right) = w(u), \quad \text{for all } u \in \mathbb{R}^*_{>0}.$$

If we pick

$$w(u) = \frac{1}{u},$$

then,

$$\frac{1}{y} w\left(\frac{u}{y}\right) = \frac{1}{y}\frac{y}{u} = \frac{1}{u} = w(u),$$

which shows that it is a good choice. In fact, this is the only choice that works, so the Haar integral on $\mathbb{R}^*_{>0}$ is given by

$$\int_0^\infty f(x)\frac{dx}{x}.$$

Before we consider the example of finite groups, let us note the following important fact about the Haar integral:

Remark: If G is a *compact* group, then

$$\int_G 1 d\sigma \quad \text{is finite.}$$

To prove this, take a small open neighborhood of 1 in G, say U. For any $\sigma \in G$, the image σU of U is an open subset around σ (because multiplication by σ is a homeomorphism). Since the measure of U is finite, so is the measure of σU. The family $\{\sigma U\}_{\sigma \in G}$ is an open cover of G, and since G is compact (Heine–Borel), it has a finite subcover, say $\sigma_1 U, \ldots, \sigma_l U$. It follows that

$$\text{meas}(G) \leq l \,\text{meas}(U) < \infty.$$

However,

$$\text{meas}(G) = \int_G 1 d\sigma,$$

which proves our remark. In fact, it can be shown that meas(G) is finite iff G is compact.

If G is compact, it turns out that the Haar measure is both left and right invariant. So, we also have

$$\int_G f(\sigma\tau) d\sigma = \int_G f(\sigma) d\sigma, \quad \text{for all} \quad \tau \in G. \qquad (**)$$

When the left-invariant Haar measure on a group is also right-invariant, we say that the group is *unimodular*.

If G is compact, then we have the *normalized Haar measure*, which is the Haar measure for which

$$\int_G 1 d\sigma = 1.$$

(3) Finite groups.

The Haar integral on a finite group is given by

$$\int_G f(\sigma)d\sigma = \frac{1}{\#(G)}\sum_{\sigma\in G} f(\sigma).$$

(Here $\#(G)$ denotes the number of elements in G.) For a finite group, the Haar integral computes the "average value" of f. A finite group is discrete (which means that every one-element subset is open), and the Haar measure is a Borel measure (every open set is measurable). The measure of a one-point set is given by

$$\text{meas}(\{\text{pt}\}) = \frac{1}{\#(G)}.$$

(4) Arbitrary Discrete Groups

Every compact discrete set is finite, so a function f on G with compact support is nonzero only on a finite subset. Also, the Haar measure of a one-point set is 1, so

$$\int_G f(\sigma)d\sigma = \sum_{\sigma\in G} f(\sigma).$$

It is now time to define group representations.

Definition 1.6. A (linear) *representation* of a (topological) group G is an action R on a complex vector space V, called the *representation space* of R, which means that there is a homomorphism $R\colon G \to \mathbf{GL}(V)$, that associates an invertible linear map $R_\sigma \in \mathbf{GL}(V)$ to every $\sigma \in G$. Furthermore, the map $\sigma \mapsto R_\sigma(v)$ is continuous for all $v \in V$. If V is finite-dimensional, we say that we have a representation of *finite degree*, and the *degree of* R is the dimension of V.

Among all representations, we have the *trivial representation*, which maps every $\sigma \in G$ to the identity in $\mathbf{GL}(V)$.

Definition 1.7. Given a representation $R\colon G \to \mathbf{GL}(V)$, a *subrepresentation* S of R consists of

(1) A subspace W of V, such that

(2) W is stable under R, which means that for every $\sigma \in G$ and all $w \in W$, we have $R_\sigma(w) \in W$. We let S_σ be the restriction of R_σ to W.

The notion of isomorphism of representations is defined as follows:

Definition 1.8. Let $R\colon G \to \mathbf{GL}(V)$ and $S\colon G \to \mathbf{GL}(W)$ be two representations of G. Then we say that R is *isomorphic* to S, denoted $R \cong S$, iff

(1) There exists a fixed linear isomorphism $L\colon V \to W$, and

(2) The following diagram commutes for all $\sigma \in G$:

$$\begin{array}{ccc} V & \xrightarrow{R_\sigma} & V \\ {\scriptstyle L}\downarrow & & \downarrow{\scriptstyle L} \\ W & \xrightarrow[S_\sigma]{} & W, \end{array}$$

which is equivalent to

$$LR_\sigma = S_\sigma L, \quad \text{for all} \quad \sigma \in G. \tag{$*$}$$

Remark: Without assuming that the linear map $L\colon V \to W$ is an isomorphism, if $(*)$ holds, then we say that L *intertwines* R and S.

Theorem 1.4. *(Maschke's Theorem, 1898) Say $R\colon G \to \mathbf{GL}(V)$ is a representation of a finite or compact group G, and $S\colon G \to \mathbf{GL}(W)$ is a subrepresentation of R. Then, there exists a subspace Z of V which is stable under R and complementary to W; that is,*

$$V = W \coprod Z.$$

(The above means that $W \cap Z = (0)$, and that every $v \in V$ can be written as $v = w + z$, for some $w \in W$ and some $z \in Z$, which are uniquely determined by v.) That Z is stable under R means that $R_\sigma(Z) \subseteq Z$, for all $\sigma \in G$.

Proof. Pick any supplement W' of W in V (so that $V = W \coprod W'$), and let P be the projection of V onto W (a stable subspace of V); since every $v \in V$ is expressed as $v = w + w'$ in a unique way, with $w \in W$ and $w' \in W'$, we have $P(v) = w$. Then, we know that $P^2 = P$ and that the restriction of P to W is the identity. Since W is stable under R, we have $R_\sigma(w) \in W$ for all $\sigma \in G$, and so

$$PR_\sigma(w) = R_\sigma(w).$$

Let Q be the linear map on V given by

$$Q(v) = \int_G R_\sigma P R_\sigma^{-1}(v) d\sigma.$$

We have the following properties:

(a) If $v \in V$, then

$$Q(v) \in W.$$

This is because

$$R_\sigma P R_\sigma^{-1}(v) = R_\sigma(P(R_\sigma^{-1}(v))) = R_\sigma(w) \in W,$$

since $w = P(R_\sigma^{-1}(v)) \in W$. Then,

$$Q(v) = \int_G R_\sigma P R_\sigma^{-1}(v) d\sigma \in W.$$

(b) The restriction of Q to W is the identity.

Pick $w \in W$, and consider

$$Q(w) = \int_G R_\sigma P R_\sigma^{-1}(w) d\sigma.$$

Since $R_\sigma^{-1}(w) \in W$ and since P is the identity of W, we have $PR_\sigma^{-1}(w) = R_\sigma^{-1}(w)$, so we get

$$Q(w) = \int_G R_\sigma R_\sigma^{-1}(w) d\sigma = \int_G w d\sigma = w.$$

(c) $Q^2 = Q$ and

$$R_\tau Q = Q R_\tau, \quad \text{for all} \quad \tau \in G.$$

By (a), we have $Q(v) \in W$ for all $v \in V$, and by (b) the restriction of Q to W is the identity, so $Q^2 = Q$. We have

$$\begin{aligned} R_\tau Q R_\tau^{-1} &= \int_G R_\tau R_\sigma P R_\sigma^{-1} R_\tau^{-1} d\sigma \\ &= \int_G R_{\tau\sigma} P R_{\tau\sigma}^{-1} d\sigma \\ &= \int_G R_\sigma P R_\sigma^{-1} d\sigma \\ &= Q, \end{aligned}$$

where we used the invariance under left translation of the Haar integral going from line 2 to line 3. Thus,

$$R_\tau Q R_\tau^{-1} = Q,$$

which implies that

$$R_\tau Q = Q R_\tau, \quad \text{for all} \quad \tau \in G.$$

From (b) and (c), we conclude that Q is the projection of V onto W.

Now, let $Z = \operatorname{Ker} Q$. Since $Q(z) = 0$ for all $z \in Z$, $R_\tau Q(z) = 0$ implies that $QR_\tau(z) = 0$, and thus $R_\tau(z) \in \operatorname{Ker} Q = Z$. This show that Z is stable under R.

If $x \in W \cap Z$, then $Q(x) = x$ by (b), but $Q(x) = 0$ since $x \in Z$, so $x = 0$. Therefore,

$$W \cap Z = (0).$$

Since every v can be written as

$$v = Q(v) + v - Q(v),$$

and since

$$Q(v - Q(v)) = Q(v) - Q^2(v) = Q(v) - Q(v) = 0,$$

we have $v - Q(v) \in Z$. This shows that

$$V = W + Z,$$

and with $W \cap Z = (0)$, we have

$$V = W \coprod Z,$$

with both W and Z stable under R. □

Definition 1.9. A representation $R\colon G \to \mathbf{GL}(V)$ is *irreducible* if $V \neq (0)$ and if for every subrepresentation $S\colon G \to \mathbf{GL}(W)$ of R, either

(a) $W = (0)$ and $S_g = 0$ for all $g \in G$, or

(b) $W = V$ and $S = R$.

It is customary to abbreviate *irreducible representation* by *irrep*.

Maschke's Theorem (Theorem 1.4) has the following important corollary:

Corollary 1.5. *If $R\colon G \to \mathbf{GL}(V)$ is a finite dimensional representation of a finite or compact group G, then it is a finite coproduct of irreducible representations of G.*

Proof. We proceed by induction on $\dim(V)$. If $R\colon G \to \mathbf{GL}(V)$ is already irreducible, we are done. If not, there is some nontrivial subspace W of V such that R restricted to W is a subrepresentation of R. By Maschke's Theorem, there exists a complementary subrepresentation (R, Z) with $V = W \coprod Z$, and we have

$$\dim(W) < \dim(V) \quad \text{and} \quad \dim(Z) < \dim(V).$$

By the induction hypothesis, we can write

$$W = W_1 \coprod \cdots \coprod W_l$$

and

$$Z = Z_1 \coprod \cdots \coprod Z_m,$$

where the subrepresentations $R\colon G \to \mathbf{GL}(W_i)$ and $R\colon G \to \mathbf{GL}(Z_j)$ are all irreducible, so

$$V = W_1 \coprod \cdots \coprod W_l \coprod Z_1 \coprod \cdots \coprod Z_m$$

yields a coproduct of irreducible subrepresentation of R. □

The property of representations stated in Corollary 1.5 is known as *complete reducibilty* or *semisimplicity*.

In practice, we have a finite set $\{x_1, \ldots, x_t\}$ of data on which a finite group G acts. Consider the finite set

$$\{R_\sigma(x_j) \mid j = 1, \ldots, t;\ \sigma \in G\}.$$

Make the vector space with the $R_\sigma(x_j)$ spanning it. This is a finite vector space V and $R\colon G \to \mathbf{GL}(V)$ is a finite-dimensional representation of G.

Proposition 1.6. *If G is a finite group and $R\colon G \to \mathbf{GL}(V)$ is an irreducible representation of G, then* $\dim(V)$ *is finite. Moreover, V is the span of any orbit $O(v)$, where $v \in V$.*

Proof. Pick any $v \in V$ and consider the orbit

$$O(v) = \{\sigma v \mid \sigma \in G\}.$$

Observe that

$$W = \mathrm{span}(O(v)) = \left\{ \sum_{\sigma \in G} a_\sigma(\sigma v) \mid a_\sigma \in \mathbb{C} \right\}.$$

Then, $R\colon G \to \mathbf{GL}(W)$ is a subrepresentation of R with $v \in W$. But R is irreducible, so we must have $W = V$. □

In particular, observe that Proposition 1.6 implies that $\dim(V) \leq \#(G)$.

We now explain how inner products help in studying representations. Recall that a *Hermitian inner product* on a complex vector space V is a map $V \times V \to \mathbb{C}$, whose value for $v, v' \in V$ is denoted by (v, v'), such that

1. $(v + w, v') = (v, v') + (w, v')$
2. $(\lambda v, v') = \lambda(v, v')$
3. $(v', v) = \overline{(v, v')}$
4. $(v, v) \geq 0$ and $(v, v) = 0$ iff $v = 0$.

If V is finite-dimensional, then V has lots of Hermitian inner products. For example, for any basis $(e_1, \ldots, e_n)$, if we write $u = \sum_i u_i e_i$ and $v = \sum_j v_j e_j$, then

$$(u, v) = \sum_{i=1}^{n} u_i \overline{v}_i$$

is a Hermitian inner product on V.

Assume G is a locally compact group and let $d\sigma$ be a Haar measure on G. We define $L^2(G, d\sigma)$ as the function space

$$L^2(G, d\sigma) = \left\{ f \mid f \colon G \to \mathbb{C},\ f \text{ is measurable and } \int_G |f(\sigma)|^2 d\sigma < \infty \right\}.$$

There is a Hermitian inner product on $L^2(G, d\sigma)$ given by

$$(f, g) = \int_G f(\sigma)\overline{g(\sigma)} d\sigma.$$

Proposition 1.7. *Let $R \colon G \to \mathbf{GL}(V)$ be a representation where V is an inner product space (the inner product is denoted by (x, y)). Assume G is finite or compact and set*

$$(x, y)_G = \int_G (\sigma x, \sigma y) d\sigma.$$

Then, we have

$$(\tau x, \tau y)_G = (x, y)_G, \quad \textit{for all} \quad \tau \in G.$$

Proof. By definition

$$(\tau x, \tau y)_G = \int_G (\sigma\tau x, \sigma\tau y) d\sigma,$$

and since a compact group is unimodular, the Haar measure is right invariant, so

$$(\tau x, \tau y)_G = \int_G (\sigma\tau x, \sigma\tau y) d\sigma = \int_G (\sigma x, \sigma y) d\sigma = (x, y)_G,$$

as claimed. □

Observe that with respect to the inner product $(-, -)_G$, the linear maps R_τ are unitary operators, since

$$(R_\tau(x), R_\tau(y))_G = (\tau x, \tau y)_G = (x, y)_G.$$

Thus, R is a unitary representation, for short a *unirep*. We also abbreviate *unitary irreducible representation* by *unirrep*!

Using Proposition 1.7, we can give another proof of Maschke's Theorem.

Another proof of Maschke's Theorem. Consider the Hermitian inner product $(-, -)_G$ on V. Then, R is a unirep. Let $W^\perp$ be the orthogonal complement of W in V (recall that $W^\perp = \{x \in V \mid (x, y)_G = 0, \quad \text{for all} \quad y \in W\}$). Because W is stable under R, it is easy to check that $W^\perp$ is also stable under W. Since

$$V = W \coprod W^\perp,$$

the restriction of R to $W^\perp$ does the job. □

Remark: The irreducible representations involved in Corollary 1.5 are almost unique. The problem is that all the W_j could be one-dimensional spaces and R could be the trivial on each W_j. In this case, uniqueness fails.

1.3 Characters, Schur's Lemma and Orthogonality Relations

In this section, we assume that $R\colon G \to \mathbf{GL}(V)$ is a unitary representation on V, with $\dim(V) < \infty$. For any basis of V, each R_σ is represented by a unitary matrix also denoted R_σ, so the trace $\mathrm{tr}(R_\sigma)$ of R_σ is well-defined. If we change basis, the new matrix is of the form $PR_\sigma P^{-1}$, whose trace is $\mathrm{tr}(PR_\sigma P^{-1})$. However, for any two matrices A, B, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, so we have

$$\mathrm{tr}(PR_\sigma P^{-1}) = \mathrm{tr}(P^{-1}PR_\sigma) = \mathrm{tr}(R_\sigma),$$

which shows that the trace of R_σ does not depend on the basis.

Definition 1.10. We denote $\mathrm{tr}(R_\sigma)$ by $\chi_R(\sigma)$, and we call the function $\sigma \mapsto \chi_R(\sigma)$ the *character* of the representation $R\colon G \to \mathbf{GL}(V)$.

Sorites.

(1) For any unirep $R\colon G \to \mathbf{GL}(V)$, If $V = W \coprod Z$ and if W and Z are stable under R, then

$$\chi_R(\sigma) = \chi_{R|W}(\sigma) + \chi_{R|Z}(\sigma).$$

(2) $\chi_R(\sigma^{-1}) = \overline{\chi_R(\sigma)}$.

(3) For all $\sigma, \tau \in G$, we have

$$\chi_R(\tau^{-1}\sigma\tau) = \chi_R(\sigma).$$

(4) $\chi_R(1) = \dim(V) = \deg(R, V)$.

Proof. (1) Since $V = W \coprod Z$, we can form a basis of V using a basis of W and a basis of Z. The matrix of R_σ with respect to this basis is a block matrix of the form

$$A_V = \begin{pmatrix} A_W & 0 \\ 0 & A_Z \end{pmatrix},$$

which implies

$$\mathrm{tr}(A_V) = \mathrm{tr}(A_W) + \mathrm{tr}(A_Z).$$

(2) Since R_σ is a unitary matrix, its eigenvalues are unit complex numbers. Furthermore, as $R_{\sigma^{-1}} = R_\sigma^{-1}$, the eigenvalues of $R_{\sigma^{-1}}$ are of the form $\lambda^{-1} = \overline{\lambda}/|\lambda|^2$, where each λ is an eigenvalue of R_σ. But $|\lambda| = 1$, so $\lambda^{-1} = \overline{\lambda}$. Now,

$$\chi_R(\sigma) = \mathrm{tr}(R_\sigma) = \lambda_1 + \cdots + \lambda_n,$$

where $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of R_σ and

$$\chi_R(\sigma^{-1}) = \mathrm{tr}(R_\sigma^{-1}) = \lambda_1^{-1} + \cdots + \lambda_n^{-1} = \overline{\lambda}_1 + \cdots + \overline{\lambda}_n = \overline{\mathrm{tr}(R_\sigma)} = \overline{\chi_R(\sigma)}.$$

(3) As we mentioned before, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for any two matrices A, B, so we get

$$\chi_R(\tau\sigma\tau^{-1}) = \mathrm{tr}(R_{\tau\sigma\tau^{-1}}) = \mathrm{tr}(R_\tau R_\sigma R_\tau^{-1}) = \mathrm{tr}(R_\sigma) = \chi_R(\sigma).$$

(4) If I is the $n \times n$ identity matrix, then $\mathrm{tr}(I) = n$, so

$$\chi_R(1) = \mathrm{tr}(R_1) = \mathrm{tr}(I) = n = \dim(V).$$

□

Any function $f\colon G \to \mathbb{C}$ which is constant on conjugacy classes of G is called a *class function*. By (3), every character is a class function.

Schur's lemma is a simple yet powerful result about intertwiners of irreducible representations. First, let us discuss how to make intertwiners using the Haar integral.

If $R\colon G \to \mathbf{GL}(V)$ and $S\colon G \to \mathbf{GL}(W)$ are two representations of G, recall that a linear map $\Lambda\colon V \to W$ *intertwines* R and S iff the following diagram commutes for all $\sigma \in G$:

$$\begin{array}{ccc} V & \xrightarrow{R_\sigma} & V \\ {\scriptstyle\Lambda}\downarrow & & \downarrow{\scriptstyle\Lambda} \\ W & \xrightarrow[S_\sigma]{} & W, \end{array}$$

which is equivalent to

$$\Lambda R_\sigma = S_\sigma \Lambda, \quad \text{for all} \quad \sigma \in G.$$

Let $L\colon V \to W$ be *any* linear map, and make

$$\Lambda = \int_G S_\sigma L R_{\sigma^{-1}} d\sigma.$$

Then, using the fact that the Haar integral is left-invariant, we have

$$S_\tau \Lambda R_{\tau^{-1}} = \int_G S_\tau S_\sigma L R_{\sigma - 1} R_{\tau^{-1}} d\sigma = \int_G S_{\tau\sigma} L R_{(\tau\sigma)^{-1}} d\sigma = \int_G S_\sigma L R_{\sigma^{-1}} d\sigma = \Lambda.$$

Therefore,

$$S_\tau \Lambda = \Lambda R_\tau,$$

which shows that Λ is an intertwiner of R and S.

Furthermore, if Σ is any intertwiner of R and S, applying the above process to Σ, we get an intertwiner

$$\int_G S_\sigma \Sigma R_{\sigma^{-1}} d\sigma.$$

Since Σ intertwines R and S,

$$S_\sigma \Sigma = \Sigma R_\sigma,$$

so

$$\int_G S_\sigma \Sigma R_{\sigma^{-1}} d\sigma = \int_G \Sigma R_\sigma R_{\sigma^{-1}} d\sigma = \int_G \Sigma d\sigma = \Sigma.$$

This shows that

1. *Every* intertwiner arises by the integral process defined above.

2. Doing the integral process twice yields the same intertwiner.

Theorem 1.8. *(Schur's Lemma) Say $R\colon G \to \mathbf{GL}(V)$ and $S\colon G \to \mathbf{GL}(W)$ are two irreducible representations of a group G and suppose Λ intertwines R and S. Then, the following facts hold:*

(1) If $R\colon G \to \mathbf{GL}(V)$ is not isomorphic to $S\colon G \to \mathbf{GL}(W)$, then $\Lambda = 0$.

(2) If $R\colon G \to \mathbf{GL}(V)$ and $S\colon G \to \mathbf{GL}(W)$ are isomorphic, then $\Lambda = 0$ or Λ is an isomorphism $\Lambda\colon V \to W$.

(3) If V is complex vector space (more generally a vector space over an algebraically-closed field), and $R\colon G \to \mathbf{GL}(V)$ and $S\colon G \to \mathbf{GL}(V)$ are isomorphic, then $\Lambda = \lambda I$, for some $\lambda \in \mathbb{C}$.

Proof. (1) Let $Z = \operatorname{Ker}\Lambda$ and $Y = \operatorname{Im}\Lambda$. We claim that $(R \mid Z, Z)$ is a subrepresentation of (R, V).

For any $z \in Z$ and any $\sigma \in G$, since

$$\Lambda R_\sigma = S_\sigma \Lambda$$

and $Z = \operatorname{Ker}\Lambda$, we have $\Lambda(z) = 0$, thus $\Lambda R_\sigma(z) = S_\sigma \Lambda(z) = 0$, which implies that $R_\sigma(z) \in \operatorname{Ker}\Lambda = Z$. Therefore, Z is stable under R. A similar argument shows that $(R \mid Y, Y)$ is a subrepresentation of R. Since R is irreducible, either $Z = (0)$ or $Z = V$, and since S is irreducible, either $Y = (0)$ or $Y = W$.

If $\operatorname{Ker}\Lambda = Z = (0)$, then Λ is injective. If $\Lambda \neq 0$, then $Y = \operatorname{Im}\Lambda \neq 0$, which implies that $Y = W$, so Λ is surjective. But then, Λ is an isomorphism, contradicting the assumption that (R, V) and (S, W) are not isomorphic. Therefore, $Z \neq (0)$, which implies that $Z = V$; that is, $\operatorname{Ker}\Lambda = V$, which means that $\Lambda = 0$.

(2) If $\Lambda \neq 0$, then $Z \neq V$, and so $Z = (0)$. Then, Λ is injective, and since $\Lambda \neq 0$ we have $Y \neq (0)$, which implies that $Y = W$. Therefore, if $\Lambda \neq 0$, then it is an isomorphism.

(3) Assume that $\Lambda \neq 0$. As $\mathbb{C}$ is algebraically-closed, Λ has some eigenvalue, λ. Consider $\Sigma = \Lambda - \lambda I$. Because Λ and I are intertwiners, so is Σ. But, $\operatorname{Ker}\Sigma \neq (0)$ (since it is the eigenspace of Λ associated with λ), so Σ is not an isomorphism. By (2), we must have $\Sigma = 0$; that is, $\Lambda = \lambda I$. □

Notation.

We denote by $L^1(G, \mathbb{C})$ the set of functions $f\colon G \to \mathbb{C}$, such that:

1. f is measurable.
2. $\|f\|_1 = \int_G |f(\sigma)| d\sigma$ is finite.

If G is finite, then $L^1(G, \mathbb{C})$ consists of all functions $f\colon G \to \mathbb{C}$.

If G is compact, then all continuous functions belong to $L^1(G, \mathbb{C})$.

If G is locally compact, then the set $\mathcal{C}_o(G, \mathbb{C})$ of continuous functions with compact support is contained in $L^1(G, \mathbb{C})$.

If G is finite, then for every $\sigma \in G$ let b_σ be the function given by

$$b_\sigma(\tau) = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{if } \sigma \neq \tau. \end{cases}$$

Clearly, these functions form a basis of $L^1(G, \mathbb{C})$, which shows that

$$\dim(L^1(G, \mathbb{C})) = \#(G).$$

Let $L^2(G, \mathbb{C})$ be the set of functions $f\colon G \to \mathbb{C}$, such that:

1. f is measurable.
2. $\|f\|_2^2 = \int_G |f(\sigma)|^2 d\sigma$ is finite.

If G is finite, then $L^2(G, \mathbb{C}) = L^1(G, \mathbb{C}) =$ all functions on G.

We have the following Hermitian inner product on $L^2(G, \mathbb{C})$:

$$(f, g) = \int_G f(\sigma)\overline{g(\sigma)} d\sigma,$$

and with this inner product, $L^2(G, \mathbb{C})$ is a Hilbert space. The corresponding norm is

$$\|f\|_2 = \sqrt{(f, f)},$$

and thus, the Cauchy–Schwarz inequality holds:

$$|(f, g)| \leq \|f\|_2 \|g\|_2 .$$

If G is compact and we use the normalized Haar measure, applying Cauchy–Schwarz to f and $g = 1$, we get

$$\left| \int_G f(\sigma) d\sigma \right| = |(f, 1)| \leq \|f\|_2 \|1\|_2 = \|f\|_2 .$$

If $\int_G f(\sigma)d\sigma$ is not real, let $\int_G f(\sigma)d\sigma = e^{i\theta}\rho$ with $\rho \in \mathbb{R}_{>0}$, so that $e^{-i\theta}\int_G f(\sigma)d\sigma$ is real, and since

$$e^{-i\theta}\int_G f(\sigma)d\sigma = \int_G e^{-i\theta}f(\sigma)d\sigma$$

we see that

$$\left\|e^{-i\theta}f\right\|_1 = \|f\|_1,$$

so we conclude that

$$\|f\|_1 \leq \|f\|_2.$$

Therefore, if G is compact, then

$$L^2(G,\mathbb{C}) \subseteq L^1(G,\mathbb{C}).$$

Our next goal is to consider various orthogonality relations. Let $R\colon G \to \mathbf{GL}(V)$ and $S\colon G \to \mathbf{GL}(W)$ be any two nonisomorphic irreducible representations of finite degree, so that we may assume that these are unitary irreps. With respect to unitary bases of V and W, R_σ and S_σ are given by matrices $(r_{a,b}(\sigma))$ and $(s_{a,b}(\sigma))$, and $r_{a,b}$ and $s_{a,b}$ are continuous functions on G.

Remark: Assume we are in Case (3) of Schur's Lemma, and let $\Lambda = \lambda I$ be the intertwiner.

Claim. For any linear map $L\colon V \to W$, if

$$\Lambda = \int_G R_\sigma L R_{\sigma^{-1}} d\sigma,$$

then

$$\mathrm{tr}(\Lambda) = \mathrm{tr}(L)$$

and

$$\lambda = \frac{1}{\deg(R)}\mathrm{tr}(L).$$

Proof. We have

$$\mathrm{tr}(\Lambda) = \int_G \mathrm{tr}(R_\sigma L R_{\sigma^{-1}})d\sigma = \int_G \mathrm{tr}(L)d\sigma = \mathrm{tr}(L).$$

For $L = \lambda I$, we have $\mathrm{tr}(\Lambda) = \mathrm{tr}(L) = \lambda\deg(R)$, and so

$$\lambda = \frac{1}{\deg(R)}\mathrm{tr}(L),$$

as claimed. □

Since (R, V) and (S, W) are not isomorphic, by (1) of Schur's lemma, we must have $\Lambda = 0$ *for all* L; that is,

$$\int_G R_\sigma L R_{\sigma^{-1}} d\sigma = 0, \quad \text{for all} \quad L\colon V \to W.$$

If L is given by the matrix (ξ_{ij}), then

$$R_\sigma L R_{\sigma^{-1}} = \sum_{\beta a} s_{\alpha\beta}(\sigma)\xi_{\beta a} r_{ab}(\sigma^{-1}),$$

and the above equation implies that

$$\sum_{\beta a} \int_G s_{\alpha\beta}(\sigma)\xi_{\beta a} r_{ab}(\sigma^{-1}) d\sigma = 0,$$

and thus,

$$\sum_{\beta a} \left(\int_G s_{\alpha\beta}(\sigma) r_{ab}(\sigma^{-1}) d\sigma \right) \xi_{\beta a} = 0. \tag{$\dagger$}$$

Since ($\dagger$) is a system of linear equations satisfied by all $\xi_{\beta a}$, the matrix of the system must be zero, which means that

$$\int_G s_{\alpha\beta}(\sigma) r_{ab}(\sigma^{-1}) d\sigma = 0, \quad \text{for all} \quad \alpha, \beta, a, b.$$

Since R is unitary, $R_\sigma^{-1} = R_\sigma^*$, so the above is equivalent to

$$\int_G s_{\alpha\beta}(\sigma)\overline{r_{ba}(\sigma)} d\sigma = 0, \quad \text{for all} \quad \alpha, \beta, a, b. \tag{ON_1}$$

In terms of the inner product on $L^2(G, \mathbb{C})$, this means that

$$(s_{\alpha\beta}, r_{ab}) = 0, \quad \text{for all} \quad \alpha, \beta, a, b.$$

We derive more orthogonality relations using part (3) of Schur's Lemma. In this case, R and S are isomorphic, and $\Lambda = \lambda I$, for some $\lambda \in \mathbb{C}$. From

$$\lambda I = \int_G R_\sigma L R_{\sigma^{-1}} d\sigma,$$

we deduce that

$$\lambda \delta_{ij} = \sum_{\rho\alpha} \int_G r_{i\rho}\xi_{\rho\alpha} r_{\alpha j}(\sigma^{-1}) d\sigma.$$

If $i \neq j$, since the $\xi_{\rho\alpha}$ are arbitrary, we must have

$$\int_G r_{i\rho} r_{\alpha j}(\sigma^{-1}) d\sigma = 0, \quad \text{for all} \quad \rho, \alpha.$$

If $i = j$, then

$$\lambda = \sum_{\rho\alpha} \int_G r_{i\rho}\xi_{\rho\alpha} r_{\alpha i}(\sigma^{-1}) d\sigma.$$

But, we showed that

$$\lambda = \frac{1}{\deg(R)}\mathrm{tr}(L) = \frac{1}{\deg(R)} \sum_{\alpha} \xi_{\alpha\alpha} = \frac{1}{\deg(R)} \sum_{\rho,\alpha} \xi_{\rho\alpha}\delta_{\rho\alpha},$$

so we get

$$\frac{1}{\deg(R)} \sum_{\rho,\alpha} \xi_{\rho\alpha}\delta_{\rho\alpha} = \sum_{\rho\alpha} \int_G r_{i\rho}\xi_{\rho\alpha} r_{\alpha i}(\sigma^{-1}) d\sigma.$$

By equating the coefficients of $\xi_{\rho\alpha}$, we get

$$\int_G r_{i\rho} r_{\alpha i}(\sigma^{-1}) d\sigma = \frac{1}{\deg(R)}\delta_{\rho\alpha}.$$

We can put the cases $i \neq j$ and $i = j$ together to obtain

$$\int_G r_{i\rho} r_{\alpha j}(\sigma^{-1}) d\sigma = \frac{1}{\deg(R)}\delta_{ij}\delta_{\rho\alpha}.$$

In the unitary case, we have $r_{\alpha j}(\sigma^{-1}) = \overline{r_{j\alpha}(\sigma)}$, and the above equations become

$$\int_G r_{i\rho}\overline{r_{j\alpha}(\sigma)} d\sigma = \frac{1}{\deg(R)}\delta_{ij}\delta_{\rho\alpha}, \tag{ON$_2$}$$

which can be expressed as

$$(r_{i\rho}, r_{\alpha j}) = \frac{1}{\deg(R)}\delta_{ij}\delta_{\rho\alpha}.$$

Equations (ON$_1$) and (ON$_2$) are the *Peter–Weyl orthogonality relations*.

Equations (ON$_1$) and (ON$_2$) can be used to derive orthogonality relations about the characters. Again, assume that (R, V) and (S, W) are nonisomorphic unitary irreps.

By (ON$_1$), we have

$$\int_G s_{\alpha\beta}(\sigma)\overline{r_{ba}(\sigma)} d\sigma = 0, \quad \text{for all} \quad \alpha, \beta, a, b.$$

If we let $\alpha = \beta$ and $a = b$ and sum with respect to α and a, we get

$$(\chi_S, \chi_R) = 0.$$

If R and S are isomorphic, we use (ON$_2$), with $i = \rho$ and $j = \alpha$. We have

$$\int_G r_{ii}\overline{r_{\alpha\alpha}(\sigma)} d\sigma = \frac{1}{\deg(R)}\delta_{i\alpha}.$$

If we sum over i and α, we get

$$(\chi_R, \chi_S) = \sum_\alpha \sum_i \frac{1}{\deg(R)} \delta_{i\alpha} = \frac{1}{\deg(R)} \sum_\alpha 1 = 1.$$

In summary, we obtained the following result:

Theorem 1.9. *If G is a finite or compact group, then for any two unitary irreducible representations R and S of G,*

$$(\chi_R, \chi_S) = \delta_{RS},$$

where $\delta_{RS} = 1$ iff R and S are isomorphic, otherwise $\delta_{RS} = 0$.

Say (R, V) is any representation of a finite or compact group G, with V finite-dimensional. Then, we know that R is the coproduct of irreducible representations

$$R = \coprod_{S \text{ irred}} n_j S_j, \quad n_j \in \mathbb{N},$$

where n_j is the number of times S appears in R in the decomposition. It follows that

$$\chi_R = \sum_{S \text{ irred}} n_S \chi_S.$$

If T is any given irred of G, then we have

$$\begin{aligned}(\chi_R, \chi_T) &= \sum_S n_S (\chi_S, \chi_T) \\ &= \sum_S n_S \delta_{ST} = n_T.\end{aligned}$$

This gives the following proposition:

Proposition 1.10. *For any representation (R, V) of finite degree of a group G where G is finite or compact, the number of times a given irrep T appears in R is (χ_R, χ_T). Hence, no matter how we decompose R, we always get the same irreps, in the same multiplicity. The canonical decomposition of R is*

$$R = \coprod_{S \text{ any irrep}} (\chi_R, \chi_S) S.$$

Corollary 1.11. *If (R, V) and (S, W) are any finite-degree representations of a finite or compact group G, then $R \cong S$ iff $\chi_R = \chi_S$. In other words, the characters of a representation determine the representation.*

Proof. We have the decompositions

$$R = \coprod_{T \text{ any irrep}} (\chi_R, \chi_T)T \quad \text{and} \quad S = \coprod_{T \text{ any irrep}} (\chi_s, \chi_T)T.$$

If $\chi_R = \chi_S$, then obviously $R \cong S$. Conversely,f if $R \cong S$, then $\chi_R = \chi_S$, because $R_\sigma = L^{-1}S_\sigma L$ (where L is the intertwining isomorphism), so the traces are the same. □

Corollary 1.12. *If (R, V) is finite-degree representation of a finite or compact group G and if T is any irrep of G, then (χ_R, χ_T) is a nonnegative integer.*

Corollary 1.13. *Given any finite-degree representation (R, V) of a finite or compact group G, the number (χ_R, χ_R) is a positive integer, and $(\chi_R, \chi_R) = 1$ iff R is irreducible.*

Proof. If we write

$$R = \coprod_{T \text{ irred}} (\chi_R, \chi_T)T,$$

then

$$\chi_R = \sum_T (\chi_R, \chi_T)\chi_T.$$

Consequently,

$$\begin{aligned}(\chi_R, \chi_R) &= \sum_{T,S} (\chi_R, \chi_T)\overline{(\chi_R, \chi_S)}(\chi_T, \chi_S) \\ &= \sum_{T,S} (\chi_R, \chi_T)\overline{(\chi_R, \chi_S)}\delta_{ST} \\ &= \sum_T |(\chi_R, \chi_T)|^2,\end{aligned}$$

which is a positive integer.

If $(\chi_R, \chi_R) = 1$, then $R = T$ for some irrep T, because R itself is an irrep. Conversely, if R is an irrep, Theorem 1.9 implies immediately that $(\chi_R, \chi_R) = 1$. □

We now define an important representation of a group G.

Any group G acts on itself by "translation," where the action is given by

$$\sigma \cdot \tau = \sigma\tau.$$

(1) Assume G is finite. Pick any vector e_τ for every $\tau \in G$, and consider the vector space V freely generated by the e_τ, so that they form a basis of V ($\dim(V) = \#(G)$). We define the representation Reg of G on V by

$$\text{Reg}_\sigma(e_\tau) = e_{\sigma\tau}.$$

This representation is called the *regular representation* of G.

(2) Now assume G is infinite. In this case, we wish to define a "regular representation" of G on $L^1(G, d\sigma)$ or $L^2(G, d\sigma)$. When G is finite, we have the functions b_σ given by

$$b_\sigma(\tau) = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{if } \sigma \neq \tau \end{cases}$$

which form a basis of $L^1(G) = L^2(G)$, and

$$\mathrm{Reg}_\sigma(b_\tau) = b_{\sigma\tau}$$

defines Reg.

How do we generalize this to infinite groups?

We want to view $\mathrm{Reg}_\sigma(b_\tau)$ as a function, so we need to define $\mathrm{Reg}_\sigma(b_\tau)(\theta)$, for any $\theta \in G$, in such a way that

$$\mathrm{Reg}_\sigma(b_\tau)(\theta) = b_{\sigma\tau}(\theta) = \delta_{\sigma\tau,\theta}.$$

However, $\sigma\tau = \theta$ iff $\tau = \sigma^{-1}\theta$, in which case

$$\mathrm{Reg}_\sigma(b_\tau)(\theta) = \delta_{\tau,\sigma^{-1}\theta} = b_\tau(\sigma^{-1}\theta).$$

This suggests that the proper way to define the regular representation on $L^1(G)$ or $L^2(G)$ is to set

$$\mathrm{Reg}_\sigma(f)(\theta) = f(\sigma^{-1}\tau), \quad \theta \in G,\ f \in L^1(G) \text{ (or } f \in L^2(G)).$$

Let us go back to the case where G is a finite group, and let us compute the matrix of Reg_σ in the basis (e_τ). The τth column of Reg_σ is $\mathrm{Reg}_\sigma(e_\tau) = e_{\sigma\tau}$, so this is a permutation matrix.

What is the entry of index (τ, τ)?

If $\sigma = 1$, the answer is 1 (since $\mathrm{Reg}_1 = I$). If $\sigma \neq 1$, then the answer is 0 for all τ. It follows that $\mathrm{tr}(\mathrm{Reg}_1) = \#(G)$ and $\mathrm{tr}(\mathrm{Reg}_\sigma) = 0$ for all $\sigma \neq 1$.

Proposition 1.14. *For any finite group G, the character χ_{Reg} of the regular representation is given by*

$$\chi_{\mathrm{Reg}}(1) = \#(G)$$
$$\chi_{\mathrm{Reg}}(\sigma) = 0, \quad \sigma \neq 1.$$

Let

$$\mathrm{Reg} = \coprod_{S \text{ irrep}} (\chi_{\mathrm{Reg}}, \chi_S) S$$

be the canonical decomposition of Reg, and compute its character

$$\chi_{\mathrm{Reg}} = \sum_{S \text{ irrep}} (\chi_{\mathrm{Reg}}, \chi_S) \chi_S.$$

However, we know χ_{Reg}, so if we write $g = \#(G)$, we get

$$(\chi_{\mathrm{Reg}}, \chi_S) = \int_G \chi_{\mathrm{Reg}} \overline{\chi_S(\sigma)} d\sigma = \frac{1}{g} \chi_{\mathrm{Reg}}(1) \overline{\chi_S(1)} = \frac{g}{g} \overline{\chi_S(1)} = \deg(S).$$

Therefore,

$$\mathrm{Reg} = \coprod_{S \text{ irrep}} \deg(S) S$$

and

$$g = \#(G) = \sum_{S \text{ irrep}} \deg(S) \chi_S(1) = \sum_{S \text{ irrep}} (\deg(S))^2.$$

In summary, we proved the following result:

Theorem 1.15. *Every irreducible representation of a finite group appears in* Reg *exactly as many times as its degree. That is, the canonical decomposition of* Reg *is*

$$\mathrm{Reg} = \coprod_{S \text{ irrep}} \deg(S) S.$$

Moreover,

$$g = \#(G) = \sum_{S \text{ irrep}} (\deg(S))^2.$$

Construction

Say (R, V) is a representation of a compact group G (not necessarily finite). Write $L^2_{\mathrm{cl}}(G)$ (resp. $L^1_{\mathrm{cl}}(G)$) for the subspace of class functions in $L^2(G)$ (resp. $L^1(G)$); that is

$$\begin{aligned} L^2_{\mathrm{cl}}(G) &= \{f \in L^2(G) \mid f(\sigma^{-1}\tau\sigma) = f(\tau), \quad \text{for all} \quad \sigma, \tau \in G\} \\ &= \{f \in L^2(G) \mid f(\sigma\tau) = f(\tau\sigma), \quad \text{for all} \quad \sigma, \tau \in G\}. \end{aligned}$$

The space $L^1_{\mathrm{cl}}(G)$ is defined analogously (*mutatis mutandis*).

For any function $f \in L^2_{\mathrm{cl}}(G)$ (or in $L^1_{\mathrm{cl}}(G)$), define $R[f]$, called the *f weighted automorphism of V*, by

$$R[f] = \int_G f(\sigma) R_\sigma d\sigma.$$

Proposition 1.16. *For any class function f, the f weighted automorphism of V is a self-intertwining operator; that is,*

$$R_\tau R[f] = R[f]R_\tau, \quad \textit{for all} \quad \tau \in G.$$

If R is irreducible and V is a complex vector space, then

$$R[f] = \lambda I,$$

with

$$\lambda = \frac{1}{\deg(R)}(f, \overline{\chi_R}).$$

Proof. We have

$$R_\tau^{-1} R[f] R_\tau = R_{\tau^{-1}} R[f] R_\tau = \int_G R_{\tau^{-1}} f(\sigma) R_\sigma R_\tau d\sigma = \int_G f(\sigma) R_{\tau^{-1}\sigma\tau} d\sigma.$$

Because the Haar integral on a compact group is left and right invariant, we have

$$\int_G f(\sigma) R_{\tau^{-1}\sigma\tau} d\sigma = \int_G f(\tau\sigma) R_{\sigma\tau} d\sigma = \int_G f(\tau\sigma\tau^{-1}) R_\sigma d\sigma,$$

and since f is a class function, we have

$$\int_G f(\tau\sigma\tau^{-1}) R_\sigma d\sigma = \int_G f(\sigma) R_\sigma d\sigma = R[f],$$

which proves that

$$R_\tau^{-1} R[f] R_\tau = R[f].$$

If R is an irrep and V is complex, then by Schur's Lemma part (3), we must have

$$R[f] = \lambda I.$$

If we apply the trace operator on both sides, we get

$$\mathrm{tr}(R[f]) = \lambda \deg(R).$$

On the other hand,

$$\begin{aligned} \mathrm{tr}(R[f]) &= \int_G f(\sigma) \mathrm{tr}(R_\sigma) d\sigma \\ &= \int_G f(\sigma) \chi_R(\sigma) d\sigma \\ &= \int_G f(\sigma) \overline{\overline{\chi_R(\sigma)}} d\sigma \\ &= (f, \overline{\chi_R}). \end{aligned}$$

Therefore,

$$\lambda = \frac{1}{\deg(R)}(f, \overline{\chi_R}),$$

as claimed. □

We now come to an important theorem proved by Frobenius and Schur for finite groups, and by Peter and Weyl for compact groups.

Theorem 1.17. *(Frobenius, Schur, Peter–Weyl) Let G be a finite or a compact group. The characters χ_R of irreducible representations of G form an orthonormal basis for $L^2_{\mathrm{cl}}(G)$ (a Hilbert basis of $L^2_{\mathrm{cl}}(G)$). This means that for any $f \in L^2_{\mathrm{cl}}(G)$, we can write*

$$f = \sum_{R \,\mathrm{irrep}} c_R \, \chi_R$$

(the Fourier series for f), with the R-Fourier coefficient given by

$$c_R = (f, \chi_R).$$

Proof. Since the characters χ_R associated with irreps form an orthonormal set in $L^2_{\mathrm{cl}}(G)$ (by the orthogonality relations), all we have to show is that they span $L^2_{\mathrm{cl}}(G)$ (in the sense of Hilbert spaces); that is, we need to show that for any $f \in L^2_{\mathrm{cl}}(G)$, if $(f, \chi_R) = 0$ for all χ_R, then $f = 0$.

Pick any $f \in L^2_{\mathrm{cl}}(G)$ such that $(f, \chi_R) = 0$ for all χ_R and consider $\overline{f}$. Take any finite dimensional representation S and form $S[\overline{f}]$. We know from Proposition 1.16 that $S[\overline{f}]$ intertwines S and itself. If S is an irrep, then by Schur's Lemma,

$$S[\overline{f}] = \lambda I,$$

and

$$\lambda = \frac{1}{\deg(S)} (\overline{f}, \overline{\chi_R}).$$

Remark: Here, we use the fact that if G is compact, then every irrep is finite-dimensional. This is left as a homework problem.

It follows that

$$\lambda = \frac{1}{\deg(S)} \overline{(f, \chi_R)} = 0,$$

by hypothesis. Therefore,

$$S[\overline{f}] = 0$$

for all irrep S. However, any finite dimensional representation is a coproduct of irreps, and this implies that

$$S[\overline{f}] = 0$$

for all finite-dimensional representations. In particular, this applies to the regular representation, so we have

$$\mathrm{Reg}[\overline{f}] = 0.$$

Remark: The regular representation is generally not finite-dimensional, but the argument can be justified for a compact group.

Recall that if $g \in L^2_{\mathrm{cl}}(G)$, then

$$\mathrm{Reg}_\tau(g)(\sigma) = g(\tau^{-1}\sigma),$$

so that

$$\begin{aligned}(\mathrm{Reg}[\overline{f}](g))(\sigma) &= \int_G \overline{f}(u)\mathrm{Reg}_u(g)(\sigma)du \\ &= \int_G \overline{f}(u)g(u^{-1}\sigma)du. \qquad (\dagger)\end{aligned}$$

Case where G is finite.

Then, we can use the basis functions b_σ. We know that

$$\mathrm{Reg}_\tau(b_\sigma) = b_{\tau\sigma}.$$

Let $g = b_1$ in (†). We get

$$\begin{aligned}\mathrm{Reg}[\overline{f}](b_1) &= \int_G \overline{f}(u)\mathrm{Reg}_u(b_1)du \\ &= \int_G \overline{f}(u)b_u du \\ &= \frac{1}{\#(G)}\sum_{u\in G}\overline{f}(u)b_u.\end{aligned}$$

But, $\mathrm{Reg}[(\overline{f}] = 0$, which implies that

$$\sum_{u\in G}\overline{f}(u)b_u = 0,$$

and since the b_u form a basis, we conclude that $\overline{f}(u) = 0$ for all u, and therefore, $f = 0$.

If G is an infinite group, how do we choose g to mimic b_1?

An Aside: $G = \mathbb{R}^+$.

In this case, Dirac comes to the rescue! To proceed rigorously, we use an idea due to Friedricks. We define some functions g_α, where g_α is a "hat function" defined on the interval $[-\alpha, \alpha]$ with $\alpha > 0$, where the value $h_\alpha = g_\alpha(0)$ is chosen so that the area under the graph of g_α is equal to 1. Then, we have the convolution

$$(f * g_\alpha)(0) = \int_\infty^\infty f(x)g_\alpha(-x)dx = \int_{-\alpha}^{\alpha} f(x)g_\alpha(-x)dx,$$

and we take the limit when $\alpha \downarrow 0$, so that

$$\lim_{\alpha \downarrow 0}(f * g_\alpha)(0) = f(0).$$

The set $\{g_\alpha\}$ is called an *approximate identity*, and when the functions are C^∞, the g_αs are *Friedricks mollifiers*.

Case where G is compact.

Going back to a compact group G, take a neighborhood U_α of 1 and a set of functions g_α that form an approximate identity at 1. Go back to (†), and let $v = u^{-1}\sigma$. Using the translation invariance of the Haar measure, (†) says that

$$\mathrm{Reg}[\overline{f}](g_\alpha)(\sigma) = \int_G \overline{f}(\sigma v^{-1}) g_\alpha(v) dv.$$

If we take the limit as $\alpha \downarrow 0$, we get the value at $v = 1$. The right-hand side yields $\overline{f}(\sigma)$, but the left-hand side is 0, since $\mathrm{Reg}[\overline{f}] = 0$. It follows that $\overline{f}(\sigma) = 0$ for all σ, and thus $f = 0$, which concludes the proof. □

Corollary 1.18. *The number of irreducible representations of a finite group G is exactly the number of distinct conjugacy classes* $\mathrm{conj}(G)$ *in G.*

Proof. Recall that for any $\sigma \in G$,

$$\mathrm{conj}(\sigma) = \{\rho\sigma\rho^{-1} \mid \rho \in G\}.$$

Define the function f_σ such that

$$f_\sigma(\tau) = \begin{cases} 1 & \text{if } \tau \in \mathrm{conj}(\sigma) \\ 0 & \text{if } \tau \notin \mathrm{conj}(\sigma). \end{cases}$$

These functions form a basis of $L^2_{\mathrm{cl}}(G)$ and there are $\mathrm{conj}(G)$ of these, so $\dim(L^2_{\mathrm{cl}}(G)) = \mathrm{conj}(G)$. By Theorem 1.17, the dimension of $L^2_{\mathrm{cl}}(G)$ is equal to the number of irreducible representations of G, which proves the corollary. □

Corollary 1.19. *(Peter–Weyl) If G is a compact group, then taking all the matrix entries in $R_\sigma = (r_{ij}(\sigma))$ as R ranges over all the uniirreps of G as functions on G (they are continuous), we find that these r_{ij} form a Hilbert basis of $L^2(G)$.*

Proof. Reprove Theorem 1.17 with $R[\overline{f}]$, but don't take traces, and use (ON_1) and (ON_2). The details are left as an exercise. □

Given any group, recall that $[G, G]$ is the subgroup of G generated by the commutators,

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}, \quad \sigma, \tau \in G.$$

Observe that

$$\begin{aligned}\rho^{-1}[\sigma,\tau]\rho &= \rho^{-1}\sigma\tau\sigma^{-1}\tau^{-1}\rho \\ &= \rho^{-1}\sigma\rho\,\rho^{-1}\tau\rho\,\rho^{-1}\sigma^{-1}\rho\,\rho^{-1}\tau^{-1}\rho \\ &= [\rho^{-1}\sigma\rho, \rho^{-1}\tau\rho],\end{aligned}$$

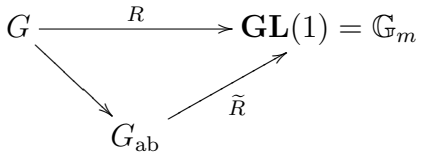
which proves that $[G,G]$ is a normal subgroup of G called the *commutator subgroup* of G. The group $[G,G]$ is characterized by the property that for any normal subgroup N of G, the quotient G/N is abelian iff $[G,G] \subseteq N$. The group

$$G_{\text{ab}} = G/[G,G]$$

is the *abelianization of* G (or G *made abelian*).

Theorem 1.20. *Say G is a group. If R is an irrep of degree 1, then*

(1) R corresponds to an irrep $\widetilde{R}$ (of degree 1) of G_{ab}, and the correspondence is one-to-one. Here, $\widetilde{R}$ is the unique homomorphism which makes the following diagam commutes:



(2) If G is abelian, then all its irreps have degree 1.

(3) Lastly, if G is finite (or compact) and all the irreps of G have degree 1 then G is abelian.

Proof. (1) This follows immediately from the first isomorphism theorem.

(2) Let (R,V) be any irrep of G and pick any $\sigma \in G$. For all $\tau \in G$,

$$R_\sigma R_\tau = R_{\sigma\tau} = R_{\tau\sigma} = R_\tau R_\sigma,$$

which means that R_σ intertwines R. By Schur's Lemma, $R_\sigma = \lambda_\sigma I$. So for every $v \in V$,

$$R_\sigma v = \lambda_\sigma v,$$

and this shows that the span of v is a subrepresentation of R. Since R is irreducible and nontrivial, we must have $\text{Span}(v) = V$, which shows that V is one-dimensional.

(3) If G is finite and if all its irreps have degree 1, then

$$g = \#(G) = \sum_{R\,\text{irrep}} (\deg(R))^2 = \sum_{R\,\text{irrep}} 1 = \text{conj}(G),$$

which shows that G is abelian. □

Proposition 1.21. *If G is any group and H is an abelian subgroup of G, then for any irrep (R, V) of G, we have*

$$\deg(R) \leq (G : H).$$

(Here, $(G : H)$ is the index of H in G; that is, $(G : H)$ is the number of cosets gH, with $g \in G$.)

Proof. Say (R, V) is an irrep of G and consider the restriction S of R to H. Then, S is a representation of H, and since H is abelian, its irreps have degree 1. Pick any irred of S, and say it is spanned by $v \in V$ $(v \neq 0)$.

If $\sigma \in H$, then

$$\sigma v = R_\sigma(v) = \lambda(v)v, \quad \text{for some} \quad \lambda(v) \in \mathbb{C}.$$

We may assume $(G : H) = t$ is finite, let $\rho_1 = 1, \rho_2, \ldots, \rho_t$ be some coset representatives for H and G, and set

$$v_j = \rho_j v, \quad 1 \leq j \leq t$$

and

$$W = \text{span}(v_1, v_2, \ldots, v_t).$$

Next, suppose $\tau \notin H$. Then, we have

$$\tau = \rho_j \sigma, \quad \text{for some} \quad \sigma \in H, \quad 1 \leq j \leq t$$

and

$$\begin{aligned} \tau v_l &= \rho_j \sigma v_l \\ &= \rho_j \sigma \rho_l v. \end{aligned}$$

But,

$$\sigma \rho_j = \rho_k \widetilde{\sigma}, \quad \text{for some} \quad \widetilde{\sigma} \in H,$$

so we get

$$\begin{aligned} \tau v_l &= \rho_j \sigma \rho_l v \\ &= \rho_j \rho_k \widetilde{\sigma} v \\ &= \rho_j \rho_k \lambda(\widetilde{\sigma}) v \\ &= \lambda(\widetilde{\sigma}) \rho_j \rho_k v, \end{aligned}$$

and since

$$\rho_j \rho_k = \rho_m \gamma, \quad \text{for some} \quad \gamma \in H, \quad 1 \leq m \leq t,$$

we get

$$\begin{aligned} \tau v_l &= \lambda(\widetilde{\sigma}) \rho_j \rho_k v \\ &= \lambda(\widetilde{\sigma}) \rho_m \gamma v \\ &= \lambda(\widetilde{\sigma}) \rho_m \lambda(\gamma) v \\ &= \lambda(\widetilde{\sigma}) \lambda(\gamma) \rho_m v \\ &= \lambda(\widetilde{\sigma}) \lambda(\gamma) v_m, \end{aligned}$$

which shows that $\tau v_l \in W$. Therefore, W is stable under R, and since R is irreducible, we must have $W = V$. As a consequence,

$$\deg(R) = \dim(V) = \dim(W) \leq t = (G : H),$$

as claimed. □

Proposition 1.22. *If G is a finite group and χ_R runs through all irreducible characters of G, then for all $\sigma, \tau \in G$, we have*

$$\sum_{R \text{ irred}} \overline{\chi_R(\sigma)}\chi_R(\tau) = \frac{g}{\#\mathrm{cl}(\sigma)}\,\delta_{\mathrm{cl}(\sigma),\mathrm{cl}(\tau)},$$

where $\mathrm{cl}(\sigma)$ denotes the conjugacy class of σ and $g = \#(G)$.

Proof. Let $f\colon G \to \mathbb{C}$ be the function defined by

$$f(\tau) = \begin{cases} 1 & \text{if } \tau \in \mathrm{cl}(\sigma) \\ 0 & \text{if } \tau \notin \mathrm{cl}(\sigma). \end{cases}$$

Clearly, f is a class function, and thus it is given by the Fourier series

$$f = \sum_{R \text{ irred}} (f, \chi_R)\chi_R,$$

with

$$(f, \chi_R) = \int_G f(\theta)\overline{\chi_R(\theta)}d\theta = \frac{1}{g}\sum_{\theta \in \mathrm{cl}(\sigma)} 1 \cdot \overline{\chi_R(\theta)} = \frac{\#\mathrm{cl}(\sigma)}{g}\,\overline{\chi_R(\sigma)},$$

and so

$$f(\tau) = \sum_{R \text{ irred}} \frac{\#\mathrm{cl}(\sigma)}{g}\,\overline{\chi_R(\sigma)}\chi_R(\tau).$$

However, the left-hand side is equal to $\delta_{\mathrm{cl}(\sigma),\mathrm{cl}(\tau)}$, so we conclude that

$$\frac{g}{\#\mathrm{cl}(\sigma)}\,\delta_{\mathrm{cl}(\sigma),\mathrm{cl}(\tau)} = \sum_{R \text{ irred}} \overline{\chi_R(\sigma)}\chi_R(\tau),$$

as claimed. □

1.4 Some (Easy) Examples & Some Techniques

(I) The symmetric group $\mathfrak{S}_3$ of order three = the symmetry group of an equilateral triangle.

The group $\mathfrak{S}_3$ is generated by 2 elements σ, τ, such that

$$\sigma^3 = \tau^2 = 1, \quad \tau\sigma = \sigma^2\tau, \quad \sigma\tau = \tau\sigma^2.$$

The group G has order $6 = 3!$, so by the first Sylow Theorem, there exist subgroups of order 2 and 3. The second Sylow Theorem says that

(a) The number of p-Sylow subgroups is $\equiv 1 \pmod{p}$.

(b) The number of p-Sylow subgroups divides $\#(G)$.

(c) Any two p-Sylow subgroups are conjugate in G.

(d) If $\sigma \in G$ has order p^k, then σ belongs to some p-Sylow subgroup.

In G, there is a subgroup of order 3.

(i) It is $\mathbb{Z}/3\mathbb{Z}$, abelian, and $(G : \mathbb{Z}/3\mathbb{Z}) = 2$; each irrep has degree at most 2.

(ii) The number of $\mathbb{Z}/3\mathbb{Z}$ subgroups in G is $\equiv 1 \pmod{3}$; this number divides 6, and by the above, it divides 2.

By (c) and counting, there exists only one subgroup $\mathbb{Z}/3\mathbb{Z}$, and by (c) again, $\mathbb{Z}/3\mathbb{Z}$ is normal in G. Then, we have an isomophism

$$G/(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z},$$

with $\mathbb{Z}/2\mathbb{Z}$ abelian. Therefore, $[G, G] = \mathbb{Z}/3\mathbb{Z}$, and since G is nonabelian,

$$G_{\text{ab}} = \mathbb{Z}/2\mathbb{Z}.$$

Therefore, the number of irreps of degree 1 of G is the number of irreps of G_{ab}. There are two of them:

The first irrep R_1 is the trivial one and has the constant character $\chi_1 = 1$ on G;

The second irrep R_2 has the character χ_2 determined by $\chi_2(\sigma) = 1$, and $\chi_2(\tau) = -1$.

What is the number of irreps of G?

We must have

$$6 = \#(G) = 1 + 1 + \text{sum of squares bigger than 1.}$$

Therefore, there is only one more irrep R_3 of degree 3 (recall that the degree of an irrep divides $\#(G)$).

Let's compute the conjugacy classes of G. Since $\text{cl}(1) = \{1\}$ and $\text{cl}(\sigma) = \{\sigma, \sigma^2\}$, there is only one more conjugacy class (since the number of irreps is equal to the number of conjugacy classes). This must be $\text{cl}(\tau) = \{\tau, \sigma^2\tau, \sigma\tau\}$.

Let G act on itself by conjugation; that is, by

$$\sigma \cdot \rho = \sigma\rho\sigma^{-1}, \quad \sigma, \rho \in G.$$

Consider the action of G on $\text{cl}(\tau)$. The action of τ on τ is

$$\tau \cdot \tau = \tau\tau\tau = \tau;$$

The action of τ on $\sigma^2\tau$ is

$$\tau \cdot \sigma^2\tau = \tau\sigma^2\tau\tau = \sigma\tau;$$

The action of τ on $\sigma\tau$ is

$$\tau \cdot \sigma\tau = \tau\sigma\tau\tau = \sigma^2\tau.$$

The action of σ on $\sigma\tau$ is

$$\sigma \cdot \tau = \sigma\tau\sigma^{-1} = \sigma\tau\sigma^2 = \sigma^2\tau.$$

The action of σ on $\sigma^2\tau$ is

$$\sigma \cdot \sigma^2\tau = \sigma^3\tau\sigma^{-1} = \tau\sigma^2 = \sigma\tau;$$

The action of σ on $\sigma\tau$ is

$$\sigma \cdot \sigma\tau = \sigma^2\tau\sigma^{-1} = \tau\sigma\sigma^2 = \tau.$$

It follows that the map $\mathrm{inn}\colon G \to \mathrm{Aut}(G)$ given by

$$\sigma \mapsto \text{action by } \sigma$$

is a homomorphism. The kernel of this homomorphism is $Z(G)$ (the center of G). But in our case, $Z(G) = (1)$, so the image of inn is the group $I(G)$ of all *inner automorphisms* of G. This is a normal subgroup of G, and $\mathrm{Aut}(G)/I(G) = \mathrm{Out}(G)$, is the group of *outer automorphisms* of G.

In summary, our third representation R has the property that the action of R_σ on $\mathrm{cl}(\tau)$ is given by

$$\begin{aligned} R_\sigma(\tau) &= \sigma^2\tau \\ R_\sigma(\sigma^2\tau) &= \sigma\tau \\ R_\sigma(\sigma\tau) &= \tau, \end{aligned}$$

and then the action of R_{σ^2} is the same as $R_\sigma R_\sigma$, and the actions of $R_{\sigma\tau}$ is the same as $R_\sigma R_\tau$.

Make a 3-dimensional complex vector space with basis $e_\tau, e_{\sigma^2\tau}, e_{\sigma\tau}$, with action

$$\begin{aligned} R_\sigma(e_\tau) &= e_{\sigma^2\tau} \\ R_\sigma(e_{\sigma^2\tau}) &= e_{\sigma\tau} \\ R_\sigma(e_{\sigma\tau}) &= e_\tau. \end{aligned}$$

The action of R_τ is given by

$$\begin{aligned} R_\tau(e_\tau) &= e_{\tau^3} = e_\tau \\ R_\tau(e_{\sigma^2\tau}) &= e_{\tau\sigma^2\tau\tau} = e_{\sigma\tau} \\ R_\tau(e_{\sigma\tau}) &= e_{\tau\sigma\tau\tau} = e_{\tau\sigma} = e_{\sigma^2\tau}. \end{aligned}$$

Let

$$v = e_\tau + e_{\sigma^2\tau} + e_{\sigma\tau}.$$

Observe that v is fixed by R_σ and R_τ. Using coordinates, we have

$$\begin{aligned} e_\tau &= (1,0,0) \\ e_{\sigma^2\tau} &= (0,1,0) \\ e_{\sigma\tau} &= (0,0,1), \end{aligned}$$

and

$$v = e_\tau + e_{\sigma^2\tau} + e_{\sigma\tau} = (1,1,1).$$

The orthogonal complement of v is the plane of equation

$$x + y + z = 0,$$

and the restriction of R to this plane is a 2-dimensional representation. Let us find a basis of this plane. First, we look for

$$w_1 = v - \alpha e_\tau$$

such that w_1 is orthogonal to v. We want $(v, w_1) = 0$, that is

$$(v,v) - \alpha(e_\tau, v) = 3 - \alpha = 0,$$

which yields $\alpha = 3$. Similarly, we look for

$$w_2 = v - \beta e_{\sigma^2\tau}$$

such that w_2 is orthogonal to v, and we find that $\beta = 3$. Thus, we have the following basis for the plane $x + y + z = 0$:

$$\begin{aligned} w_1 &= v - 3e_\tau \\ w_2 &= v - 3e_{\sigma^2\tau}. \end{aligned}$$

Let us find the action of R_σ on this basis. We have

$$R_\sigma(w_1) = \sigma \cdot v - 3\sigma \cdot e_\tau = v - 3e_{\sigma^2\tau} = w_2,$$

and

$$R_\sigma(w_2) = \sigma \cdot v - 3\sigma \cdot e_{\sigma^2\tau} = v - 3e_{\sigma\tau}.$$

Since

$$v = e_\tau + e_{\sigma^2\tau} + e_{\sigma\tau},$$

we have

$$e_{\sigma\tau} = v - e_\tau - e_{\sigma^2\tau},$$

which yields

$$\begin{aligned} R_\sigma(w_2) &= v - 3e_{\sigma\tau} \\ &= v - 3(v - e_\tau - e_{\sigma^2\tau}) \\ &= -2v + 3e_\tau + 3e_{\sigma^2\tau} \\ &= -(v - 3e_\tau) - (v - 3e_{\sigma^2\tau}) \\ &= -w_1 - w_2. \end{aligned}$$

Using the above, we see that the matrix of R_σ over the basis (w_1, w_2) is

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

and thus, $\chi_R(\sigma) = -1$.

For the action of R_τ, we have

$$R_\tau(w_1) = \tau \cdot v - 3\tau \cdot e_\tau = v - 3e_\tau = w_1,$$

and

$$\begin{aligned} R_\tau(w_2) &= \tau \cdot v - 3\tau \cdot e_{\sigma^2\tau} \\ &= v - 3e_{\sigma\tau} \\ &= v - 3(v - e_\tau - e_{\sigma^2\tau}) \\ &= -2v + 3e_\tau + 3e_{\sigma^2\tau} \\ &= -(v - 3e_\tau) - (v - 3e_{\sigma^2\tau}) \\ &= -w_1 - w_2. \end{aligned}$$

The matrix of R_τ is

$$\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix},$$

and thus, $\chi_R(\tau) = 0$. Finally, we obtain the following character table for the irreducible characters of $G = \mathfrak{S}_3$:

	cl(1)	cl(τ)	cl(σ)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

The columns and the rows of a character table are not independent. Here are three "tricks" to fill an incomplete character table.

Method 1. Use column orthogonality:

$$\sum_R \overline{\chi_R(\sigma)}\chi_R(\tau) = \frac{g}{\#\mathrm{cl}(\sigma)}\,\delta_{\mathrm{cl}(\sigma),\mathrm{cl}(\tau)}.$$

This means that the inner product of any two distinct columns in the character table are orthogonal. For example, if we have the incomplete character table

	cl(1)	cl(τ)	cl(σ)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	x	y

,

orthogonality of the first two columns yields

$$2x = 0$$

and orthogonality of the first and the third column yields

$$2y + 2 = 0.$$

Therefore, $x = 0$ and $y = 1$, as we already know.

Method 2. Use the regular representation. Namely, from

$$\mathrm{Reg} = \coprod_R \deg(R)R,$$

we have

$$\chi_{\mathrm{Reg}} = \sum_R \deg(R)\chi_R.$$

In our example, $\chi_{\mathrm{Reg}}(\sigma) = \chi_{\mathrm{Reg}}(\tau) = 0$, so we get

$$\chi_1\begin{pmatrix}\sigma\\ \tau\end{pmatrix} + \chi_2\begin{pmatrix}\sigma\\ \tau\end{pmatrix} + 2\chi_3\begin{pmatrix}\sigma\\ \tau\end{pmatrix} = 0,$$

that is

$$\begin{pmatrix}1\\ 1\end{pmatrix} + \begin{pmatrix}1\\ -1\end{pmatrix} + 2\begin{pmatrix}y\\ x\end{pmatrix} = 0,$$

and again, we get $x = 0$ and $y = -1$.

Method 3. Use character orthogonality; that is,

$$\begin{aligned}(\chi_R, \chi_S) = \delta_{R,S} &= \frac{1}{g}\sum_{\sigma\in G} \chi_R(\sigma)\overline{\chi_S(\sigma)} \\ &= \sum_{\text{conj. classes}} \frac{\#\mathrm{cl}(\sigma)}{g}\,\chi_R(\sigma)\overline{\chi_S(\sigma)}.\end{aligned}$$

This means that we use the orthogonality of the rows of the character table with weighting factors. For our example, the incomplete table is:

	1/6	1/2	1/3
	cl(1)	cl(τ)	cl(σ)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	x	y

The weighted inner product of row 1 and row 3 is

$$\frac{1}{6}\times 2 + \frac{1}{2}x + \frac{1}{3}y = 0,$$

and the weighted inner product of row 2 and row 3 is

$$\frac{1}{6} \times 2 - \frac{1}{2}x + \frac{1}{3}y = 0.$$

Again, the solution is $x = 0$, $y = -1$.

II. The group G of symmetries of the regular pentagon ($g = \#G = 10$), see Figure 1.3.

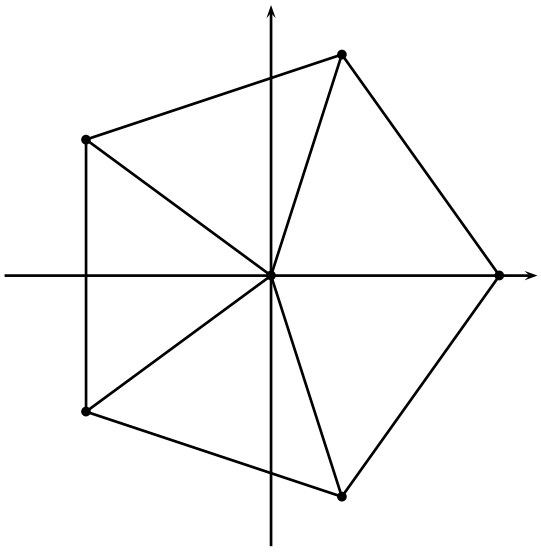


Figure 1.3: Symmetries of a Pentagon

This group is generated by the rotation σ by $2\pi/5$ around the origin, and the reflection τ about the x-axis. These generators satisfy the relations

$$\sigma^5 = \tau^2 = 1, \quad \tau\sigma = \sigma^4\tau,$$

which characterize the group (as a quotient of the free group on two generators).

Actually, we claim that any nonabelian group G of order 10 is isomorphic to the group of the pentagon.

By the first Sylow theorem, a nonabelian group of order 10 has a subgroup of order 5. By the second Sylow theorem, there exist 1 or 6 such subgroups, but counting implies that there is only one. Therefore this subgroup is normal, and we have the exact sequence

$$0 \longrightarrow \mathbb{Z}/5\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \qquad (*)$$

Pick a generator θ in $\mathbb{Z}/2\mathbb{Z}$ and lift it to τ in G. The element τ must have order 2 because otherwise it would generate G, but G is not cyclic. We can define an action of τ on $\mathbb{Z}/5\mathbb{Z}$ as follows:

$$\tau \cdot \sigma^k = \tau\sigma^k\tau^{-1} = \tau\sigma^k\tau,$$

where σ is a generator of $\mathbb{Z}/5\mathbb{Z}$. If $\widetilde{\tau}$ is another lift of θ in G, then $\widetilde{\tau} = \tau h$ for some $h \in \mathbb{Z}/5\mathbb{Z}$, and as $\mathbb{Z}/5\mathbb{Z}$ is abelian, for any $\alpha \in \mathbb{Z}/5\mathbb{Z}$, we have

$$\widetilde{\tau}\alpha(\widetilde{\tau})^{-1} = \tau h \alpha h^{-1}\tau^{-1} = \tau\alpha\tau^{-1},$$

which shows that this action only depends on θ. It follows that the exact sequence $(*)$ defines an action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/5\mathbb{Z}$, *via*

$$\theta \cdot \alpha = \tau\alpha\tau^{-1}, \quad \alpha \in \mathbb{Z}/5\mathbb{Z},$$

and where τ is any lift of $\theta \in \mathbb{Z}/2\mathbb{Z}$. For any generator σ in $\mathbb{Z}/5\mathbb{Z}$, there are four possibilities for $\theta \cdot \sigma = \tau\sigma\tau^{-1}$:

$$\sigma,\ \sigma^2,\ \sigma^3,\ \sigma^4.$$

Our action is an automorphism $\neq$ id on $\mathbb{Z}/5\mathbb{Z}$, and it has order 2 (since τ has order 2).

If $\tau\sigma\tau^{-1} = \sigma$, then $\tau\sigma = \sigma\tau$, but then G would be abelian, a contradiction.

If $\tau\sigma\tau^{-1} = \sigma^2$, then $\tau\sigma^2\tau^{-1} = (\tau\sigma\tau^{-1})^2 = \sigma^4 \neq 1$, also a contradiction.

If $\tau\sigma\tau^{-1} = \sigma^3$, then $\tau\sigma^3\tau^{-1} = (\tau\sigma\tau^{-1})^3 = \sigma^6 = \sigma \neq 1$, also a contradiction.

So, we must have $\tau\sigma\tau^{-1} = \sigma^4$, which works out since $\tau\sigma^4\tau^{-1} = (\tau\sigma\tau^{-1})^4 = \sigma^{16} = \sigma$.

In summary, σ and τ generate G,

$$\sigma^5 = \tau^2 = 1,$$

and

$$\tau\sigma = \sigma^4\tau,$$

which shows that G is the group of the pentagon.

From the above, we know that there exists in G an abelian subgroup of index 2. Therefore, the degree of irreducible representations of G is less than or equal to 2. Because G is nonabelian, we have $[G, G] = \mathbb{Z}/5\mathbb{Z}$, and

$$G_{\text{ab}} = G/[G, G] = \mathbb{Z}/2\mathbb{Z}.$$

Therefore, there are two irreps of degree 1 (these are the irreps of G_{ab}):

1. The trivial irrep, with $R_\sigma = R_\tau = I$;

2. The irrep given by

$$R_\sigma = I$$
$$R_\tau = -I.$$

We also know that

$$10 = g = \sum_{d=\deg(R)} d^2 = 1 + 1 + n \times 2^2,$$

where R ranges over irreps of G and where n is the number of irreps of degree 2. This yields

$$8 = 4n,$$

and so, $n = 2$. Therefore, G has four irreps, including two of degee 1, and two of degree 2.

It is not hard to find the conjugacy classes of G. There are four of them:

$$\mathrm{cl}(1) = \{1\}, \quad \mathrm{cl}(\sigma) = \{\sigma, \sigma^4\}, \quad \mathrm{cl}(\sigma^2) = \{\sigma^2, \sigma^3\}, \quad \mathrm{cl}(\tau) = \{\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau\}.$$

Then, we can begin the character table:

	1/10	1/5	1/5	1/2
	$\mathrm{cl}(1)$	$\mathrm{cl}(\sigma)$	$\mathrm{cl}(\sigma^2)$	$\mathrm{cl}(\tau)$
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	x	y	z
χ_4	2	p	q	r

By column orthogonality, writing that col 1 and col 2 are orthogonal, we get

$$2 + 2x + 2p = 0,$$

that is,

$$x + p = -1;$$

writing that col 1 and col 3 are orthogonal, we get

$$y + q = -1;$$

writing that col 1 and col 4 are orthogonal, we get

$$z + r = 0.$$

Therefore, our character table becomes

	1/10	1/5	1/5	1/2
	$\mathrm{cl}(1)$	$\mathrm{cl}(\sigma)$	$\mathrm{cl}(\sigma^2)$	$\mathrm{cl}(\tau)$
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	x	y	z
χ_4	2	p	q	$-z$

Using the orthogonality relations

$$\sum_{R\,\text{irrep}} \overline{\chi_R(\sigma)}\chi_R(\tau) = \frac{g}{\text{cl}(\sigma)}\,\delta_{\text{cl}(\sigma),\text{cl}(\tau)},$$

applying this to columns 2, 3 and 3, we get

$$\begin{aligned} 2 + \overline{x}x + \overline{p}p &= \frac{10}{2} = 5 \\ 2 + \overline{y}y + \overline{q}q &= \frac{10}{2} = 5 \\ 2 + 2\overline{z}z &= \frac{10}{2} = 5, \end{aligned}$$

which yields

$$z = r = 0,$$

and

$$\begin{aligned} \overline{x}x + \overline{p}p &= 3 \\ \overline{y}y + \overline{q}q &= 3. \end{aligned}$$

We also have

$$\|\chi_3\|^2 = (\chi_3, \overline{\chi_3}) = 1 = \frac{4}{10} + \frac{2}{10}x\overline{x} + \frac{2}{10}y\overline{y},$$

which yields

$$x\overline{x} + y\overline{y} = 3.$$

Similarly, since $\|\chi_3\|^2 = (\chi_3, \overline{\chi_3}) = 1$, we get

$$p + q\overline{q} = 3.$$

Then, we have

$$x\overline{x} + y\overline{y} = 3 = \overline{x}x + \overline{p}p,$$

which yields

$$y\overline{y} = \overline{p}p.$$

From

$$(\chi_3, \chi_1) = 0,$$

we get

$$\frac{1}{10} \times 2 + \frac{1}{5}x + \frac{1}{5}y = 0,$$

and so

$$x + y = -1.$$

Using $x + p = -1$ we deduce that

$$y = p.$$

From

$$(\chi_3, \chi_4) = 0,$$

we get

$$\frac{1}{10} \times 4 + \frac{1}{5} x\overline{y} + \frac{1}{5} y\overline{q} = 0,$$

which yields

$$x\overline{y} + y\overline{q} = -2.$$

But, $y = p$, so we have

$$x\overline{y} + p\overline{q} = -2.$$

Let us now us the regular representation. Since

$$\chi_{\text{Reg}} = \chi_1 + \chi_2 + 2\chi_3 + 2\chi_4,$$

we get

$$\begin{aligned}
\chi_{\text{Reg}}(1) &= 1 + 1 + 4 + 4 = 10 \\
\chi_{\text{Reg}}(\sigma) &= 1 + 1 + 2x + 2y \\
\chi_{\text{Reg}}(\sigma^2) &= 1 + 1 + 2y + 2q \\
\chi_{\text{Reg}}(\tau) &= 1 - 1 + 2 \times 0 + 2 \times 0.
\end{aligned}$$

From $\chi_{\text{Reg}}(\sigma) = 0$, we get

$$x + y = -1,$$

and since $y + q = -1$, we deduce that

$$x = q.$$

From $\chi_{\text{Reg}}(\sigma^2) = 0$, we obtain $y + q = -1$, which we already knew.

In summary,

$$\begin{aligned}
x &= q \\
y &= p \\
p &= -1 - q,
\end{aligned}$$

and the character table becomes

	1/10	1/5	1/5	1/2
	cl(1)	cl(σ)	cl(σ^2)	cl(τ)
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	q	$-1-q$	0
χ_4	2	$-1-q$	q	0

To complete the character table, we use the fact that

$$(R_3)_\sigma^5 = I.$$

This is because

$$(R_3)_\sigma^5 = (R_3)_{\sigma^5} = (R_3)_1 = I.$$

Therefore, as $q = \chi_3(\sigma) = \mathrm{tr}((R_3)_\sigma)$, we see that q must be a sum of fifth roots of unity. If ζ is a primitive fifth root of unity, then as $\zeta^5 = 1$, we have $\zeta^{-1} = \overline{\zeta} = \zeta^4$ and $\zeta^3 = \zeta^{-2}$. The size of the second column of the table gives only one possibility, namely

$$q = \zeta + \zeta^{-1},$$

and then

$$-1 - q = -1 - \zeta - \zeta^{-1} = -1 - \zeta - \zeta^4 = \zeta^2 \ + \zeta^3 = \zeta^2 \ + \zeta^{-2}.$$

Finally, we get the character table (consisting of real entries):

	1/10	1/5	1/5	1/2
	cl(1)	cl(σ)	cl(σ^2)	cl(τ)
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	$\zeta + \zeta^{-1}$	$\zeta^2 + \zeta^{-2}$	0
χ_4	2	$\zeta^2 + \zeta^{-2}$	$\zeta + \zeta^{-1}$	0

It turns out that the character table can be used to find all the irreps of the group, and we first illustrate how to do this on the group of the pentagon.

Let G act on itself by conjugation. The action of τ on cl(τ) is

$$\begin{aligned}
\tau \cdot \tau &= \tau \\
\tau \cdot (\sigma\tau) &= \tau\sigma\tau\tau = \tau\sigma = \sigma^4\tau \\
\tau \cdot (\sigma^2\tau) &= \tau\sigma^2\tau\tau = \tau\sigma^2 = \sigma^4\tau\sigma = \sigma^8\tau = \sigma^3\tau \\
\tau \cdot (\sigma^3\tau) &= \sigma^2\tau \\
\tau \cdot (\sigma^4\tau) &= \sigma\tau.
\end{aligned}$$

Therefore, cl(τ) is invariant under the action of τ. Observe that from

$$\tau\sigma = \sigma^4\tau$$

we get $\tau\sigma\tau = \sigma^4$, and then

$$\sigma\tau = \tau\sigma^4.$$

The action of σ on $\mathrm{cl}(\tau)$ is

$$\begin{aligned}
\sigma \cdot \tau &= \sigma\tau\sigma^{-1} = \sigma\tau\sigma^4 = \sigma\sigma\tau = \sigma^2\tau \\
\sigma \cdot (\sigma\tau) &= \sigma\sigma\tau\sigma^{-1} = \sigma^2\tau\sigma^4 = \sigma^3\tau \\
\sigma \cdot (\sigma^2\tau) &= \sigma\sigma^2\tau\sigma^4 = \sigma^3\sigma\tau = \sigma^4\tau \\
\sigma \cdot (\sigma^3\tau) &= \sigma\sigma^3\tau\sigma^4 = \sigma^4\sigma\tau = \tau \\
\sigma \cdot (\sigma^4\tau) &= \sigma\sigma^4\tau\sigma^4 = \tau\sigma^4 = \sigma\tau.
\end{aligned}$$

Consider $\mathbb{C}^5$ with basis

$$e_\tau,\ e_{\sigma\tau},\ e_{\sigma^2\tau},\ e_{\sigma^3\tau},\ e_{\sigma^4\tau}.$$

The action of R is

$$\begin{aligned}
R_\sigma e_i &= e_{\sigma\cdot i} \\
R_\tau e_i &= e_{\tau\cdot i}.
\end{aligned}$$

If

$$v = e_\tau + e_{\sigma\tau} + e_{\sigma^2\tau} + e_{\sigma^3\tau} + e_{\sigma^4\tau},$$

then the subspace $W = \mathrm{span}(v)$ is stable. Then $W^\perp$ is a four-dimensional representation, and by Gram-Schmidt we get the basis

$$\begin{aligned}
z_1 &= v - 5e_{\sigma\tau} \\
z_2 &= v - 5e_{\sigma^4\tau} \\
z_3 &= v - 5e_{\sigma^2\tau} \\
z_4 &= v - 5e_{\sigma^3\tau}.
\end{aligned}$$

The matrix of R_τ on this basis is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and the matrix of R_σ on this basis is

$$\begin{pmatrix} 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix},$$

because

$$\begin{aligned}
R_\sigma(z_4) &= v - 5e_\tau \\
&= v - 5(v - e_{\sigma\tau} - e_{\sigma^2\tau} - e_{\sigma^3\tau} - e_{\sigma^4\tau}) \\
&= -(v - 5e_{\sigma\tau} + v - 5e_{\sigma^2\tau} + v - 5e_{\sigma^3\tau} + v - 5e_{\sigma^4\tau}) \\
&= -(z_1 + z_2 + z_3 + z_4).
\end{aligned}$$

Look at the eigenvectors of R_τ. Since $\tau^2 = 1$, the eigenvalues are ± 1. So we must have

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} b \\ a \\ d \\ c \end{pmatrix} = \pm \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

which in the + case yields

$$b = a; \quad c = d,$$

and in the − case

$$b = -a; \quad d = -c.$$

In the + case, a basis of the eigenspace of R_τ is given by

$$(1, 1, 0, 0), \quad (0, 0, 1, 1).$$

In the − case, a basis of the eigenspace of R_τ is given by

$$(1, -1, 0, 0), \quad (0, 0, 1, -1).$$

Let' s see whether (a, a, c, c) is an eigenvector of R_σ, for $a, c \neq 0$. We should have

$$\begin{pmatrix} 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ a \\ c \\ c \end{pmatrix} = \begin{pmatrix} a - c \\ 0 \\ -c \\ a - c \end{pmatrix} = \lambda \begin{pmatrix} a \\ a \\ c \\ c \end{pmatrix},$$

with $\lambda^5 = 1$ (since $R_\sigma^5 = I$). From $\lambda a = 0$, we get $a = 0$, and from $\lambda c = -c$, we get $c = 0$.

It follows that no eigenvector of R_τ is an eigenvector of R_σ in the + case.

A similar computation shows that no eigenvector of R_τ is an eigenvector of R_σ in the − case. But then, $W^\perp$ has no one-dimensional irrep, which implies that

$$W^\perp = R_3 \coprod R_4,$$

where R_3 and R_4 are 2-dimensional irreps and we can check that $R_4 = \overline{R_3}$. We can find the representations using geometry. Look at the pentagon again, and let ζ be a primitive fifth root of unity. Then the action of R_3 is given by

$$(R_3)_\sigma = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad (R_3)_\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and the action of R_4 is given by

$$(R_4)_\sigma = \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta^{-2} \end{pmatrix}, \quad (R_4)_\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We can check that R_3 and R_4 are irreps and that they are not equivalent.

In general, say we know the irreducible characters of a group G. How do we promote this to the irreps?

Proposition 1.23. *If (S, V) is a representation of G and if we write*

$$V = \coprod_{R \text{ irrep}} W_R^{(\chi_S, \chi_R)},$$

then the projection π_R of V onto $W_R^{(\chi_S,\chi_R)} = \coprod_{(\chi_S,\chi_R)} W$ is given by

$$\pi_R = \deg(R) \int_G \overline{\chi_R(\sigma)} S_\sigma d\sigma.$$

Proof. If we write

$$P = \deg(R) \int_G \overline{\chi_R(\sigma)} S_\sigma d\sigma,$$

then $\overline{\chi_R(\sigma)}$ is a class function and

$$\int_G \overline{\chi_R(\sigma)} S_\sigma d\sigma = S[\overline{\chi_R(\sigma)}]$$

intertwines S with itself. Then, for any irrep $\widetilde{R}$, observe that by Schur's Lemma, we have

$$P \mid W_{\widetilde{R}} = \begin{cases} 0 & \text{if } \widetilde{R} \neq R \\ \text{id} & \text{if } \widetilde{R} = R. \end{cases}$$

By Schur's Lemma again, $P \mid W_R = \lambda I$, with

$$\lambda = \frac{\deg(R)}{\deg(R)} (\overline{\overline{\chi_R}}, \chi_R) = 1.$$

Therefore, $P \mid W_R = I$ and $P \mid W_{\widetilde{R}} = 0$ if $\widetilde{R} \neq R$, which shows that P is indeed the projection onto $W_R^{(\chi_S,\chi_R)} = \coprod_{(\chi_S,\chi_R)} W$. □

Apply Proposition 1.23 to the regular representation. We know that

$$\text{Reg} = \coprod_{R \text{ irrep}} V_R^{\deg(R)}$$

with

$$\deg(R) = (\chi_{\text{Reg}}, \chi_R),$$

and Proposition 1.23 yields the projection

$$\pi_R \colon V_{\text{Reg}} \longrightarrow V_R^{\deg(R)}.$$

Consequently, since we know V_{Reg} and $\deg(R)$ (from the character table), we obtain V_R. Therefore, knowledge of the character table and of the regular representation yields all irreps of the group.

1.5 Induced Representations and Frobenius Reciprocity

The set-up is the following:

G is a group with a Haar measure, H is a subgroup of G (not necessarily normal), and we are given a representation (S, W) of H. The goal is to make a representation of G from these data.

The basic construction is to define the set of functions $\mathrm{Map}_H(G, W)$ given by:

$$\mathrm{Map}_H(G,W) = \left\{ f\colon G \to W \;\middle|\; \begin{array}{l} 1.\ f \in L^2(G,W) \\ 2.\ f(\sigma\tau) = \tau^{-1}\cdot f(\sigma), \\ \qquad \text{for all } \sigma \in G \text{ and all } \tau \in H \end{array} \right\}.$$

The set $\mathrm{Map}_H(G, W)$ is a vector space which is also known under the following notation in the literature:

(1) $\pi^G_{*H}(W)$, called the *direct image of* W.

(2) $\mathrm{ind}^G_H(W)$, called the *induced space of* W.

Observe that

$$\begin{aligned} f(\sigma(\tau\rho)) &= f((\sigma\tau)\rho) \\ &= \rho^{-1} f(\sigma\tau) \\ &= \rho^{-1}\tau^{-1} f(\sigma) \\ &= (\tau\rho)^{-1} f(\sigma). \end{aligned}$$

We can define a G-action on $\pi^G_{*H}(W)$ *via*:

$$(\sigma f)(\rho) = f(\sigma^{-1}\rho), \quad f \in \pi^G_{*H}(W),\ \sigma, \rho \in G.$$

Let's check that this is indeed an action. We have

$$\begin{aligned} ((\sigma\tau)(f))(\rho) &= f((\sigma\tau)^{-1}\rho) \\ &= f(\tau^{-1}\sigma^{-1}\rho) \\ &= (\tau f)(\sigma^{-1}\rho) \\ &= (\sigma(\tau f))(\rho), \end{aligned}$$

as required.

The representation of G whose space is $\mathrm{Map}_H(G, W) = \pi^G_{*H}(W)$ is the *representation induced by* (S, W) *on* G *(from* H*)*. This representation is denoted by $\pi^G_{*H}(S)$.

We can also go backwards. Given any representation (R, V) of G, the restriction of R to H yields a representation of H with representation space called *representation of G restricted to H*. The notation for this representation is

$$\pi_H^{*G}(R) = \mathrm{res}_H^G(R),$$

and it is also called the *inverse image of (R, V) on H*.

Proposition 1.24. *Given any group G and two subgroups K, H of G such that $K \subseteq H \subseteq G$, we have (transitivity of induction)*

$$\pi_{*H}^G(\pi_{*K}^H) = \pi_{*K}^G,$$

and similarly (transitivity of restriction)

$$\pi_K^{*H}(\pi_H^{*G}) = \pi_K^{*G}.$$

Proof. The second statement is a tautology.

For the first statement, pick a K-space W, and consider

$$\mathrm{Map}_H(G, \mathrm{Map}_K(H, W)) = \pi_{*H}^G(\pi_{*K}^H).$$

Pick $f \in \mathrm{Map}_H(G, \mathrm{Map}_K(H, W))$ and $\sigma \in G$. Then

$$f(\sigma) \in \mathrm{Map}_K(H, W).$$

If $\rho \in K$, then

$$f(\sigma)(\tau\rho) = \rho^{-1}(f(\sigma)(\tau)). \tag{$*$}$$

Since $f \in \mathrm{Map}_H(G, -)$, we have

$$f(\sigma\theta) = \theta^{-1} f(\sigma), \quad \theta \in H,$$

and since $f(\sigma) \in \mathrm{Map}_K(H, W)$, we get

$$(\tau^{-1} f(\sigma))(\theta) = f(\sigma)(\theta\tau).$$

If we set $\theta = 1$, then

$$(\tau^{-1} f(\sigma))(1) = f(\sigma)(\tau).$$

Then, substituting the left-hand side for the right-hand side in $(*)$, we obtain

$$f(\sigma)(\tau\rho) = \rho^{-1}(\tau^{-1} f(\sigma))(1)) = (\tau\rho)^{-1}(f(\sigma)(1)).$$

If we set $\tau = 1$, we obtain

$$f(\sigma)(\rho) = \rho^{-1}(f(\sigma)(1)). \tag{$**$}$$

Define $\Theta\colon \mathrm{Map}_H(G, \mathrm{Map}_K(H, W)) \to \mathrm{Map}_K(G, W)$ such that

$$\Theta(f)(\sigma) = f(\sigma)(1), \quad \sigma \in G.$$

Observe that $(**)$ implies that

$$\rho^{-1}\Theta(f)(\sigma) = f(\sigma)(\rho), \quad \rho \in K. \tag{a}$$

We would like to prove that

$$\Theta(f)(\sigma\rho) = \rho^{-1}\Theta(f)(\sigma), \quad \sigma \in G,\ \rho \in K.$$

For this, note that by $(**)$,

$$\Theta(f)(\sigma\rho) = f(\sigma\rho)(1) = (\rho^{-1}f(\sigma))(1) = f(\sigma)(\rho). \tag{b}$$

Then, using (a) and (b), we get

$$\Theta(f)(\sigma\rho) = f(\sigma)(\rho) = \rho^{-1}\Theta(f)(\sigma)$$

as required. This shows that $\Theta(f) \in \mathrm{Map}_K(G, W)$.

We can also define an inverse map and show that Θ and this maps are mutual inverses (DX). □

Take $H = \{1\}$, and take the representation to be the identity representation I from H to $\mathbb{C}^*$, where $1 \mapsto 1$. In this case, the representation space is

$$\mathrm{Map}_1(G, \mathbb{C}) = L^2(G, \mathbb{C}),$$

and the action is given by

$$(\sigma f)(\theta) = f(\sigma^{-1}\theta).$$

Therefore, we get the regular representation and

$$\pi_{*1}^G(I) = \mathrm{Reg}_G.$$

Corollary 1.25. *If $H \subseteq G$, then*

$$\pi_{*H}^G(\mathrm{Reg}_H) = \mathrm{Reg}_G.$$

Proof. By the remark just before Corollary 1.25,

$$\mathrm{Reg}_H = \pi_{*1}^H(I),$$

and by Corollary 1.25,

$$\begin{aligned}\pi_{*H}^G(\mathrm{Reg}_H) &= \pi_{*H}^G(\pi_{*1}^H(I)) \\ &= \pi_{*1}^G(I) \\ &= \mathrm{Reg}_G,\end{aligned}$$

as required. □

Proposition 1.26. *(Adjointness of π^* and π_*) Say H is a subgroup of G, W is a representation space of H, and V is a representation space of G. Then, there exists a natural isomorphism*

$$\mathrm{Hom}_H(\pi_H^{*G}(V), W) \approx \mathrm{Hom}_G(V, \pi_{*H}^G(W)),$$

where the left-hand side is the set of all linear maps θ such that

$$\theta(hv) = h\theta(v), \quad h \in H,\ v \in V,$$

and mutatis mutandis for the right-hand-side.

Proof. If $\varphi \in \mathrm{Hom}_G(V, \mathrm{Map}_H(G, W))$, then $\varphi(v) \in \mathrm{Map}_H(G, W)$ and

$$\varphi(\sigma v) = \sigma\varphi(v).$$

It follows that

$$\varphi(\sigma v)(\tau) = (\sigma\varphi(v))(\tau) = \varphi(v)(\sigma^{-1}\tau). \tag{$\dagger$}$$

We define the map $\Theta\colon \mathrm{Hom}_G(V, \mathrm{Map}_H(G, W)) \to \mathrm{Hom}_H(\pi_H^{*G}(V), W)$ by

$$\Theta(\varphi)(v) = \varphi(v)(1), \quad v \in V.$$

We need to check that $\Theta(\varphi) \in \mathrm{Hom}_H(\pi_H^{*G}(V), W)$, *i.e.* that

$$\Theta(\varphi)(hv) = h(\Theta(\varphi)(v)), \quad h \in H,$$

or equivalently

$$\varphi(hv)(1) = h(\varphi(v)(1)), \quad h \in H.$$

As $\varphi(v) \in \mathrm{Map}_H(G, W)$, we have

$$\varphi(v)(\sigma h) = h^{-1}(\varphi(v)(\sigma)).$$

But, as $\varphi \in \mathrm{Hom}_G(-, -)$,

$$\varphi(\tau v) = \tau\varphi(v),$$

so

$$\varphi(\tau v)(\sigma) = (\tau\varphi(v))(\sigma) = \varphi(v)(\tau^{-1}\sigma), \quad \tau \in G.$$

If we let $\sigma = 1$ and $\tau = h \in H$ in the above equation, we get

$$\varphi(hv)(1) = \varphi(v)(h^{-1}) = \varphi(v)(1 \cdot h^{-1}) = h(\varphi(v)(1)),$$

as required.

Next, we define $\Psi\colon \mathrm{Hom}_H(\pi_H^{*G}(V), W) \to \mathrm{Hom}_G(V, \mathrm{Map}_H(G, W))$ so that for every $\xi\colon \pi_H^{*G}(V) \to W$,

$$\Psi(\xi)(v)(\sigma) = \xi(\sigma^{-1}v), \quad v \in V,\ \sigma \in G.$$

Then we can check that Θ and Ψ are mutual inverses. Indeed, we have

$$\begin{aligned}(\Theta\Psi)(\xi)(v) &= \Theta(\Psi(\xi))(v)\\ &= \Psi(\xi)(v)(1)\\ &= \xi(1^{-1}v)\\ &= \xi(v),\end{aligned}$$

and

$$\begin{aligned}(\Psi\Theta)(\varphi)(v)(\sigma) &= \Psi(\Theta(\varphi))(v)(\sigma)\\ &= \Theta(\varphi)(\sigma^{-1}v)\\ &= \varphi(\sigma^{-1}v)(1)\\ &= \varphi(v)(\sigma),\end{aligned}$$

using (†) in the last step. □

Say (S, W_1) and (T, W_2) are representations for H, and consider $\mathrm{Hom}_H(W_1, W_2)$. This space consists of all linear maps $\varphi\colon W_1 \to W_2$ such that

$$\varphi(\sigma w_1) = \sigma\varphi(w_1), \quad w_1 \in W_1,\ \sigma \in H.$$

However, in terms of our representations

$$\begin{aligned}\sigma w_1 &= S_\sigma(w_1)\\ \sigma\varphi(w_1) &= T_\sigma(\varphi(w_1)),\end{aligned}$$

so the condition $\varphi(\sigma w_1) = \sigma\varphi(w_1)$ says that

$$\varphi(S_\sigma(w_1)) = T_\sigma(\varphi(w_1)),$$

namely that φ is an intertwiner of S and T.

Pick $f \in \mathrm{Map}_H(G, W)$, and let R be a system of left coset representatives for H in G. This measn that every $\sigma \in G$ has the form

$$\sigma = rh,$$

where $r \in R$ is some coset representative and $h \in H$ (the axiom of choice is needed to define R if G and H are infinite). Since

$$f(\sigma) = f(rh) = h^{-1}f(r),$$

we see that f is determined on G if we know $f(r)$ for all $r \in R$. So, f belongs to the product

$$\prod_{r\in R} W = W^R.$$

If R is finite, say $R = \{r_1, \ldots, r_t\}$, then $f \in \mathrm{Map}_H(G, W)$ is a t-tuple $(f(r_1), \ldots, f(r_t)) \in W^t$. The action of G is given by

$$(\sigma f)(\tau) = f(\sigma^{-1}\tau), \quad \sigma, \tau \in G.$$

We would like to know how an element $\sigma \in G$ acts on $\prod_{r \in R} W$. We have $\sigma = \rho h$ for some $\rho \in R$ and some $h \in H$. For any $r \in R$, we have

$$(\sigma f)(r) = f(\sigma^{-1} r) = f(h^{-1}\rho^{-1} r).$$

Now, $\rho^{-1} r = r(\rho)\widetilde{h}$, for some coset representative $r(\rho) \in R$ and some $\widetilde{h} \in H$, so if $f(r) \in W_r$, then $f(\rho^{-1}) \in W_{r(\rho)}$. We can write

$$h^{-1}\rho^{-1} r = (h^{-1}\rho^{-1} r h)h^{-1},$$

and we get

$$f(h^{-1}\rho^{-1} r) = h f(h^{-1}\rho^{-1} r h) \in W_{h^{-1}\rho^{-1} r h}.$$

This shows that $\sigma = \rho h$ permutes the copies of W. Note also that

$$\dim(\mathrm{Map}_H(G, W)) = (G : H)\dim(W).$$

Let us now consider the isomorhism of Proposition 1.26 in the special case where W is a uniirrep of H and V is a uniirrep of G, with

1. $\dim(W)$ finite.
2. $\dim(V)$ finite.

   (The above conditions are satisfied if G is finite or compact.)

3. $(G : H)$ is finite.

Then,

$$\mathrm{Map}_H(G, V) \approx \prod_{r \in R} W = \coprod_{U \text{ irrep}} U^{n_U},$$

where n_U is the number of times that U appears. Then,

$$\mathrm{Hom}_G(V, \mathrm{Map}_H(G, V)) \approx \mathrm{Hom}_G\left(V, \coprod_{U \text{ irrep}} U^{n_U}\right) \approx \prod_{U \text{ irrep}} (\mathrm{Hom}_G(V, U))^{n_U}.$$

However, recall that $\mathrm{Hom}_G(V, U)$ consists of the intertwiners of V and U, so if U and V are not equivalent, then by Schur's lemma,

$$\mathrm{Hom}_G(V, U) = (0),$$

and if U and V are equivalent, then, V appears n_U times in $\mathrm{Map}_H(G, V)$.

Similarly,

$$\pi_H^{*G}(V) \approx \coprod_{T \text{ irred}} T^{m_T},$$

where m_T is the number of times that T appears in $\pi_H^{*G}(V)$, and we have

$$\mathrm{Hom}_H(\pi_H^{*G}(V), W) \approx \mathrm{Hom}_H\left(\coprod_{T \text{ irred}} T^{m_T}, W\right) \approx \prod_{T \text{ irred}} (\mathrm{Hom}_H(T, W))^{m_T}.$$

By Schur's Lemma again, if T and W are inequivalent, then

$$\mathrm{Hom}_H(T, W) = (0),$$

else if T and W are equivalent then T appears m_T times in $\pi_H^{*G}(V)$. But then, the isomorphism

$$\mathrm{Hom}_H(\pi_H^{*G}(V), W) \approx \mathrm{Hom}_G(V, \pi_{*H}^G(W))$$

implies that the number of times that W appears in $\pi_H^{*G}(V)$ is equal to the number of times that V appears in $\pi_{*H}^G(W)$, which we state as the following theorem:

Theorem 1.27. *(Weak Frobenius Reciprocity) Given two groups $H \subseteq G$, if $(G : H)$ is finite and if the irreps of H and G are finite-dimensional, then for any irrep W of H and any irrep V of G, the number of times that W appears in $\pi_H^{*G}(V)$ is equal to the number of times V that appears in $\pi_{*H}^G(W)$.*

Given two groups G and H with $H \subseteq G$, if S is a representation of H and χ_S is its character, then a (messy) computation shows that

$$\chi_{\pi_{*H}(S)}(\xi) = \sum_{\substack{\rho \in R \\ \rho^{-1}\xi\rho \in H}} \chi_S(\rho^{-1}\xi\rho) = (G : H) \int_{I(H,\xi)} \chi_S(\sigma^{-1}\xi\sigma) d\sigma, \qquad (*)$$

where

(1) R is a system of coset representatives of H in G, and

(2) $I(H, \xi) = \{\sigma \in G \mid \sigma^{-1}\xi\sigma \in H\}$.

Equality of these two formulae come from the fact that if

$$\sigma = \rho h, \quad \rho \in R,\ h \in H$$

then

$$\sigma^{-1}\xi\sigma = h(\rho^{-1}\xi\rho)h.$$

Therefore, $\sigma \in I(H,\xi)$ iff $\rho \in R$ and $\rho^{-1}\xi\rho \in H$. Then, we have

$$\begin{aligned}\int_{I(H,\xi)} \chi_S(\sigma^{-1}\xi\sigma)d\sigma &= \frac{1}{g}\sum_{\sigma\in I(H,\xi)} \chi_S(\sigma^{-1}\xi\sigma)\\ &= \frac{1}{g}\sum_{h\in H}\sum_{\substack{\rho\in R\\ \rho^{-1}\xi\rho\in H}} \chi_S(h^{-1}\rho^{-1}\xi\rho h)\\ &= \frac{1}{g}\sum_{h\in H}\sum_{\substack{\rho\in R\\ \rho^{-1}\xi\rho\in H}} \chi_S(\rho^{-1}\xi\rho)\\ &= \frac{h}{g}\sum_{\substack{\rho\in R\\ \rho^{-1}\xi\rho\in H}} \chi_S(\rho^{-1}\xi\rho),\end{aligned}$$

so

$$\sum_{\substack{\rho\in R\\ \rho^{-1}\xi\rho\in H}} \chi_S(\rho^{-1}\xi\rho) = \frac{g}{h} = \int_{I(H,\xi)} \chi_S(\sigma^{-1}\xi\sigma)d\sigma,$$

as claimed.

Sketch of proof for equation $(*)$. We choose a convenient basis to make the computation of the matrices and we compute their traces.

Recall that $\pi_{*H}(S)$ acts on $\mathrm{Map}_H(G,W)$ where W is the representation space of S. We know that

$$\mathrm{Map}_H(G,W) = \coprod_{\rho\in R} W;$$

write ρW for the copy of W corresponding to the coset ρH, with $\rho \in R$. Choose a basis for W, say $e_1,\dots,e_t$; then "repeat these" indexing the repetitions by ρ. The basis consists of pairs (ρ, e_j), with $\rho \in R$ and $j = 1,\dots,t$. The "mess" comes from explicating the action of $\sigma \in G$, where we write $\sigma = \rho h$, and then determining the diagonal elements of the matrix. □

Say $f \in L^2_{\mathrm{cl}}(H)$, we want to make $\pi_* f \in L^2_{\mathrm{cl}}(G)$. Inspired by the above formula, we set

$$(\pi_* f)(\xi) = (G:H)\int_{I(H,\xi)} f(\sigma^{-1}\xi\sigma)d\sigma.$$

Observe that using the invariance of the Haar integral, we have

$$\begin{aligned}(\pi_* f)(\theta^{-1}\xi\theta) &= (G:H)\int_{I(H,\theta^{-1}\xi\theta)} f(\sigma^{-1}\theta^{-1}\xi\theta\sigma)d\sigma \\ &= (G:H)\int_{I(H,\theta^{-1}\xi\theta)} f((\theta\sigma)^{-1}\xi\theta\sigma)d\sigma \\ &= (G:H)\int_{I(H,\xi)} f(\eta^{-1}\xi\eta)d\eta \\ &= (\pi_* f)(\xi).\end{aligned}$$

This means that $(\pi_* f)(\xi)$ is a class function. Given a class function $g \in L^2_{\mathrm{cl}}(G)$, we let $\pi^*(g)$ denote the restriction of f to H.

Theorem 1.28. *(Frobenius Reciprocity) Say H is a subgroup of G, of finite index. Given any $f \in L^2_{\mathrm{cl}}(H)$ and any $g \in L^2_{\mathrm{cl}}(G)$, we have*

$$(\pi^* g, f)_H = (g, \pi_* f)_G.$$

Thus, the two linear maps $\pi^*\colon L^2_{\mathrm{cl}}(G) \to L^2_{\mathrm{cl}}(H)$ (restriction) and $\pi_*\colon L^2_{\mathrm{cl}}(H) \to L^2_{\mathrm{cl}}(G)$ (induction) are adjoint maps.

Proof. Any class function on H is a linear combination of characters of H and characters of H are linear combinations of irreducible characters. The same is true for the class functions of G. Both sides of the Frobenius equation are bilinear, therefore we only need to check the adjunction for $f = \chi_S$ and $g = \chi_R$, where S is an irrep of H and R is an irrep of G. We have

$$\begin{aligned}\pi^* g &= \pi^* \chi_R = \chi_{\pi^* R} \\ \pi_* f &= \pi_* \chi_S = \chi_{\pi_* S},\end{aligned}$$

so

$$(\pi^* g, \chi_S)_H = (\chi_{\pi^* R}, \chi_S)_H = \text{number of times } S \text{ appears in } \pi^* R$$

and

$$(\chi_R, \pi_* f)_G = (\chi_R, \chi_{\pi_* S})_G = \text{number of times } R \text{ appears in } \pi_* S.$$

By the Weak Frobenius Reciprocity, the right-hand sides are equal, which establishes the Frobenius reciprocity equation. □

We now return to finite groups and show that the degree of any irrep of G divides the order of G. The proof makes use of some basic properties of rings, namely of the integral closure of a ring.

The set-up is this: We have an integral domain A and some commutative ring B such that $A \subseteq B$.

Definition 1.11. (Emmy Noether, 1921) An element $b \in B$ is *integral over* A if there is a monic polynomial

$$P(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n,$$

with $\alpha_1, \ldots, \alpha_n \in A$, so that $P(b) = 0$. Let

$$\mathrm{Int}_A(B) = \{\xi \in B \mid \xi \text{ integral over } A\}.$$

The following facts hold:

(1) The sum of two integral elements of B is again integral.

(2) The product of two integral elements of B is again integral.

(3) If $A \subseteq C \subseteq B$ and if $b \in B$ is integral over C and all the coefficients of the polynomial for b (over C) are themselves integral over$A$, then b is integral over A.

Given an integral domain A, denote by $K = \mathrm{Frac}(A)$ the field of fractions of A. For example

1. If $A = \mathbb{Z}$, then $K = \mathbb{Q}$.
2. If $A = \mathbb{C}[x]$, then $K = \mathbb{C}(x) = \{f/g \mid f, g \in \mathbb{C}[x], g \neq 0\}$.
3. If $A = \mathbb{C}[x_1, \ldots, x_n]$, then $K = \mathbb{C}(x_1, \ldots, x_n) = \{f/g \mid f, g \in \mathbb{C}[x_1, \ldots, x_n], g \neq 0\}$.

A ring is a UFD iff every element of A is uniquely a product of irreducible elements, up to order and up to a unit. All the above examples are UFD's.

Proposition 1.29. *If A is a UFD then*

$$\mathrm{Int}_A(\mathrm{Frac}(A)) = \{\xi \in \mathrm{Frac}(A) \mid \xi \textit{ integral over } A\} = A.$$

We say that A is integrally closed.

Proof. Say $\xi = a/b \in \mathrm{Frac}(A)$ satisfies a monic polynomial with coefficients in A,

$$P(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n.$$

Since A is a UFD, we may assume that no irreducible factor belongs to both a and b. From

$$\frac{a^n}{b^n} + \alpha_1 \frac{a^{n-1}}{b^{n-1}} + \cdots + \alpha_n = 0,$$

multiplying both sides by b^n, we get

$$-a^n = b(\alpha_1 a^{n-1} + \cdots + \alpha_n b^{n-1}).$$

However, in a UFD, an irreducible element p that divides a product $\alpha\beta$ divides one of the factors. Therefore, if p is irreducible and if p divide b, then p divides a^n, and thus p divides a. This contradicts the fact that a and b have no irreducible factor in common, and so b has no irreducible factor, which implies that b is unit. Then $b^{-1} \in A$, and $a/b \in A$. □

Next, we need the group algebra $\mathbb{C}[G]$, defined by

$$\mathbb{C}[G] = \left\{ \text{formal finite sums } \sum_{\sigma \in G} a(\sigma)\sigma \mid a(\sigma) \in \mathbb{C} \right\}.$$

This is a complex vector space and we define a (noncommutative) multiplication on $\mathbb{C}[G]$ *via*

$$\left(\sum_{\sigma \in G} a(\sigma)\sigma \right) \left(\sum_{\tau \in G} b(\tau)\tau \right) = \sum_{\theta \in G} \left(\sum_{\sigma\tau = \theta} a(\sigma)b(\tau) \right) \theta.$$

The integral group algebra $\mathbb{Z}[G]$ is defined in a similar fashion.

Proposition 1.30. *If G is finite group, an element $\sum_{\sigma \in G} a(\sigma)\sigma \in \mathbb{C}[G]$ is in the center $Z(\mathbb{C}[G])$ of $\mathbb{C}[G]$ iff the function $\sigma \mapsto a(\sigma)$ is a class function. Moreover, a basis of $Z(\mathbb{C}[G])$ consists of the elements*

$$\epsilon_C = \sum_{\sigma \in C} \sigma,$$

where C is a conjugacy class of G. Therefore

$$\dim_{\mathbb{C}}(Z(\mathbb{C}[G])) = \text{conj}(G) = \#(\textit{irreps of } G).$$

Proof. Let $\alpha = \sum_{\sigma \in G} a(\sigma)\sigma$, then $\alpha \in Z(\mathbb{C}[G])$ iff

$$\alpha\tau = \tau\alpha, \quad \text{for all } \tau \in G$$

iff

$$\tau^{-1}\alpha\tau = \alpha, \quad \text{for all } \tau \in G.$$

But,

$$\tau^{-1}\alpha\tau = \sum_{\sigma \in G} a(\sigma)\tau^{-1}\sigma\tau,$$

so $\alpha = \tau^{-1}\alpha\tau$ iff

$$a(\tau^{-1}\sigma\tau) = a(\tau), \quad \text{for all } \tau \in G,$$

which shows that a is a class function. Write $a(C)$ for the common value of a on the conjugacty class C. Then, $\alpha \in Z(\mathbb{C}[G])$ iff

$$\begin{aligned} \alpha &= \sum_C \left(\sum_{\sigma \in C} a(C)\sigma \right) \\ &= \sum_C a(C) \left(\sum_{\sigma \in C} \sigma \right) \\ &= \sum_C a(C)\epsilon_C. \end{aligned}$$

Therefore, the ϵ_C span $Z(\mathbb{C}[G])$, and because conjugacy classes are disjoint, they are linearly independent. □

Proposition 1.31. *Say $\alpha = \sum_{\sigma \in G} a(\sigma)\sigma \in Z(\mathbb{C}[G])$, and $a(\sigma)$ is integral over $\mathbb{Z}$. Then, α itself is integral over $\mathbb{Z}$.*

Proof. By Proposition 1.30, we have

$$\alpha = \sum_C a(C)\epsilon_C.$$

If all ϵ_C are integral over $\mathbb{Z}$, then α is integral over $\mathbb{Z}$. The ϵ_C form a basis for $Z(\mathbb{C}[G])$ and they are contained in a finitely generated module over $\mathbb{Z}$, namely the set of all elements of the form

$$\left\{ \sum_C n(C)\epsilon_C \mid n_C \in \mathbb{Z} \right\}.$$

Emmy Noether proved that such elements are indeed integral over $\mathbb{Z}$. □

Theorem 1.32. *If G is a finite group and d is the degree of any irrep of G, then d divides the order of G.*

Proof. Consider the character χ_R of any representation R of G and write

$$\xi = \sum_{\sigma \in G} \overline{\chi_R(\sigma)}\sigma.$$

Since each σ satisfies $\sigma^n = 1$, for some n, we have

$$R_\sigma^n = R_{\sigma^n} = R_1 = I,$$

which implies that the eigenvalues of R_σ are roots of unity, and thus integral over $\mathbb{Z}$. But $\chi_R(\sigma)$ is the sum of the eigenvalues of R_σ, so it is also integral over $\mathbb{Z}$. Therefore, by the previous two Propositions, ξ is integral over $\mathbb{Z}$.

Now, let $\chi = \chi_R$ be the character of an irreducible representation R. When we apply R to ξ we get

$$R(\xi) = \sum_{\sigma \in G} \overline{\chi_R(\sigma)} R_\sigma,$$

and $R(\xi)$ is integral over $\mathbb{Z}$ because ξ is, and because R is a homomorphism ($R(\xi)$ and ξ are satisfy the same polynomial). But, $R(\xi) = R[\overline{\chi}]$, the $\overline{\chi}$-weighted automorphism from R. Since R is irreducible, by Schur's Lemma

$$R(\xi) = xI$$

for some $x \in \mathbb{C}$. From the above discussion, x is integral over $\mathbb{Z}$. By previous work,

$$x = \frac{\#(G)}{d}\overline{(\chi_R, \chi_R)},$$

and because R is irreducible, $(\chi_R, \chi_R) = 1$, so

$$x = \frac{\#(G)}{d}$$

is integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is a UFD, it is integrally closed, so $\#(G)/d \in \mathbb{Z}$, and d must divide $\#(G)$. □

Here are a few more facts stated without proof.

1. If $Z(G)$ denotes the center of G and if d is the degree of any irrep of G, then d divides $(G : Z(G))$.

2. Say A is a normal, abelian subgroup of G. Then d (as in (1)) divides $(G : A)$.

3. *Artin Induction Theorem* (1920). Every rational combination of irreducible characters of G, ($\sum_{R\,\text{irrep}} a(R)\chi_R$, with $a(R) \in \mathbb{Q}$), is a sum (with coefficients in $\mathbb{Q}$) of characters induced from *cyclic* subgroups of G.

4. *Brauer Induction Theorem* (1948). Every irreducible character of G is a linear combination with integral coefficients of characters induced by *elementary* subgroups of G

   A subgroup H of G is *elementary* if $H = P \times C$, where P is a p-group (P has order p^h, for some prime p) and C is cyclic of order prime to p. (A shorter proof was given later in the 1950's by Brauer and Tate.)

5. *Converse of Brauer's Theorem, J. Green.* Let $\mathcal{F}$ be a family of subgroups of G, and assume that each irreducible character of G is an integral linear combination of induced characters from subgroups in $\mathcal{F}$. Then, $\mathcal{F}$ contains a conjugate of every elementary subgroup of G.

Proofs of most of the above results, as well as a masterly presentation of the linear representation of finite groups, are found in Serre [13].

1.6 Lie Groups and Lie Algebras

A Lie group G is a topological space which is a smooth manifold and a topological group, which means that group multiplication and inverse are smooth functions.

Examples

1. (a) $G = \mathbf{GL}(n, \mathbb{R})$, the group of $n \times n$ real invertible matrices.
   (b) $G = \mathbf{GL}(n, \mathbb{C})$, the group of $n \times n$ complex invertible matrices. In the special case $n = 1$, $\mathbb{G}_{m,\mathbb{R}} = \mathbf{GL}(1, \mathbb{R}) = \mathbb{R}^*$, and $\mathbb{G}_{m,\mathbb{C}} = \mathbf{GL}(1, \mathbb{C}) = \mathbb{C}^*$.

2. $\mathbb{G}_a(\mathbb{R}^n)$, the group of translations by a fixed vector in $\mathbb{R}^n$, and $\mathbb{G}_a(\mathbb{C}^n)$, the group of translations by a fixed vector in $\mathbb{C}^n$.

3. Let V be a complex vector space of dimension n with a Hermitian inner product denoted by $(-,-)$. Let $\mathbf{U}(n)$ be group given by

$$\mathbf{U}(n) = \{\sigma \in \mathbf{GL}(n,\mathbb{C}) \mid (\sigma(x),\sigma(y)) = (x,y),\ x,y \in V\}.$$

The group $\mathbf{U}(n)$ is the *unitary group*. The unitary group is a closed subgroup of $\mathbf{GL}(n,\mathbb{C})$, and the implicit function theorem can be used to find smooth charts on $\mathbf{U}(n)$, so $\mathbf{U}(n)$ is a Lie group. A matrix σ belongs to $\mathbf{U}(n)$ iff

$$\sigma\sigma^* = \sigma^*\sigma = I,$$

where $\sigma^* = (\overline{\sigma})^\top = \overline{(\sigma^\top)}$. The subgroup of $\mathbf{U}(n)$ given by

$$\mathbf{SU}(n) = \{\sigma \in \mathbf{U}(n) \mid \det(\sigma) = 1\}$$

is again a Lie group. In the special case when $n = 1$, we have

$$\mathbf{U}(1) = \{\lambda \in \mathbb{C}^* \mid \lambda^{-1} = \overline{\lambda}\} = \{\lambda \in \mathbb{C}^* \mid |\lambda| = 1\},$$

so $\mathbf{U}(1)$ is the set of points on the unit circle, S^1, and $\mathbf{SU}(1) = \{1\}$.

We have the exact sequence

$$0 \longrightarrow \mathbf{SU}(n) \longrightarrow \mathbf{U}(n) \xrightarrow{\det} S^1 \longrightarrow 0.$$

In $\mathbb{R}^n$, if $(-,-)$ is a Euclidean inner product (a symmetric bilinear form which is positive definite), we define $\mathbf{O}(n)$ and $\mathbf{SO}(n)$ by

$$\mathbf{O}(n) = \{\sigma \in \mathbf{GL}(n,\mathbb{R}) \mid (\sigma(u),\sigma(v)) = (u,v),\ u,v \in \mathbb{R}^n\},$$

and

$$\mathbf{SO}(n) = \{\sigma \in \mathbf{O}(n) \mid \det(\sigma) = 1\}.$$

We have $\sigma \in \mathbf{O}(n)$ iff

$$\sigma^{-1} = \sigma^\top.$$

Both $\mathbf{O}(n)$ and $\mathbf{SO}(n)$ are Lie groups.

If $[-,-]$ is a bilinear skew-symmetric form ($[v,u] = -[u,v]$) on $\mathbb{R}^n$ which is nondegenerate (which means that if $[u,v] = 0$ for all v, then $u = 0$), then n must be even, and we define the *symplectic group* by

$$\mathbf{Sp}(n) = \{\sigma \in \mathbf{GL}(n,\mathbb{R}) \mid [\sigma(u),\sigma(v)] = [u,v],\ u,v \in \mathbb{R}^n\}.$$

It is easy to see that the adjoint of σ with respect to $[-,-]$ is $-\sigma^\top$, so $\sigma \in \mathbf{Sp}(n)$ iff

$$\sigma^{-1} = -\sigma^\top.$$

Observe that if $\sigma \in \mathbf{Sp}$, then $i\sigma \in \mathbf{U}(n)$.

Every bilinear form φ on $\mathbb{R}^n$ is given by an $n \times n$ matrix B, where

$$\varphi(x, y) = x^\top B y.$$

The bilinear form φ is symmetric iff B is a symmetric matrix, and nondegenerate iff B is invertible. The bilinear form φ is skew-symmetric iff $B^\top = -B$. In the symmetric case, the symmetric matrix B can be diagonalized by an orthonormal basis Q, as

$$B = QDQ^\top,$$

where D is a real diagonal matrix

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 & 0 \\ 0 & \lambda_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \lambda_{n-1} & 0 \\ 0 & 0 & \dots & 0 & \lambda_n \end{pmatrix}.$$

With respect to the orthonormal basis given by Q,

$$B(x, y) = \sum_{=1}^{n} \lambda_i x_i y_i.$$

If B is a nondegenerate skew-symmetric matrix, it can be block-diagonalized by an orthonormal basis Q, as

$$B = QDQ^\top,$$

where D is a real skew-symmetric matrix of the form

$$D = \begin{pmatrix} 0 & -\lambda_1 & \dots & 0 & 0 \\ \lambda_1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & & -\lambda_n \\ 0 & 0 & \dots & \lambda_n & 0 \end{pmatrix}.$$

Say X and Y are two manifolds, with X connected and let $\varphi\colon X \to Y$ be a smooth map between them. We say that φ is a *covering map* iff for every $y \in Y$, there is some open subset $U \subseteq Y$ with $y \in U$, so that $\varphi^{-1}(U)$ is a disjoint union of open sets $V_\alpha \subseteq X$, and

$\varphi \mid V_\alpha$ is a diffeomorphism from V_α onto U. From an intuitive point of view, X locally over y "looks like a stack of pancakes."

Example. $X = \mathbb{R}$, $Y = S^1 = \mathbf{U}(1)$, and $\varphi\colon \mathbb{R} \to S^1$ is given by

$$\varphi(x) = e^{2\pi i x}.$$

Consider $y = 1$, take a small $U = (e^{-2\pi i\epsilon}, e^{2\pi i\epsilon})$, then

$$\varphi^{-1}(U) = \{x \in \mathbb{R} \mid e^{2\pi i x} \in U\} = \bigcup_{n\in\mathbb{Z}} (-2\pi\epsilon + n2\pi, 2\pi\epsilon + n2\pi).$$

Here are a few fundamental facts:

(1) Say $\varphi\colon X \to G$ is a covering map with X connected and G a topological group or a Lie group. For any $e \in X$ lying over the identity element 1_G of G (*i.e.* $\varphi(e) = 1_G$) , there exists a unique group structure on X with e as its identity element and φ is a homomorphism. Moreover,

$$\operatorname{Ker}\varphi \subseteq Z(G),$$

where $Z(G)$ denotes the center of G. Also, X is a Lie group if G is.

(2) Partial converse of (1). Say Y is a connected topological group or a Lie group, if Γ is a discrete subgroup of the center of X, then X/Γ has has a unique topology (or differentiable structure) so that the homomorphism $\varphi\colon X \to X/\Gamma$ is a covering map.

(3) If G is a connected topological group (or a Lie group), write $\widetilde{G}$ for its universal cover. If $Z(G)$ is discrete then

$$\widetilde{G}/Z(\widetilde{G}) \simeq G/Z(G),$$

$\widetilde{G}$ is a topological group (resp. a Lie group), $Z(\widetilde{G})$ is discrete and

(a) $Z(\widetilde{G}/Z(\widetilde{G})) = Z(G/Z(G)) = (1)$

(b) $\pi_1(G, 1)$ is a subgroup of $Z(G)$ and $\pi_1(G/Z(G), 1) = Z(G)$.

Nomenclature (from algebraic geometry).

If $G \longrightarrow H$ is a covering map, with G connected and $Z(G)$ discrete, we say that G is *isogenous* to H. The smallest equivalence so generated yields the *isogeny class* of G.

If X is a smooth manifold of dimension n and if $p \in X$ is any point on X, recall that two curves $\gamma_1\colon (-\epsilon, \epsilon) \to X$ and $\gamma_2\colon (-\epsilon, \epsilon) \to X$ are *equivalent* iff for some chart $\varphi\colon U \to \mathbb{R}^n$ with $p \in U$, we have

$$(\varphi \circ \gamma_1)'(0) = (\varphi \circ \gamma_2)'(0).$$

This equivalence relation does not depend on the choice of the chart (use the transition functions). The set of all equivalence classes of curves through p is the *tangent space*, $T_p(X)$,

to X at p. It is a vector space of dimension n. If G is a Lie group, the tangent space $T_1(G)$ at the identity element plays a special role. The tangent space $T_1(G)$ is also denoted by $\mathfrak{g}$.

Given two normed vector spaces X and Y, for any function $f\colon X \to Y$, for any $x \in X$, we say that f *is differentiable at* x if there is a continuous linear map $L\colon X \to Y$ such that

$$f(x+h) = f(x) + L(h) + o(\|h\|),$$

for all $h \in X$, and where $o(\|h\|)$ is a small vector with respect to h, which means that

$$\lim_{\|h\| \mapsto 0} \frac{o(\|h\|)}{\|h\|} = 0.$$

Observe that we can write

$$\frac{f(x+h) - f(x)}{\|h\|} = L\left(\frac{h}{\|h\|}\right) + \frac{o(\|h\|)}{\|h\|},$$

which shows that as $h \mapsto 0$, the linear map L is uniquely determined on vectors of norm 1, and thus, it is unique. We write

$$L = \mathrm{D}f(x), \quad \text{or} \quad L = \mathrm{D}f_x.$$

If X and Y are finite dimensional with $\dim(X) = q$ and $\dim(Y) = p$, then with respect to bases of X and Y the function f is given by q functions $f_i(x_1, \ldots, x_p)$, and the linear map $Df(x)$ is given by the $p \times q$ *Jacobian matrix*

$$A = J(f)(x) = \left(\frac{\partial f_i}{\partial x_j}(x)\right).$$

Given two smooth manifolds X and Y and a smooth function $f\colon X \to Y$, for any $x \in X$, we define the *tangent map of* f *at* x (or *differential map of* f *at* x), df_x, as the linear map $df_x\colon T_x(X) \to T_{f(x)}Y$ defined as follows: for every tangent vector $v \in T_xX$ given as some equivalence class $[\gamma]$ of curves in X through x, we set

$$df_x(v) = [f \circ \gamma],$$

the equivalence class $[f \circ \gamma]$ of curves in Y through $f(x)$.

In particular, if G and H are Lie groups and if $f\colon G \to H$ is a homomorphism of Lie groups (a group homomorphism which is also a smooth map), then we get a linear map $df_1\colon \mathfrak{g} \to \mathfrak{h}$.

Fact. If G is a connected Lie group and if U is any connected neighbothood of 1_G, then the group generated by U is G (DX). As a corollary, if G and H are Lie groups and G is connected, any homomorphism $f\colon G \to H$ is determined by its restriction to any open neighborhood of 1_G.

Next, we define the adjoint representation of a Lie group. Given a Lie group G, for any $\sigma \in G$, let $\mathfrak{I}_\sigma \colon G \to G$ be the inner automorphism given by

$$\mathfrak{I}_\sigma(\tau) = \sigma\tau\sigma^{-1}, \quad \tau \in G.$$

We get a homomorphism, $\sigma \mapsto \mathfrak{I}_\sigma$, from G to $\mathrm{Aut}(G)$. The derivative of $\mathfrak{I}_\sigma$ at 1_G is a linear map

$$d(\mathfrak{I}_\sigma)_1 \colon \mathfrak{g} \to \mathfrak{g},$$

and since $\mathfrak{I}_\sigma$ is an automorphism, $d(\mathfrak{I}_\sigma)_1 \in \mathrm{Aut}(\mathfrak{g}) = \mathbf{GL}(\mathfrak{g})$. Therefore, we obtain a homomorphism $\sigma \mapsto d(\mathfrak{I}_\sigma)_1$ from G to $\mathbf{GL}(\mathfrak{g})$, namely a representation of G. Is is customary to denote $d(\mathfrak{I}_\sigma)_1$ by Ad_σ, and to denote the above representation called the *adjoint representation* of G by

$$\mathrm{Ad} \colon G \to \mathbf{GL}(\mathfrak{g}),$$

with

$$\mathrm{Ad}(\sigma) = \mathrm{Ad}_\sigma.$$

If $\theta \colon G \to H$ is a Lie group homomorphism, then for all $\sigma, g \in G$, we have

$$\begin{aligned} \mathfrak{I}_{\theta(\sigma)}(\theta(g)) &= \theta(\sigma)\theta(g)\theta(\sigma)^{-1} \\ &= \theta(\sigma g \sigma^{-1}) \\ &= \theta(\mathfrak{I}_\sigma(g)), \end{aligned}$$

so that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\theta} & H \\ {\scriptstyle \mathfrak{I}_\sigma}\downarrow & & \downarrow{\scriptstyle \mathfrak{I}_{\theta(\sigma)}} \\ G & \xrightarrow[\theta]{} & H. \end{array}$$

Taking differentials, we get the commutative diagram

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{d\theta_1} & \mathfrak{h} \\ {\scriptstyle \mathrm{Ad}_\sigma}\downarrow & & \downarrow{\scriptstyle \mathrm{Ad}_{\theta(\sigma)}} \\ \mathfrak{g} & \xrightarrow[d\theta_1]{} & \mathfrak{h}. \end{array}$$

Now, the derivative $d\mathrm{Ad}_1 \colon \mathfrak{g} \to \mathfrak{g}$ of Ad at 1 is a linear map denoted by ad, with

$$\mathrm{ad} \colon \mathfrak{g} \to \mathrm{End}(\mathfrak{g}),$$

and for every $X \in \mathfrak{g}$, the map $\mathrm{ad}(X)$ is an arbitrary endomorphism in $\mathrm{End}(\mathfrak{g})$. By taking derivatives in the diagram above, we get the commutative diagram

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{d\theta_1} & \mathfrak{h} \\ {\scriptstyle \mathrm{ad}(X)}\downarrow & & \downarrow{\scriptstyle \mathrm{ad}(d\theta_1(X)} \\ \mathfrak{g} & \xrightarrow[d\theta_1]{} & \mathfrak{h}, \end{array}$$

which says that

$$d\theta_1(\mathrm{ad}(X)(Y)) = \mathrm{ad}(d\theta_1(X))(d\theta_1(Y)), \quad X, Y \in \mathfrak{g}. \tag{$\dagger$}$$

We write

$$[X, Y] = \mathrm{ad}(X)(Y),$$

and call $[X, Y]$ the *Lie bracket* of X and Y. Then equation ($\dagger$) says that

$$d\theta_1([X, Y]) = [d\theta_1(X), d\theta_1(Y)], \quad X, Y \in \mathfrak{g}. \tag{$\dagger\dagger$}$$

Fundamental Fact. If G and H are Lie groups and if G is connected, then every homomorphism $h\colon G \to H$ is determined by its differential $d\theta_1\colon \mathfrak{g} \to \mathfrak{h}$.

The above implies that the map $\theta \mapsto d\theta_1$ from $\mathrm{Hom}_{\mathrm{Lie}}(G, H)$ to $\mathrm{Hom}_{\mathrm{Vec}}(\mathfrak{g}, \mathfrak{h})$ is injective. Moreover, if G is *simply connected*, then a necessary and sufficient condition for the above map to be surjective is that if $f \in \mathrm{Hom}_{\mathrm{Vec}}(\mathfrak{g}, \mathfrak{h})$, then

$$f([X, Y]) = [f(X), f(Y)], \quad X, Y \in \mathfrak{g}.$$

Remark: We proved the necessity of this condition.

The above considerations motivate the following definition:

Definition 1.12. A *lie algebra* $\mathcal{A}$ (over a field k) is an algebraic structure such that:

(1) $\mathcal{A}$ is vector space (over k).

(2) There is a bilinear map, $[-,-]\colon \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ (the *Lie bracket*), so that

(a) $[X, X] = 0$

(b) (*Jacobi identity*)

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0.$$

Property 2(a) and bilinearity yield the identity

$$[Y, X] = -[X, Y].$$

The tangent space $\mathfrak{g} = T_1 G$ of a Lie group at the identity is a Lie algebra. The Lie algebra of a Lie group G is also denoted by $\mathrm{L}(G)$, or $\mathrm{Lie}(G)$. We will determine explicitly $\mathfrak{g} = \mathrm{Lie}(G)$ and its Lie brackets for several familiar groups G ($\mathbf{GL}(n, \mathbb{R})$, $\mathbf{SL}(n, \mathbb{R})$, $\mathbf{O}(n)$, $\mathbf{SO}(n)$, $\mathbf{U}(n)$, $\mathbf{SU}(n)$).

We begin with $G = \mathbf{GL}(n, \mathbb{R})$. In this case, $T_1(G) = \mathfrak{gl}(n, \mathbb{R}) = \mathrm{M}_n(\mathbb{R})$, the vector space of all $n \times n$ real matrices. Since the inner automorphism $\mathfrak{I}_\sigma$ is given by $\tau \mapsto \sigma\tau\sigma^{-1}$, we see that $\mathrm{Ad}_\sigma = d(\mathfrak{I}_\sigma)_1$ is conjugation by σ:

$$\mathrm{Ad}_\sigma(X) = \sigma X \sigma^{-1}.$$

Let γ be a curve in $\mathbf{GL}(n,\mathbb{R})$ passing through 1_G for $t = 0$ and let $X = \gamma'(0)$. The curve γ is given by an invertible $n \times n$ matrix whose entries are differentiable functions, and $\gamma(0) = I$. We have

$$\begin{aligned}[X,Y] = \mathrm{ad}(X)(Y) &= \frac{d}{dt}\mathrm{Ad}(\gamma(t))\Big|_{t=0}(Y)\\ &= \frac{d}{dt}(\gamma(t)Y\gamma(t)^{-1})\Big|_{t=0}\\ &= \gamma(0)\frac{d}{dt}(Y\gamma(t)^{-1})\Big|_{t=0} + \gamma'(0)Y\gamma^{-1}(0)\\ &= Y\frac{d}{dt}(\gamma(t)^{-1})\Big|_{t=0} + XY.\end{aligned}$$

On the other hand, from $\gamma(t)^{-1}\gamma(t) = I$, we get

$$\frac{d}{dt}(\gamma(t)^{-1})\gamma(t) + \gamma(t)^{-1}\gamma'(t) = 0,$$

which yields

$$\frac{d}{dt}(\gamma(t)^{-1}) = -\gamma(t)^{-1}\gamma'(t)\gamma(t)^{-1}.$$

For $t = 0$, we obtain

$$\frac{d}{dt}(\gamma(t)^{-1})\Big|_{t=0} = -I\gamma'(0)I = -X.$$

Therefore,

$$[X,Y] = Y(-X) + XY = XY - YX,$$

which shows that the Lie bracket in $\mathfrak{gl}(n,\mathbb{R})$ is the commutator operator for matrices. As a consequence, if G is a closed subgroup of $\mathbf{GL}(n,\mathbb{R})$, then $\mathfrak{g}$ is a subspace of $\mathfrak{gl}(n,\mathbb{R})$, and since 2(a) and 2(b) hold for $[-,-]$ in $\mathfrak{gl}(n,\mathbb{R})$, it also holds in $\mathfrak{g}$, which implies that $\mathfrak{g}$ is a Lie algebra.

Given two Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$, a *Lie algebra homomorphism* is a linear map $\varphi\colon \mathfrak{g} \to \mathfrak{h}$ such that

$$[\varphi(X), \varphi(Y)]_{\mathfrak{h}} = \varphi([X,Y]_{\mathfrak{g}}), \quad X, Y \in \mathfrak{g}.$$

If G is a connected and simply connected Lie group, then there is an isomorphism

$$\mathrm{Hom}_{\mathrm{Lie-gr}}(G, \mathbf{GL}(n,\mathbb{C})) \cong \mathrm{Hom}_{\mathrm{Lie-alg}}(\mathfrak{g}, \mathfrak{gl}(n,\mathbb{C})),$$

that is, a bijective correspondence between Lie group representations of G and Lie algebra representations of $\mathfrak{g}$. On the right-hand side, a linear map $\psi\colon \mathfrak{g} \to \mathfrak{gl}(n,\mathbb{C})$ has the property that

$$\psi([X,Y])(v) = X(Y(v)) - Y(X(v)), \quad X, Y \in \mathfrak{g},\ v \in \mathbb{C}^n.$$

Examples of Lie Algebras

(1) $\mathfrak{sl}(n,\mathbb{R})$

Pick any basis $(e_1,\ldots,e_n)$ of $\mathbb{R}^n$, and let $A \in \mathbf{GL}(n,\mathbb{R})$. We have

$$(\bigwedge^n A)(e_1 \wedge \cdots \wedge e_n) = A(e_1) \wedge \cdots \wedge A(e_n) = \det(A)(e_1 \wedge \cdots \wedge e_n). \tag{$\dagger$}$$

Since $A \in \mathbf{SL}(n,\mathbb{R})$ iff $\det(A) = 1$, we have

$$A(e_1) \wedge \cdots \wedge A(e_n) = e_1 \wedge \cdots \wedge e_n.$$

Let A_t be a curve in $\mathbf{SL}(n,\mathbb{R})$ passing through I such that $A_0 = I$ and $A'(0) = X \in \mathfrak{sl}(n,\mathbb{R})$. If we differentiate ($\dagger$) and evaluate at $t = 0$, we get

$$\sum_{j=1}^{n} A(e_1) \wedge \cdots \wedge A(e_{j-1}) \wedge A'(0)(e_j) \wedge A(e_{j+1}) \wedge \cdots \wedge A(e_n) = 0$$

and then

$$\sum_{j=1}^{n} e_1 \wedge \cdots \wedge e_{j-1} \wedge X(e_j) \wedge e_{j+1} \wedge \cdots \wedge e_n = 0.$$

But, $X(e_j)$ is the j-column of the matrix X, so $X(e_j) = \sum_{i=1}^n X_{ij} e_i$, and then

$$\begin{aligned}
0 &= \sum_{j=1}^{n} e_1 \wedge \cdots \wedge e_{j-1} \wedge X(e_j) \wedge e_{j+1} \wedge \cdots \wedge e_n \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} e_1 \wedge \cdots \wedge e_{j-1} \wedge X_{ij} e_i \wedge e_{j+1} \wedge \cdots \wedge e_n \\
&= \left(\sum_{i=1}^{n} X_{ii}\right) e_1 \wedge \cdots \wedge e_n \\
&= \operatorname{tr}(X)(e_1 \wedge \cdots \wedge e_n),
\end{aligned}$$

which implies that

$$\operatorname{tr}(X) = 0.$$

In conclusion,

$$\mathfrak{sl}(n,\mathbb{R}) = \{X \in \mathrm{M}_n(\mathbb{R}) \mid \operatorname{tr}(X) = 0\}.$$

A similar computation shows that

$$\mathfrak{sl}(n,\mathbb{C}) = \{X \in \mathrm{M}_n(\mathbb{C}) \mid \operatorname{tr}(X) = 0\}.$$

(2) Let Q be any symmetric bilinear form which is nondegenerate, and let

$$\mathbf{O}(Q) = \{A \in \mathrm{GL}(n,\mathbb{R}) \mid Q(Au, Av) = Q(u,v),\ u, v \in \mathbb{R}^n\}.$$

In order to find out what $\mathfrak{o}(Q)$ is, we consider a curve A_t in $\mathbf{O}(Q)$ though I so that $A(0) = I$ and $A'(0) = X$. If we differentiate the equation

$$Q(Au, Av) = Q(u, v)$$

and evaluate at $t = 0$, we get

$$Q(A(0)u, Xv) + Q(Xu, A(0)v) = 0,$$

that is,

$$Q(u, Xv) + Q(Xu, v) = 0, \quad u, v \in \mathbb{R}^n.$$

If the quadratic form Q is defined by the invertible symmetric matrix P, so that $Q(u, v) = u^\top Pv$, then the above condition becomes

$$u^\top PXv + u^\top X^\top Pv = 0, \quad u, v \in \mathbb{R}^n,$$

which implies that

$$PX + X^\top P = 0.$$

Therefore,

$$\mathfrak{o}(Q) = \{X \in \mathrm{M}_n(\mathbb{R}) \mid PX + X^\top P = 0\}.$$

In particular, if Q is the standard Euclidean inner product, for which $P = I$, we get

$$\mathfrak{o}(n, \mathbb{R}) = \{X \in \mathrm{M}_n(\mathbb{R}) \mid X^\top = -X\},$$

the space of skew-symmetric matrices. For real matrices, $X^\top = -X$ implies that $\mathrm{tr}(X) = 0$, so

$$\mathfrak{so}(n, \mathbb{R}) = \mathfrak{o}(n, \mathbb{R}) = \{X \in \mathrm{M}_n(\mathbb{R}) \mid X^\top = -X\}.$$

(3) Let Q be any skew symmetric nondegenerate bilinear form on $\mathbb{R}^{2m}$ and consider

$$\mathbf{Sp}(Q) = \{A \in \mathbf{GL}(2m, \mathbb{R}) \mid Q(Au, Av) = A(u, v),\ u, v \in \mathbb{R}^{2m}\}.$$

If Q is given by a skew symmetric matrix P, so that $Q(u, v) = u^\top Pv$, then by taking the derivative of

$$Q(Au, Av) = Q(u, v)$$

as in case (2), we get the same condition

$$X^\top P + PX = 0,$$

and

$$\mathfrak{sp}(Q) = \{X \in \mathrm{M}_{2m}(\mathbb{R}) \mid PX + X^\top P = 0\}.$$

(4) Let Q be a Hermitian form on $\mathbb{C}^n$. Then

$$\mathbf{U}(Q) = \{A \in \mathrm{GL}(n, \mathbb{C}) \mid Q(Au, Av) = Q(u, v),\ u, v \in \mathbb{C}^n\}.$$

If Q is given by the Hermitian matrix P, then

$$Q(u,v) = v^*Pu = \overline{u^*Pv} = \overline{Q(v,u)}.$$

As before, the derivative of the condition $Q(Au,Av) = Q(u,v)$ yields

$$Q(u,Xv) + Q(Xu,v) = 0, \quad u,v \in \mathbb{C}^n.$$

In terms of the matrix P, this is

$$v^*X^*Pu + v^*PXu = 0,$$

which yields

$$X^*P + PX = 0.$$

Therefore,

$$\mathfrak{u}(Q) = \{X \in \mathrm{M}_n(\mathbb{C}) \mid PX + X^*P = 0\}.$$

In the standard case, $P = I$, so

$$\mathfrak{u}(n) = \{X \in \mathrm{M}_n(\mathbb{C}) \mid X^* = -X\}.$$

Since $\mathbf{SU}(n) = \mathbf{U}(n) \cap \mathbf{SL}(n,\mathbb{C})$, we have

$$\mathfrak{u}(n) = \{X \in \mathrm{M}_n(\mathbb{C}) \mid X^* = -X,\ \mathrm{tr}(X) = 0\}.$$

Unlike the real case, we have $\mathfrak{su}(n) \neq \mathfrak{u}(n)$.

Our next goal is to show that given a Lie group G, there is a map $\exp\colon \mathfrak{g} \to G$ defined on the Lie algebra $\mathfrak{g}$ of G, and which is locally a diffeomorphism. For this, we need to consider left-invariant vector fields.

Given any element $\sigma \in G$, let $L_\sigma\colon G \to G$ denote left multiplication by σ, that is,

$$L_\sigma(\tau) = \sigma\tau.$$

Each L_σ is a diffeomorphism, so the derivative $d(L_\sigma)_1\colon \mathfrak{g} \to \mathfrak{g}$ is a linear isomorphism. A vector field X on G is *left-invariant* iff

$$d(L_\sigma)_\tau(X(\tau)) = X(L_\sigma(\tau)) = X(\sigma\tau), \quad \text{for all } \sigma,\tau \in G.$$

By setting $\tau = 1$, we see that a left-invariant vector field X is completely determined by the tangent vector $X(1) \in \mathfrak{g}$, since

$$X(\sigma) = d(L_\sigma)_1(X(1)).$$

Conversely, given any vector $v \in \mathfrak{g}$, we can define the vector field X_v by

$$X_v(\sigma) = d(L_\sigma)_1(v), \quad \sigma \in G.$$

It is easy to check that X_v is left-invariant, so the map $X \mapsto X(1)$ is a bijection between the Lie algebra of left-invariant vector fields (under the Lie bracket on vector fields) and the Lie algebra $\mathfrak{g}$ (DX).

Given any left-invariant vector field X on G, for any $g \in G$, by the fundamental theorem existence for ODE's, there is some integral curve $\gamma_g \colon (-\epsilon, \epsilon) \to G$ such that $\gamma_g(0) = g$ and

$$\gamma'(t) = X(\gamma_g(t)), \quad t \in (-\epsilon, \epsilon).$$

For every $g \in G$, there is a unique maximal integral curve Γ_g such that $\Gamma_g(0) = g$, whose domain is denoted $I(g)$. Then, if we let

$$\mathcal{D}(X) = \{(t, g) \in \mathbb{R} \times G \mid t \in I(g)\},$$

the function $\Phi \colon \mathcal{D}(X) \to G$ given by

$$\Phi(t, g) = \Gamma_g(t)$$

is called the *flow* of X. We often write $\Phi_t(g)$ instead of $\Phi(t, g)$.

One of the main properties of the flow of a left-invariant vector field on a Lie group is that it is complete, which means that

$$\mathcal{D}(X) = \mathbb{R} \times G,$$

that is, every integral curve Γ_g is defined for all $t \in \mathbb{R}$.

We have the following proposition:

Proposition 1.33. *Given a Lie group G and a left-invariant vector field X, if Φ is the flow of X, then*

$$\Phi_t(g) = g\Phi_t(1), \quad \textit{for all } (t, g) \in \mathcal{D}(X).$$

Proof. Define the curve γ by

$$\gamma(t) = g\Phi_t(1) = L_g(\Phi_t(1)).$$

We have $\gamma(0) = g$, and using the chain rule

$$\gamma'(t) = d(L_g)_{\Phi_t(1)}(\Phi_t'(1)) = d(L_g)_{\Phi_t(1)}(X(\Phi_t(1))) = X(L_g(\Phi_t(1))) = X(\gamma(t)).$$

By the uniqueness of maximal integral curves, $\gamma(t) = \Phi_t(g)$ for all t, and so

$$\Phi_t(g) = g\Phi_t(1).$$

□

Using Proposition 1.33, we can prove the following crucial result:

Proposition 1.34. *Given a Lie group G, for every $v \in \mathfrak{g}$, there is a unique smooth homomorphism $h_v \colon (\mathbb{R}, +) \to G$ such that $h_v'(0) = v$. Furthermore, $h_v(t)$ is the maximal integral curve of the left-invariant vector field X_v, and it is defined for all $t \in \mathbb{R}$.*

Proof. Let $\Phi_t(g)$ denote the flow of X_v. By a familiar property of the flow,

$$\Phi_{s+t}(1) = \Phi_s(\Phi_t(1)),$$

whenever both sides are defined. By Proposition 1.33, we have

$$\Phi_{s+t}(1) = \Phi_s(\Phi_t(1)) = \Phi_t(1)\Phi_s(1).$$

It follows that if $\Phi_t(1)$ is defined on $(-\epsilon, \epsilon)$, with $s = t$, we see that $\Phi_t(1)$ is actually defined on $(-2\epsilon, 2\epsilon)$. By induction, $\Phi_t(1)$ is defined on $(-2^n\epsilon, 2^n\epsilon)$ for all $n \geq 1$, so the map $t \mapsto \Phi_t(1)$ is defined for all $t \in \mathbb{R}$. Let h_v be the homomorphism given by

$$h_v(t) = \Phi_t(1),$$

then, $h_v'(0) = v$. To show that h_v is smooth, consider the map from $\mathbb{R} \times G \times \mathfrak{g}$ to $G \times \mathfrak{g}$ given by

$$(t, g, v) \mapsto (g\Phi_t(1), v).$$

It is easy to see that this map is the flow of the vector field

$$(g, v) \mapsto (v(g), 0).$$

and thus, it is smooth.

Next, assume that $h \colon \mathbb{R} \to G$ is a smooth homomorphism with $h'(0) = v$. From

$$h(s + t) = h(t)h(s),$$

by differentiating at $s = 0$, we get

$$h'(t) = d(L_{h(t)})_1(v) = X_v(g(t)).$$

Therefore, $h(t)$ is an integral curve for X_v with initial condition $h(0) = 1$, so by uniqueness $h(t) = \Phi_t(1)$. □

Definition 1.13. Given a Lie group G, the *exponential map* $\exp \colon \mathfrak{g} \to G$ is given by

$$\exp(v) = h_v(1) = \Phi_1(1), \quad \text{for all } v \in \mathfrak{g}.$$

The map exp is smooth because it is the restriction of the flow of the vector field

$$(g, v) \mapsto (v(g), 0)$$

to $\{1\} \times \{1\} \times \mathfrak{g}$. Obviously,

$$\exp(0) = 1_G.$$

For any fixed t, the map $s \mapsto h_v(st)$ is a smooth homomorphism h such that $h'(0) = tv$. By uniquenes,

$$h_v(st) = h_{tv}(s).$$

If we set $s = 1$, we find that

$$h_v(t) = \exp(tv), \quad \text{for all } v \in \mathfrak{g},\ t \in \mathbb{R}.$$

The homomorphism $t \mapsto \exp(tv)$ is called a *one-parameter group*. Differentiating with respect to t at $t = 0$, we get

$$v = d\exp_0(v),$$

that is,

$$d\exp_0 = \mathrm{id}_{\mathfrak{g}}.$$

By the inverse function theorem, exp is a local diffeomorphism at 0.

The exponential map is also natural in the following sense:

Proposition 1.35. *Given any two Lie groups, G and H, for every Lie group homomorphism, $f\colon G \to H$, the following diagram commutes:*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle \exp}\uparrow & & \uparrow{\scriptstyle \exp} \\ \mathfrak{g} & \xrightarrow[df_1]{} & \mathfrak{h} \end{array}$$

Proof. Observe that the map $h\colon t \mapsto f(\exp(tv))$ is a homomorphism from $(\mathbb{R}, +)$ to G such that $h'(0) = df_1(v)$. Proposition 1.34 shows that $f(\exp(v)) = \exp(df_1(v))$. □

A useful corollary of Proposition 1.35 is:

Proposition 1.36. *Let G be a connected Lie group and H be any Lie group. For any two homomorphisms, $\varphi_1\colon G \to H$ and $\varphi_2\colon G \to H$, if $d(\varphi_1)_1 = d(\varphi_2)_1$, then $\varphi_1 = \varphi_2$.*

Let us find out what the exponential map is in $\mathbf{GL}(n, \mathbb{C})$. For any $n \times n$ complex matrix A, let

$$e^A = I + \sum_{k=1}^{\infty} \frac{A^k}{k!}.$$

For any operator norm $\|\ \|$ on $n \times n$ matrices, $\|I\| = 1$ and $\left\|A^k\right\| \leq \|A\|^k$, so

$$\|I\| + \sum_{k=1}^{n} \left\| \frac{A^k}{k!} \right\| \leq e^{\|A\|},$$

which proves that the series $\sum_{k=0}^{\infty} \left\| \frac{A^k}{k!} \right\|$ converges, and thus the series $\sum_{k=0}^{\infty} \frac{A^k}{k!}$ is absolutely convergent. In fact, it converges uniformly in any compact subset of $\mathrm{M}_n(\mathbb{C})$. It is not hard to show that if $AB = BA$, then

$$e^{A+B} = e^A e^B,$$

and so

$$e^{(\lambda+\mu)A} = e^{\lambda A} e^{\mu A}, \quad \text{for all } \lambda, \mu \in \mathbb{C}.$$

Therefore, the map $h_A \colon t \mapsto e^{tA}$ is a smooth homomorphism from $\mathbb{R}$ to $\mathbf{GL}(n, \mathbb{C})$. It is also easy to see that

$$h'_A(0) = A.$$

It follows from Proposition 1.34 that h_A is the maximal integral curve through I such that $h'_A(0) = A$, which implies that

$$\exp(A) = e^A.$$

If $\|I - X\| < 1$, the series

$$\log(X) = (X - I) - \frac{(X-I)^2}{2} + \cdots + (-1)^{n-1} \frac{(X-I)^n}{n} + \cdots$$

is convergent, and we can check that

$$\exp(\log(X)) = X$$
$$\log(\exp(X)) = X,$$

with $\|I - X\| < 1$ in the first equation, and $\|X\|$ small enough in the second equation.

Caution. In general

$$e^{X+Y} \neq e^X e^Y,$$

unless $XY = YX$. Therefore, it is natural to ask if there is an expression $\mu(X, Y)$ (also denoted $X * Y$) of X and Y such that

$$e^{\mu(X,Y)} = e^X e^Y.$$

It turns out that there is such a formula known as the *Campbell–Baker–Hausdorff–Dynkin formula*. It turns out that for X and Y in a small enough neighborhood of 0,

$$\mu(X, Y) = \log(\exp(X) \exp(Y))$$

sagtisfies the equation

$$e^{\mu(X,Y)} = e^X e^Y.$$

A Taylor expansion of $\mu(X, Y)$ was obtained by Dynkin (1947). Here is a version due to Serre.

Theorem 1.37. *(Dynkin's Formula) If we write* $\mu(X,Y) = \sum_{n=1}^{\infty} z_n(X,Y)$*, then we have*

$$z_n(X,Y) = \frac{1}{n}\sum_{p+q=n}(z'_{p,q}(X,Y) + z''_{p,q}(X,Y)),$$

with

$$z'_{p,q}(X,Y) = \sum_{\substack{p_1+\cdots+p_m=p\\ q_1+\cdots+q_{m-1}=q-1\\ p_i+q_i\geq 1,\, p_m\geq 1,\, m\geq 1}} \frac{(-1)^{m+1}}{m}\left(\left(\prod_{i=1}^{m-1}\frac{(\operatorname{ad}X)^{p_i}}{p_i!}\frac{(\operatorname{ad}Y)^{q_i}}{q_i!}\right)\frac{(\operatorname{ad}X)^{p_m}}{p_m!}\right)(Y)$$

and

$$z''_{p,q}(X,Y) = \sum_{\substack{p_1+\cdots+p_{m-1}=p-1\\ q_1+\cdots+q_{m-1}=q\\ p_i+q_i\geq 1,\, m\geq 1}} \frac{(-1)^{m+1}}{m}\left(\prod_{i=1}^{m-1}\frac{(\operatorname{ad}X)^{p_i}}{p_i!}\frac{(\operatorname{ad}Y)^{q_i}}{q_i!}\right)(X).$$

As a concrete illustration of Dynkin's formula, after some labor, the following Taylor expansion up to order 4 is obtained:

$$\begin{aligned}\mu(X,Y) &= X+Y+\frac{1}{2}[X,Y]+\frac{1}{12}[X,[X,Y]]+\frac{1}{12}[Y,[Y,X]]-\frac{1}{24}[X,[Y,[X,Y]]]\\ &\quad + \text{higher order terms.}\end{aligned}$$

Observe that due the lack of associativity of the Lie bracket quite different looking expressions can be obtained using the Jacobi identity. For example,

$$-[X,[Y,[X,Y]]] = [Y,[X,[Y,X]]].$$

(1) The CBHD formula shows that multiplication in the group G is already determined by addition in $\mathfrak{g}$. For connected groups, homomorphisms of G are also determined by homomrphisms of $\mathfrak{g}$, and for simply-connected groups, representations of G are determined by representations of $\mathfrak{g}$.

(2) The CBHD formula also shows that if $\mathfrak{h}$ is a subalgebra of the Lie algebra $\mathfrak{g} = T_1(G)$ of a Lie group G, then $\exp(\mathfrak{h})$ is an immersed subgroup of G. Recall that an *immersion* $\varphi\colon H \to G$ is an injective homomorphism such that $d\varphi_\sigma$ is injective for all $\sigma \in H$, yet not an embedding. An *embedding* is an immersion which is also a homeomorphism onto $\varphi(H)$, with the manifold structure on $\varphi(H)$ induced from G. An example of an immersion which is not an embedding is the following map $\varphi\colon \mathbb{R} \to S^1$ from $\mathbb{R}$ to the unit circle given by

$$\varphi(t) = e^{i2\arctan(t)}.$$

The problem is that the inverse image of a small open connected neighborhood of $e^{i\pi}$ consists of two disjoint open subsets of $\mathbb{R}$.

Also observe that multiplication in $\exp(\mathfrak{h})$ is given by $\exp(x * y)$, with $x, y \in \mathfrak{h}$.

(3) Every Lie algegra is the Lie algebra of some Lie group. Indeed, by Ado's Theorem, a Lie algebra can be embedded in $\mathfrak{gl}(n,\mathbb{C})$, so $\exp(\mathfrak{g})$ is an immersed subgroup in $\mathbf{GL}(n,\mathbb{C})$.

1.7 Some Lie Algebra Representations

There are useful analogies between various notions for groups and for Lie algebras, some of which are listed below.

Groups	Lie Algebras
Subgroup H of G	Subalgebra $\mathfrak{h}$ of $\mathfrak{g}$: a linear subspace $\mathfrak{h}$ of $\mathfrak{g}$ closed under the Lie bracket
Normal subgroup H of G Notation: $H \lhd G$	Ideal $\mathfrak{h}$ of $\mathfrak{g}$: for all $X \in \mathfrak{h}$, all $Y \in \mathfrak{g}$, $[X, Y] \in \mathfrak{h}$ Notation: $\mathfrak{h} \lhd \mathfrak{g}$
Commutator subgroup $[G, G] \lhd G$ Derived series $D^1 = [G, G]$; $D^{k+1}G = [D^kG, D^kG]$ $G \supseteq D^1G \supseteq D^2G \supseteq \cdots$ $D^kG/D^{k+1}G$ is abelian G is solvable iff $D^nG = (1)$, for some n	Commutator ideal $[\mathfrak{g}, \mathfrak{g}] \lhd \mathfrak{g}$ Derived series $D^1\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$; $D^{k+1}\mathfrak{g} = [D^k\mathfrak{g}, D^k\mathfrak{g}]$ $\mathfrak{g} \supseteq D^1\mathfrak{g} \supseteq D^2\mathfrak{g} \supseteq \cdots$ $D^k\mathfrak{g}/D^{k+1}\mathfrak{g}$ is abelian $\mathfrak{g}$ is solvable iff $D^n\mathfrak{g} = (0)$, for some n
Lower central series $\Gamma_1 G = [G, G] = D^1G$; $\Gamma_{k+1}G = [G, \Gamma_k G] \supseteq D^{k+1}G$ G is nilpotent iff $\Gamma_n G = (1)$, for some n	Lower central series $\Gamma_1\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}] = D^1\mathfrak{g}$; $\Gamma_{k+1}\mathfrak{g} = [\mathfrak{g}, \Gamma_k\mathfrak{g}] \supseteq D^{k+1}\mathfrak{g}$ $\mathfrak{g}$ is nilpotent iff $\Gamma_n\mathfrak{g} = (0)$, for some n

Note that nilpotent implies solvable.

Theorem 1.38. *(Engel's Theorem) If $\mathfrak{g}$ is Lie subalgebra of $\mathfrak{gl}(n, \mathbb{R})$ (or $\mathfrak{gl}(n, \mathbb{C})$) and if every $X \in \mathfrak{g}$ is nilpotent, then $\mathfrak{g}$ is nilpotent, and there is a common eigenvector for all $X \in \mathfrak{g}$; that is, there is some $v \neq 0$ such that $X(v) = 0$ for all $X \in \mathfrak{g}$.*

Recall that a *representation* ρ of a Lie algebra $\mathfrak{g}$ is a Lie algebra homomorphism $\rho\colon \mathfrak{g} \to \mathrm{End}(V)$, where V is some finite-dimensional vector space over $\mathbb{C}$; so, ρ is linear, and

$$\rho([X, Y]) = \rho(X)\rho(Y) - \rho(Y)\rho(X), \quad \text{for all } X, Y \in \mathfrak{g}.$$

Theorem 1.39. *(Lie's Theorem) If $\mathfrak{g}$ is solvable Lie algebra and if $\rho\colon \mathfrak{g} \to \mathrm{End}(V)$ is a finite-dimensional representation of $\mathfrak{g}$, then there exists a common eigenvector v of all $\rho(X)$, where $X \in \mathfrak{g}$.*

Consider a representation $\rho\colon \mathfrak{g} \to \mathrm{End}(V)$ of a complex solvable Lie algebra $\mathfrak{g}$. By Lie's Theorem, there is a vector $v_1 \neq 0$ which is a common eigenvector of all $\rho(X)$, with $X \in \mathfrak{g}$.

The subspace $U = \mathrm{Span}(v_1)$ is invariant under ρ, so we can define a representation $\overline{\rho}$ of $\mathfrak{g}$ on $W = V/U$ as follows:

$$\overline{\rho}(X)(\overline{v}) = \overline{\rho(X)(v)} = \rho(v) \mod U, \quad \text{for all } v \in V.$$

Since $\dim(V/U) = \dim(V) - 1$, by induction we can find a sequence of subspaces (a flag)

$$V/U = W_0 \supseteq W_1 \supseteq \cdots \supseteq W_{n-1} = (0),$$

with W_i invariant under $\overline{\rho}$ (which means that $\overline{\rho}(X)(W_i) \subseteq W_i$), and $\dim(W_i) = n - 1 - i$. If $\pi\colon V \to V/U$ is the quotient map (which commutes with all $\rho(X)$), set $V_i = \pi^{-1}(W_i)$ and $V_n = (0)$. Then, we obtain a flag

$$V = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_n = (0),$$

with V_i invariant under ρ and $\dim(V_i) = n - i$, and if we choose a basis from this flag, the matrices representing the $\rho(X)$ (with $X \in \mathfrak{g}$) are all upper triangular.

There is also a version of Engel's Theorem for nilpotent Lie algebra.

Theorem 1.40. *(Engel's Theorem (2)) Say $\mathfrak{g}$ is a Lie algebra and $\rho\colon \mathfrak{g} \to \mathrm{End}(V)$ is a finite-dimensional representation of $\mathfrak{g}$. If $\rho(X)$ is nilpotent for all $X \in \mathfrak{g}$, then $\mathfrak{g}$ is nilpotent, and there is a vector $v \neq 0$ in V such that $\rho(X)(v) = 0$, for all $X \in \mathfrak{g}$.*

If $\mathfrak{g}$ is a nilpotent Lie algebra, then by Engel's Theorem, it is easy to show by induction that there is a flag

$$V = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_n = (0),$$

such that $\rho(X)(V_i) \subseteq V_{i+1}$ and $\dim(V_i) = n - i$. As a consequence, there is a basis in which the matrices $\rho(X)$ are strictly upper-triangular for all $X \in \mathfrak{g}$ (they are upper triangular and they have zero diagonal elements).

Theorem 1.41. *(Ado's Theorem) Every real or complex Lie algebra $\mathfrak{g}$ embeds as a subalgebra of $\mathfrak{gl}(n, \mathbb{C}) = \mathrm{M}_n(\mathbb{C})$. When $\mathfrak{g}$ is a complex Lie algebra, the embedding can be taken as complex linear.*

Say ρ is an irrep of a solvable Lie algebra $\mathfrak{g}$ (over $\mathbb{C}$). Lie's Theorem implies that there is an eigenvector v such that

$$X(v) = \lambda(v)v, \quad \text{for all } X \in \mathfrak{g},$$

for some $\lambda(v) \in \mathbb{C}$. As a consequence, the subspace $U = \mathrm{Span}(v)$ is invariant under ρ, and it defines a subrepresentation of ρ. As ρ is an irrep, by Schur's Lemma, ρ is one-dimensional.

Corollary 1.42. *Every irrep of a solvable Lie algebra (over $\mathbb{C}$) is one-dimensional.*

Remarks:

(1) If
$$0 \longrightarrow \mathfrak{h} \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}/\mathfrak{h} \longrightarrow 0$$
is an exact sequence with $\mathfrak{h}$ an ideal of $\mathfrak{g}$, then $\mathfrak{g}$ is solvable iff $\mathfrak{h}$ and $\mathfrak{g}/\mathfrak{h}$ are solvable.

(2) If $\mathfrak{h}$ and $\mathfrak{h}'$ are ideals in $\mathfrak{g}$ and both $\mathfrak{h}$ and $\mathfrak{h}'$ are solvable, then $\mathfrak{h} + \mathfrak{h}' \lhd \mathfrak{g}$ is solvable. Therefore, there exists a unique maximal ideal in $\mathfrak{g}$ (the sum of all solvable ideals) called the *radical* of $\mathfrak{g}$ and denoted by $\mathrm{rad}(\mathfrak{g})$.

Definition 1.14. A Lie algebra $\mathfrak{g}$ is *semi-simple* if $\mathrm{rad}(\mathfrak{g}) = (0)$. This is equivalent to the property that $\mathfrak{g}$ has no nonzero abelian ideal.

The quotient $\mathfrak{g}/\mathrm{rad}(\mathfrak{g}) = \mathfrak{g}_{\mathrm{ss}}$ is the *semi-simple* part of $\mathfrak{g}$. We have the exact sequence
$$0 \longrightarrow \mathrm{rad}(\mathfrak{g}) \longrightarrow \mathfrak{g} \xrightarrow{\pi} \mathfrak{g}_{\mathrm{ss}} \longrightarrow 0. \qquad (\dagger)$$

Theorem 1.43. *(Levi's Theorem) The exact sequence* (†) *splits. This means that there is some semi-simple Lie subalgebra* $\widetilde{\mathfrak{g}}$ *of* $\mathfrak{g}$ *(there are many) and an isomorphism* $\epsilon\colon \mathfrak{g}_{\mathrm{ss}} \to \widetilde{\mathfrak{g}}$ *such that*
$$\pi \circ \epsilon = \mathrm{id}.$$

Elementary Remarks

(1) If
$$0 \longrightarrow \mathfrak{h} \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}/\mathfrak{h} \longrightarrow 0$$
is an exact sequence, then $\mathfrak{g}$ is semi-simple iff each of $\mathfrak{h}$ and $\mathfrak{g}/\mathfrak{h}$ are semi-simple.

(2) Noncompactness of a Lie group may result in a bad behavior of its representations. For example, if $G = \mathbb{C}$, then

(a) In the representation
$$z \mapsto \begin{pmatrix} 0 & z \\ 0 & 0 \end{pmatrix}$$
every element is nilpotent, but

(b) in the representation
$$z \mapsto \begin{pmatrix} z & z \\ 0 & 0 \end{pmatrix}$$
the matrices are neither diagonalizable nor nilpotent.

Fundamental Fact.

Say $\mathfrak{g}$ is a complex semi-simple Lie algebra.

(1) If $\rho\colon \mathfrak{g} \to \mathrm{End}(V)$ is a representation of $\mathfrak{g}$, for every subspace W of V associated with a subrepresentation of ρ, there is some subspace Z of V which is invariant under ρ such that

$$V = W \coprod Z.$$

We say that all representations of $\mathfrak{g}$ are *completely reducible*.

(2) Recall that the *Jordan decomposition* of a matrix A is

$$A = A_\Delta + A_n,$$

whre A_Δ is a diagonalizable matrix and A_n is a nilpotent matrix, with

$$A_\Delta A_n = A_n A_\Delta,$$

and both A_Δ and A_n are polynomials in A. In general, for an arbitrary Lie algebra, the Jordan decomposition is not preserved by a representation. However, the following result holds in the semi-simple case.

Proposition 1.44. *Let $\mathfrak{g}$ be a semi-simple Lie algebra. For any $X \in \mathfrak{g}$, there exist $X_\Delta, X_n \in \mathfrak{g}$ so that if ρ is any representation of $\mathfrak{g}$, then*

$$\rho(X_\Delta) = \rho(X)_\Delta$$
$$\rho(X_n) = \rho(X)_n.$$

In particular, if ρ is injective and if we view $\mathfrak{g}$ as a subalgebra of $\mathfrak{gl}(V)$, then the diagonalizable and nilpotents parts of any element X of $\mathfrak{g}$ are again in $\mathfrak{g}$ and are independent of ρ.

(3) From Levi's Theorem, the following facts hold:

(a) The representation space of every irreducible representation ρ of a Lie algebra $\mathfrak{g}$ is of the form $C \otimes L$, where the restriction of ρ to V is an irrep of $\mathfrak{g}_{\mathrm{ss}}$ and the restriction of ρ to L is a one-dimensional representation.

(b) From the elementary remark and Levi's Theorem, every semi-simple Lie algebra $\mathfrak{g}$ is a coproduct

$$\mathfrak{g} = \coprod_\alpha \mathfrak{g}_\alpha,$$

where each $\mathfrak{g}_\alpha$ is a simple Lie algebra (this means that $\mathfrak{g}_\alpha$ is nonabelian and has only the trivial ideals (0) and $\mathfrak{g}$).

Theorem 1.45. *(Elie Cartan, Killing, 1898) Every simple Lie algebra (over $\mathbb{C}$) belongs to one of four infinite families A_n, B_n, C_n, D_n, or to five "exceptional" Lie algebra:*

(1) For $n \geq 1$, $A_n = \mathfrak{sl}(n+1, \mathbb{C})$, the Lie algebra of $\mathbf{SL}(n+1, \mathbb{C})$.

(2) For $n \geq 2$, $B_n = \mathfrak{so}(2n+1, \mathbb{C})$, with

$$\mathfrak{so}(2n+1, \mathbb{C}) = \{X \in \mathfrak{gl}(2n+1, \mathbb{C}) \mid X^\top = -X\},$$

the Lie algebra of $\mathbf{SO}(2n+1, \mathbb{C})$.

(3) For $n \geq 3$, $C_n = \mathfrak{sp}(2n)$, with

$$\mathfrak{sp}(2n) = \{X \in \mathfrak{gl}(2n, \mathbb{C}) \mid X^\top J + JX = 0\},$$

with

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

the Lie algebra of $\mathbf{Sp}(2n)$.

(4) For $n \geq 4$, $D_n = \mathfrak{so}(2n, \mathbb{C})$, with

$$\mathfrak{so}(2n, \mathbb{C}) = \{X \in \mathfrak{gl}(2n, \mathbb{C}) \mid X^\top = -X\},$$

the Lie algebra of $\mathbf{SO}(2n, \mathbb{C})$.

(5) The five exceptional Lie algebra G_2, F_4, E_6, E_7, and E_8, whose dimensions are respectively, $14, 52, 78, 133$, *and* 248.

Remark: The somewhat peculiar indexing of the families A_n, B_n, C_n, D_n is motivated by the fact that for small n, there are repetitions in these series. For instance, $A_1 \cong B_1 \cong C_1$, $B_2 \cong C_2$, and $A_3 \cong D_3$.

Representation of Some Low-Dimensional Simple Lie Algebras

(A) $\mathfrak{sl}(2, \mathbb{C})$. These are the complex 2×2 matrices

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a + d = 0.$$

A basis of $\mathfrak{sl}(2, \mathbb{C})$ consists of the three matrices

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

We easily check that

$$\begin{aligned} [H, X] &= 2X \\ [H, Y] &= -2Y \\ [X, Y] &= H. \end{aligned}$$

The crucial idea is to examine the eigenspaces of H on V. Let V_λ be the eigenspace where $H(v) = \lambda v$. If v is an eigenvector of H, then $X(v) \in V_{\lambda+2}$ and $Y(v) \in V_{\lambda-2}$. Indeed,

$$H(X(v)) = [H, X](v) + XH(v) = 2X(v) + \lambda X(v) = (\lambda + 2)X(v),$$

and similarly for $Y(v)$. We get

$$HX^r(v) = (\lambda + 2r)X^r(v) \quad \text{and} \quad HY^r(v) = (\lambda - 2r)Y^r(v).$$

But, V is finite-dimensional, so both X and Y are nilpotent on the eigenvectors of H in V.

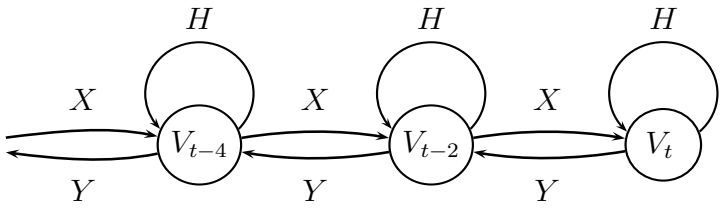


Figure 1.4: Action of X, Y, H on a representation space V

Definition 1.15. (Lefschetz) An element, v, of the finite-dimensional representation space, V, for $\mathfrak{sl}(2, \mathbb{C})$ is *primitive* iff it is an eigenvector for H and $X(v) = 0$.

As V is a finite-dimensional $\mathbb{C}$-space, a primitive element must exist. Indeed, H has at least some eigenvalue, λ, and if $v \in V_\lambda$, then $X^r(v) \in V_{\lambda+2r}$, for all r. Since $V_{\lambda+2r} \cap V_{\lambda+2s} = (0)$, for $r \neq s$ and V is finite-dimensional, there is a smallest r so that $X^r(v) \neq 0$ and $X^{r+1}(v) = 0$. The vector $X^r(v)$ is a primitive element.

Proposition 1.46. *Let V be a finite-dimensional irreducible representation space for $\mathfrak{sl}(2, \mathbb{C})$ and pick any primitive vector, v, in V. Then, the vectors*

$$v, Y(v), Y^2(v), \ldots, Y^t(v),$$

where $Y^{t+1}(v) = 0$, form a basis for V. Hence,

(1) $\dim_{\mathbb{C}} V = t + 1 =$ *index of nilpotence of Y on V.*

(2) Any two primitive v's give the same index of nilpotence.

Proof. Consider

$$W = \operatorname{span}(v, Y(v), Y^2(v), \ldots, Y^t(v)).$$

If we show that H, X, Y take W to itself, irreducibility of V implies $W = V$. Clearly, $Y(W) \subseteq W$. As

$$HY^r(v) = (\lambda - 2r)Y^r(v), \quad \text{if} \quad H(v) = \lambda v,$$

we also have $H(W) \subseteq W$. For X, we prove by induction on l that $XY^l(v) \in W$. When $l = 0$, we get $X(v) = 0$, and the claim holds trivially. Assume the claim holds for $l - 1$. We have

$$\begin{aligned} XY^l(v) &= XY\,Y^{l-1}(v) \\ &= (H + YX)(Y^{l-1}(v)) \\ &= (\lambda - 2(l-1))Y^{l-1}(v) + Y(XY^{l-1}(v)), \end{aligned}$$

and $XY^{l-1}(v) \in W$, by the induction hypothesis. So, both terms on the right hand side are in W and the induction step is done. Now, $v, Y(v), Y^2(v), \ldots, Y^t(v)$ are eigenvectors with distinct eigenvalues, so they must be linearly independent. Therefore, they form a basis of V. The rest is obvious. □

Call an eigenspace for H on any (finite-dimensional) representation space a *weight space* and the *weight* is just the eigenvalue. We get

Corollary 1.47. *Every irreducible finite-dimensional representation, V, of $\mathfrak{sl}(2, \mathbb{C})$ is a finite coproduct of one-dimensional weight spaces, V_λ,*

$$V = \coprod_\lambda V_\lambda.$$

The "highest weight space" consists of 0 *and all the primitive vectors (each a multiple of the other).*

Proposition 1.48. *Say V is a finite-dimensional $\mathfrak{sl}(2, \mathbb{C})$-module, then every eigenvalue of V is an integer. If V is irreducible, these are*

$$-t, -t + 2, \ldots, t - 2, t,$$

where $\dim_{\mathbb{C}} V = t + 1 =$ index of nilpotence of Y on V. Therefore, the irreducible $\mathfrak{sl}(2, \mathbb{C})$-modules are in one-to-one correspondence with the non-negative integers, t, via

$$t \mapsto V(t) = \coprod_{0 \le 2j \le t} V_{-t+2j} \amalg \coprod_{0 \le 2j \le t} V_{t-2j}$$

with $\dim_{\mathbb{C}} V = t + 1$.

Proof. As V is finite-dimensional, there is a primitive element, v, and let λ be its weight (eigenvalue). Look at $XY^l(v)$. I claim:

$$XY^l(v) = (l\lambda - l(l-1))Y^{l-1}(v).$$

This is shown by induction on l. For $l = 0$, this is trivial ($0 = 0$). Assume the claim hols for l. We have

$$\begin{aligned} XY^{l+1}(v) &= XY(Y^l(v)) \\ &= H(Y^l(v)) + YX(Y^l(v)) \\ &= (\lambda - 2l)Y^l(v) + Y(l\lambda - l(l-1))Y^{l-1}(v) \\ &= (\lambda - 2l + l\lambda - l^2 + l)Y^l(v) \\ &= ((l+1)\lambda - (l+1)l)Y^l(v), \end{aligned}$$

proving the induction hypothesis. Now, we know that there is some $t \geq 0$ so that $Y^t(v) \neq 0$ and $Y^{t+1}(v) = 0$, so let $l = t + 1$. We get

$$0 = XY^{t+1}(v) = ((t+1)\lambda - (t+1)t)Y^l(v),$$

that is,

$$(t+1)\lambda - (t+1)t = 0,$$

which means that $\lambda = t$, an integer. Now, say V is irreducible and t is the maximum weight in V. If V has weight t, then $X(v)$ has weight $t + 2$, a contradiction, unless $X(v) = 0$. Therefore, v is primitive. Now, Proposition 1.46 implies that V is as claimed. □

Observe that the standard representation of $\mathfrak{sl}(2, \mathbb{C})$ is given by

$$H\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix}, \quad X\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ 0 \end{pmatrix}, \quad Y\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ x \end{pmatrix}.$$

Consider any Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$ ane let us find out how it operates on tensor products. Given two representations of G with representation spaces V and W, for every $\sigma \in G$, we have

$$\sigma(v \otimes w) = \sigma v \otimes \sigma w.$$

Let γ be a curve in G through 1_G, with $\gamma'(0) = X \in \mathfrak{g}$. We must have

$$\begin{aligned} X(v \otimes w) &= \frac{d}{dt}(\gamma(t)v \otimes \gamma(t)w)\Big|_{t=0} \\ &= (\gamma(t)v \otimes \gamma'(t)w + \gamma'(t)v \otimes \gamma(t)w)\Big|_{t=0} \\ &= v \otimes X(w) + X(v) \otimes w. \end{aligned}$$

This shows that X acts as a derivation. Later, we will also need to know how a Lie algebra acts on the dual of a representation space. First, if $R\colon G \to \mathbf{GL}(V)$ is a group representation, we define the *dual representation* $R^D\colon G \to \mathbf{GL}(V^D)$ by

$$R^D(g) = (R(g^{-1}))^\top = (R(g)^{-1})^\top\colon V^D \longrightarrow V^D.$$

Then, differentiating as in the tensor product case, we see that if $\rho\colon \mathfrak{g} \to \mathrm{End}(V)$ is a representatiom of a Lie algebra $\mathfrak{g}$, then the *dual representation* $\rho^D\colon \mathfrak{g} \to \mathrm{End}(V^D)$ is given by

$$\rho^D(X) = -\rho(X)^\top : V^D \longrightarrow V^D.$$

Now, look at $\mathrm{Sym}^n(\mathbb{C}^2)$. If we choose a basis (e_1, e_2) for $\mathbb{C}^2$, then the symmetric tensors of the form $e_1^r e_2^s$ form a basis of $\mathrm{Sym}^n(\mathbb{C}^2)$, which is isomorphic to the vector space of homogeneous polynomials of degree n in two variables x and y. Let us find out what is the action of H on the basis element $x^r y^s$. Since $H(x) = x$ and $H(y) = -y$, we get

$$\begin{aligned} H(x^r y^s) &= x^r H(y^s) + H(x^r) y^s \\ &= s x^r y^{s-1} H(y) + r x^{r-1} y^s H(x) \\ &= -s x^r y^s + r x^r y^s \\ &= (r - s) x^r y^s. \end{aligned}$$

It follows that H acts on $\mathrm{Sym}^n(\mathbb{C}^2)$ as it acts on $V(n)$, and the irrep corresponding to $V(t)$ has an explicit description as derivations on complex homogeneous polynomials of degree n in two variables. We recover, $V(0) = \mathbb{C}$, and $V(1) = \mathbb{C}^2$, the standard representation.

(B) $\mathfrak{sl}(3, \mathbb{C})$. These are the complex 3×3 matrices X with zero trace,

$$\left\{ \begin{pmatrix} a & * & * \\ * & b & * \\ * & * & c \end{pmatrix} \;\middle|\; a + b + c = 0 \right\}.$$

The subspace of diagonal traceless matrices

$$\mathfrak{h} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \;\middle|\; a + b + c = 0 \right\}$$

plays the role of H. The space $\mathfrak{h}$ is a maximal abelian subalgebra of $\mathfrak{sl}(3, \mathbb{C})$. It is a *Cartan subalgebra*. Because the matrices in $\mathfrak{h}$ are diagonalizable and commute, and because $\mathfrak{sl}(3, \mathbb{C})$ is semisimple, by Proposition 1.44, in any representation of $\mathfrak{sl}(3, \mathbb{C})$, the matrices corresponding to the elements of $\mathfrak{h}$ are diagonalizable with respect to a common basis. It follows that the representation space V can be written as a finite coproduct of "eigenspaces,"

$$V = \coprod_\alpha V_\alpha, \tag{$*$}$$

where

$$V_\alpha = \{v \in V \mid H(v) = \alpha(H)v \text{ for some } \alpha(H) \in \mathbb{C}, \text{ for all } H \in \mathfrak{h}\}.$$

Observe that $H \mapsto \alpha(H)$ defines a linear form on $\mathfrak{h}$, that is, an element of the dual, $\mathfrak{h}^D$, of $\mathfrak{h}$. We say that V_α is an *eigenspace for* $\mathfrak{h}$, that the nonzero vectors $v \in V_\alpha$ are *eigenvectors for*

$\mathfrak{h}$, and that $\alpha \in \mathfrak{h}^D$ is an *eigenvalue for* $\mathfrak{h}$. Only finitely many $\alpha \in \mathfrak{h}$ appear in the coproduct $(*)$.

What is the analog of X and Y? Going back to $\mathfrak{sl}(2,\mathbb{C})$, we note that the equations

$$[H,X] = 2X$$
$$[H,Y] = -2Y$$

can be interpreted in terms of the adjoint action of $\mathfrak{sl}(2,\mathbb{C})$ as saying that X and Y are eigenvectors of $\mathrm{ad}(H)$, for every $H \in \mathfrak{h}$:

$$\mathrm{ad}(H)(X) = 2X$$
$$\mathrm{ad}(H)(Y) = -2Y.$$

Observe that $\mathfrak{h}$ is spanned by the linear forms L_1, L_2, L_3 given by

$$L_i \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix} = a_i,$$

and that

$$L_1 + L_2 + L_3 = 0.$$

Given any matrix $M = (m_{ij})$, it is clear that

$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix} M - M \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix} = \Big((a_i - a_j)m_{ij}\Big).$$

Therefore, $M = (m_{ij})$ is an eigenvector for $\mathrm{ad}(H)$ (for all $H \in \mathfrak{h}$) iff $M = E_{ij}$, where E_{ij} is the matrix given by

$$(E_{ij})_{hk} = \begin{cases} 1 & \text{if } h = i \text{ and } k = j \\ 0 & \text{otherwise,} \end{cases}$$

with $1 \leq i, j \leq 3$ and $i \neq j$. It follows that E_{ij} is an eigenvector for $L_i - L_j \in \mathfrak{h}^D$, and there are six such elements, for $i \neq j$. The decomposition $(*)$ applied to $A = \mathfrak{sl}(3,\mathbb{C})$, the representation space of the adjoint representation of $\mathfrak{sl}(3,\mathbb{C})$, yields

$$\mathfrak{sl}(3,\mathbb{C}) = A_{L_3-L_2} \coprod A_{L_3-L_1} \coprod A_{L_2-L_1} \coprod \mathfrak{h} \coprod A_{L_1-L_2} \coprod A_{L_1-L_3} \coprod A_{L_2-L_3},$$

with each $A_{L_i-L_j}$ one-dimensional and spanned by E_{ij}.

More generally, for any semisimple Lie algebra $\mathfrak{g}$, there is a similar decomposition

$$\mathfrak{g} = \mathfrak{h} \amalg \coprod_{\alpha} \mathfrak{g}_\alpha,$$

where the $\mathfrak{g}_\alpha$ are some of the eigenspaces for $\mathfrak{h}$ (finitely many).

Nomenclature

(1) The eigenvectors α for $\mathfrak{h}$ appearing in the decomposition

$$V = \coprod_{\alpha} V_\alpha$$

are the *weights* of the representation V.

(2) Each V_α is the *weight space* corresponding to $\alpha \in \mathfrak{h}^D$.

(3) Each nonzero vector $v \in V_\alpha$ is a *weight vector* for α.

(4) When the representation is the adjoint representation with $V = \mathfrak{g}$ as a vector space and with

$$X(v) = \mathrm{ad}(X)(v) = [X, v], \text{ for all } X \in \mathfrak{g},$$

the weights of this representation are called the *roots* of $\mathfrak{g}$.

(5) The space $\mathfrak{g}_\alpha$ is the αth *root space*.

(6) Each nonzero $v \in \mathfrak{g}_\alpha$ is a *root vector*.

Let us now consider the decomposition

$$\mathfrak{g} = \mathfrak{h} \amalg \coprod_{\alpha} \mathfrak{g}_\alpha$$

associated with the adjoint representation. Given $X \in \mathfrak{g}_\alpha$ and $Y \in \mathfrak{g}_\beta$, what is $\mathrm{ad}(X)(Y) = [X, Y]$? To find out what this is, see how $\mathfrak{h}$ acts on it, so pick any $H \in \mathfrak{h}$ and compute

$$\begin{aligned} H(\mathrm{ad}(X)(Y) &= \mathrm{ad}(H)(\mathrm{ad}(X)(Y)) \\ &= \mathrm{ad}(H)([X, Y]) = [H, [X, Y]]. \end{aligned}$$

Using the Jacobi identity, we get

$$\begin{aligned} [H, [X, Y]] &= -[X, [Y, H]] - [Y, [H, X]] \\ &= [X, [H, Y]] - [Y, [H, X]] \\ &= [X, \beta(H)Y] - [Y, \alpha(H)X] \\ &= (\alpha(H) + \beta(H))[X, Y]. \end{aligned}$$

This shows that $\mathrm{ad}(X)(Y) = [X, Y]$ is an eigenvector for $\mathfrak{h}$ for the weight $\alpha + \beta$. Thus, we obtain the following Proposition:

Proposition 1.49. *If $\mathfrak{g}$ is a Lie algebra and*

$$\mathfrak{g} = \mathfrak{h} \amalg \coprod_{\alpha} \mathfrak{g}_\alpha$$

is the decomposition associated with the adjoint representation, if $X \in \mathfrak{g}_\alpha$ and $Y \in \mathfrak{g}_\beta$, then $[X, Y] \in \mathfrak{g}_{\alpha+\beta}$.

We can prove a similar result for the decomposition

$$V = \mathfrak{h} \amalg \coprod_{\alpha} V_\alpha$$

associated with any representation.

Proposition 1.50. *For any representation V of a lie algebra $\mathfrak{g}$, if*

$$V = \mathfrak{h} \amalg \coprod_{\alpha} V_\alpha,$$

then for any $X \in \mathfrak{g}_\alpha$ and any $v \in V_\beta$, we have $X(v) \in V_{\alpha+\beta}$.

Proof. For any $H \in \mathfrak{h}$, we have

$$\begin{aligned} H(X(v)) &= X(H(v)) + [H, X](v) \\ &= X(\beta(H)v) + \mathrm{ad}(H)(X)(v) \\ &= \beta(H)X(v) + \alpha(H)X(v) \\ &= (\beta(H) + \alpha(H))X(v), \end{aligned}$$

whenever α is a root and β is a weight for V. □

An important consequence of Proposition 1.50 is this:

Proposition 1.51. *For any irreducible representation V of a Lie algebra $\mathfrak{g}$, the weights for V differ by integral linear combinations of the roots of $\mathfrak{g}$.*

Proof. Consider

$$W = \mathfrak{h} \amalg \coprod V_{\lambda + \sum k_\alpha \alpha},$$

where α runs over the roots and $k_\alpha \in \mathbb{Z}$. Then the action of $\mathfrak{g}$ takes W into W, and by Schur's Lemma, $V = W$. □

The roots of $\mathfrak{g}$ form an integral lattice in $\mathfrak{h}^D$ denoted by Λ_{root} and called the *root lattice*.

Now, what we need to do is to find an extremal root that corresponds to an extremal V_t in the case of $\mathfrak{sl}(2, \mathbb{C})$. We can do so by choosing a linear form φ on Λ_{root}, in order to divide the roots into positive roots (those on one side of the line determined by φ), and negative roots (those on the other side of the line determined by φ). To make sure that this line does not pass through any point of the lattice Λ_{root} besides the origin, we pick $\varphi(L_1) = a$, $\varphi(L_2) = b$, and $\varphi(L_3) = b$, real and irrational (with $a + b + c = 0$). We extend φ to $\mathfrak{h}^D$ by linearity.

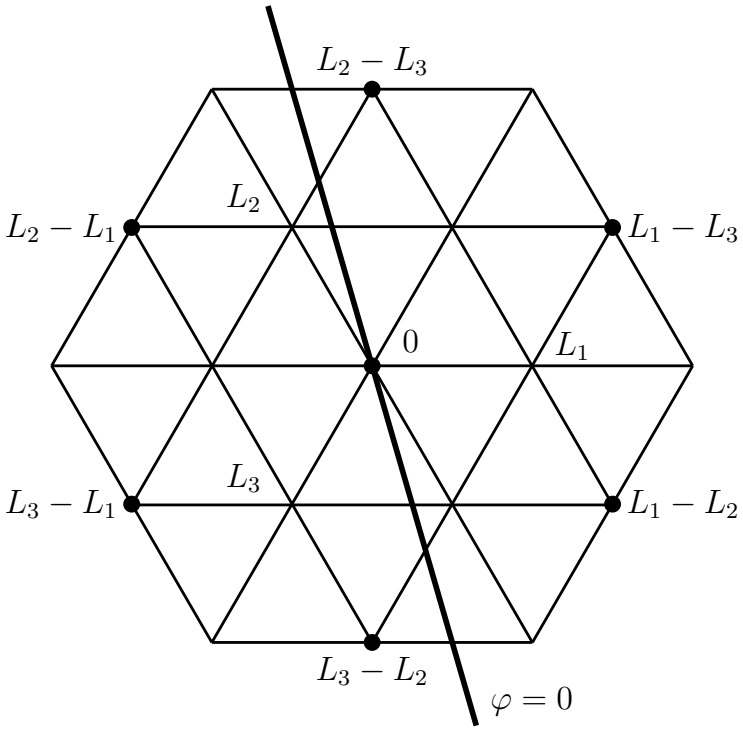


Figure 1.5: Choosing the Positive Roots

Then, we pick a weight α in V such that $\mathrm{Re}(\varphi(\alpha))$ is maximal. If we assume that $a > b > c$, then we have

$$\begin{aligned}\varphi(L_1 - L_3) &= a - c > 0\\ \varphi(L_1 - L_2) &= a - b > 0\\ \varphi(L_2 - L_3) &= b - c > 0,\end{aligned}$$

and with respect to this choice of φ, the roots $L_1 - L_3$, $L_1 - L_2$, and $L_2 - L_3$ are positive roots.

Remark: By convention, 0 is not a root.

Say β is a root and $\varphi(\beta) > 0$. Then for every $X \in \mathfrak{g}_\beta$ and for every nonzero $v \in V_\alpha$ where α is maximal, we know that $X(v) \in V_{\alpha+\beta}$. But,

$$\begin{aligned}\mathrm{Re}(\varphi(\alpha+\beta)) &= \mathrm{Re}(\varphi(\alpha)) + \mathrm{Re}(\varphi(\beta))\\ &= \mathrm{Re}(\varphi(\alpha)) + \varphi(\beta) > \mathrm{Re}(\varphi(\alpha)).\end{aligned}$$

By maximality of α, we see that

$$V_{\alpha+\beta} = (0).$$

As a consequence, all positive root vectors of $\mathfrak{sl}(3,\mathbb{C})$ kill V_α, and so

$$E_{ij}(v) = 0, \quad \text{whenever } i < j.$$

A nonzero vector $v \in V_\alpha$ with α maximal is called a *highest weight vector* and α is called a *highest weight*.

By analogy with the case of $\mathfrak{sl}(2,\mathbb{C})$, we will show that if V is an irrep, then V is generated by applying compositions of the E_{ij} to any highest weight vector v, with $i > j$, that is, to the E_{ij} corresponding to negative roots.

Let $E_{(ij)}^{(k)}$ denote any k-fold composition of the E_{ij} with $i > j$.

Proposition 1.52. *For any representation V of a Lie algebra $\mathfrak{g}$, for any highest weight vector v, the space W spanned by the vectors $E_{(ij)}^{(k)}v$ with $i > j$ and $k \geq 1$ is an irreducible subrepresentation of V. In particular, if V is an irrep, then $V = W$.*

Sketch of proof. We need to prove that $E_{ij}(W) \subseteq W$. Since

$$E_{ij}(v) = 0, \quad \text{if } i < j,$$

we just need to check that $E_{1,2}, E_{2,3}$, and $E_{1,3}$ carry W into itself. Since

$$E_{1,3} = [E_{1,2}, E_{2,3}],$$

it suffices to prove it for $E_{1,2}$ and $E_{2,3}$. We proceed by induction on the length of words. Let $w_n(v)$ denote any word of length at most n in the letters $E_{2,1}$ and $E_{3,2}$, and let W_n be the vector space spanned by the vectors $w_n(v)$, with $W_0 = \mathrm{Span}(v)$. Clearly, there is some n such that $W = W_n$. We claim that

$$\begin{aligned} E_{12}(W_n) &\subseteq W_{n-1} \\ E_{2,3}(W_n) &\subseteq W_{n-1}. \end{aligned}$$

For $n = 0$, we have

$$\begin{aligned} E_{1,2}(E_{2,1}(v)) &= E_{2,1}(E_{1,2}(v)) + [E_{1,2}, E_{2,1}](v) \\ &= \alpha([E_{1,2}, E_{2,1}])v, \end{aligned}$$

since $E_{1,2}(v) = 0$ and $[E_{1,2}, E_{2,1}] \in \mathfrak{h}$. We also have

$$\begin{aligned} E_{2,3}(E_{2,1}(v)) &= E_{2,1}(E_{2,3}(v)) + [E_{2,3}, E_{2,1}](v) \\ &= 0, \end{aligned}$$

since $E_{2,3}(v) = 0$ and $[E_{2,3}, E_{2,1}] = 0$. A similar computation shows that $E_{3,2}(v)$ is also carried into W_0 by $E_{1,2}$ and $E_{2,3}$.

For the induction step, w_n is either of the form $E_{2,1} \circ w_{n-1}$ or of the form $E_{3,2} \circ w_{n-1}$. In either case, $w_{n-1}(v)$ is an eigenvector for $\mathfrak{h}$ for some eigenvalue β. If $w_n = E_{2,1} \circ w_{n-1}$, for the action of $E_{1,2}$ we have

$$\begin{aligned} E_{1,2}(w_n(v)) &= E_{1,2}(E_{2,1}(w_{n-1}(v))) \\ &= E_{2,1}(E_{1,2}(w_{n-1}(v))) + [E_{1,2}, E_{2,1}](w_{n-1}(v)) \\ &\in E_{2,1}(W_{n-2}) + \beta([E_{1,2}, E_{2,1}])w_{n-1}(v) \\ &\subseteq W_{n-1}, \end{aligned}$$

since $[E_{1,2}, E_{2,1}] \in \mathfrak{h}$. For the action of $E_{2,3}$ we have

$$\begin{aligned} E_{2,3}(w_n(v)) &= E_{2,3}(E_{2,1}(w_{n-1}(v))) \\ &= E_{2,1}(E_{2,3}(w_{n-1}(v))) + [E_{2,3}, E_{2,1}](w_{n-1}(v)) \\ &\in E_{2,1}(W_{n-2}) \\ &\subseteq W_{n-1}, \end{aligned}$$

since $[E_{2,3}, E_{2,1}] = 0$. A similar computation covers the case $w_n = E_{3,2} \circ w_{n-1}$. □

We obtain the following corollaries:

(1) If V is an irrep and α is a highest weight, then $\dim(V_\alpha) = 1$.

(2) If V is an irrep then there is a unique highest weight vector, up to scalars.

(3) If V is any representation of $\mathfrak{sl}(3, \mathbb{C})$, and if α is a highest weight, then V is irreducible iff $\dim(V_\alpha) = 1$. Indeed, assume that

$$V = W \coprod W'.$$

Projection onto W or W' commutes with the action of $\mathfrak{h}$. Consequently,

$$V_\alpha = W_\alpha \coprod W'_\alpha,$$

but $\dim(V_\alpha) = 1$, so v is either in W_α or in W'_α. We may assume that $v \in W_\alpha$, and so $W'_\alpha = (0)$. The action of $\mathfrak{g}_\alpha$ on W' gives 0, so $W' = (0)$, and $V = W$.

Let

$$[E_{1,2}, E_{2,1}] = H_{1,2} = E_{1,1} - E_{2,2}.$$

More generally, write

$$[E_{i,j}, E_{j,i}] = H_{i,j}.$$

Note that $H_{i,j} \in \mathfrak{h}$. We find that

$$[H_{1,2}, E_{1,2}] = [E_{1,1}, E_{1,2}] - [E_{2,2}, E_{1,2}] = 2E_{1,,2}$$

and

$$[H_{1,2}, E_{2,1}] = -2E_{2,1}.$$

Therefore, $E_{1,2}, E_{2,1}$, and $H_{1,2}$ generate a subalgebra $\mathfrak{s}_{L_1-L2}$ of $\mathfrak{sl}(3,\mathbb{C})$ isomorphic to $\mathfrak{sl}(2,\mathbb{C})$ *via* the map

$$\begin{aligned} E_{1,2} &\mapsto X \\ E_{2,1} &\mapsto Y \\ H_{1,2} &\mapsto H. \end{aligned}$$

More generally, for any β root of $\mathfrak{g}$, the coproduct

$$W = \coprod_{k\in\mathbb{Z}} \mathfrak{g}_{\beta+k(L_i-L_j)}$$

is a representation of $\mathfrak{s}_{L_i-L_j}$ (which is isomorphic to $\mathfrak{sl}(2,\mathbb{C})$).

In order to understand better the structure of the root lattice, we need to figure out the symmetries induced by the action of $\mathfrak{s}_{L_1-L2}$. Recall the pairing between $\mathfrak{h}$ and $\mathfrak{h}^D$ given by

$$\langle X, \beta\rangle = \beta(X), \quad X \in \mathfrak{h},\ \beta \in \mathfrak{h}^D.$$

Let us find out what is the line given by the equation

$$\langle H_{1,2}, \beta\rangle = 0.$$

We can write $\beta = \xi_1 L_1 + \xi_2 L_2 + \xi_3 L_3$, with $\xi_1 + \xi_2 + \xi_3 = 0$, and we get

$$\begin{aligned} \langle H_{1,2}, \beta\rangle &= (\xi_1 L_1 + \xi_2 L_2 + \xi_3 L_3)(H_{1,2}) \\ &= \xi_1 L_1(H_{1,2}) + \xi_2 L_2(H_{1,2}) + \xi_3 L_3(H_{1,2}) \\ &= \xi_1 - \xi_2. \end{aligned}$$

It follows that the line given by $\langle H_{1,2}, \beta\rangle = 0$ is the line spanned by L_3. But, as $L_1+L_2+L_3 = 0$, we have $L_3 = -L_1 - L_2$, which is orthogonal to $L_1 - L_2$.

The same reasoning applies to the lines defined by $H_{1,3}$ and $H_{2,3}$, and we deduce the following facts for any highest weight α:

(1) If we reflect α about the lines spanned by L_1, L_2, and L_3, then all the weights must occur inside or on the boundary of the convex hull of these various reflected points; See Figure 1.6.

(2) The various extreme points (the reflections of α) are heighest weights for different orderings of a, b, c (in φ); for example, in Figure 1.6, the weight $\widetilde{\alpha}$ corresponds to the ordering $b > a > c$.

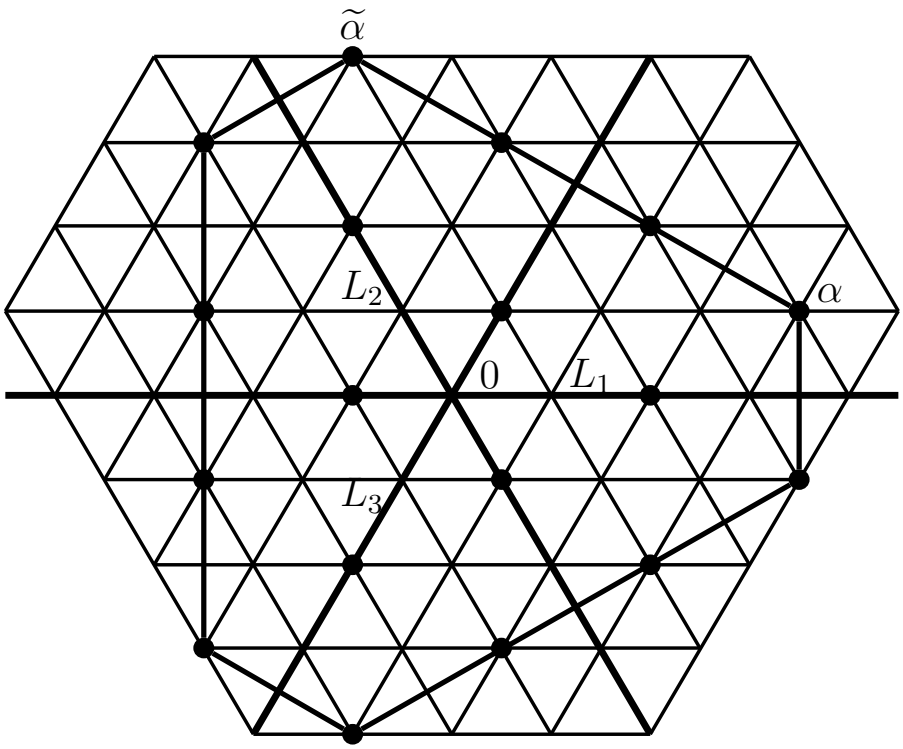


Figure 1.6: Root Lattice and weights

(3) Applying $\mathfrak{sl}(2,\mathbb{C})$ to any boundary point, we get any point in the interior as a weight if it is on the root lattice.

We can summarize all these facts in the following theorem:

Theorem 1.53. *If V is an irrep of $\mathfrak{sl}(3,\mathbb{C})$, then there is a unique highest weight α (up to a scalar) such that the set of weights in V is exactly the set of linear forms congruent to α modulo the root lattice $\Lambda_{\text{root}} = \mathbb{Z}L_1 + \mathbb{Z}L_2 + \mathbb{Z}L_3$ ($L_1 + L_2 + L_3 = 0$) and lying in the hexagon with vertices the images of α under the reflections in the lines $\langle H_{i,j}, \beta\rangle = 0$, that is, the lines spanned by the L_i.*

Our previous discussion shows that any highest weight α must lie in the part of the plane determined by the inequalities $\langle H_{1,2}, L\rangle \geq 0$ and $\langle H_{2,3}, L\rangle \geq 0$. It follows that α must be of the form

$$\alpha = (m_1 + m_2)L_1 + m_2 L_2 = m_1 L_1 - m_2 L_3,$$

for some nonnegative integers $m_1, m_2 \in \mathbb{N}$. We also have a sort of converse.

Theorem 1.54. *For every pair of natural numbers $a, b \in \mathbb{N}$, there exists a unique irrep of $\mathfrak{sl}(3,\mathbb{C})$ with heighest weight $aL_1 - bL_2$; denote it by $\Gamma_{a,b}$.*

Proof Sketch. First, consider uniqueness. Say Z and $\widetilde{Z}$ are two irrreps of $\mathfrak{g}$ with the same heighest weight α and consider the vector space $Z \coprod \widetilde{Z}$. Then, $Z \coprod \widetilde{Z}$ is a representation of $\mathfrak{g}$ also with heighest weight α. This is because if z and $\widetilde{z}$ are (unique up to a scalar) heighest weight vectors, then $(z, \widetilde{z})$ is a highest weight vector in $Z \coprod \widetilde{Z}$ (recall that the action of $\mathfrak{g}$ on $Z \coprod \widetilde{Z}$ is given by $X(z, \widetilde{z}) = (X(z), X(\widetilde{z}))$). By Proposition 1.52, the vector $(z, \widetilde{z})$ generates an irrep $Q \subseteq Z \coprod \widetilde{Z}$. Consider the maps induced by the projection of $Z \coprod \widetilde{Z}$ onto its factors

$$Q \hookrightarrow Z \coprod \widetilde{Z} \longrightarrow Z$$
$$Q \hookrightarrow Z \coprod \widetilde{Z} \longrightarrow \widetilde{Z}.$$

Both maps are not zero, yet $Q, Z, \widetilde{Z}$ are irreducible, so Schur's Lemma implies that $Q \cong Z$ and $Q \cong \widetilde{Z}$, and thus $Z \cong \widetilde{Z}$.

Next we consider existence. Let $V = \mathbb{C}^3$ and construe V as a representation of $\mathfrak{sl}(3, \mathbb{C})$, namely the standard representation. The eigenvalues for $\mathfrak{h}$ are L_1, L_2, L_3. For the dual representation, by a previous remark, the eigenvalues are $-L_1, -L_2, -L_3$.

Observe that if W and Z are representations of $\mathfrak{g}$, and if $w \in W$ and $z \in Z$ are highest weight vectors with weights α and β, then $w \otimes z$ is a highest weight vector in $W \otimes Z$ with weight $\alpha + \beta$. This fact has the following consequences:

(1) The highest weight vector $w \otimes z \in W \otimes Z$ generates a subrepresentation of $W \otimes Z$ which is an irrep.

(2) The representations $\mathrm{Sym}^a V$ is an irrep with highest weight aL_1.

(3) The representations $\mathrm{Sym}^b V^D$ is an irrep with highest weight $-bL_3$.

Consequently, we see that the irreps $\Gamma_{a,0}$ and $\Gamma_{0,b}$ are given by $\Gamma_{a,0} = \mathrm{Sym}^a V$ and $\Gamma_{0,b} = \mathrm{Sym}^b V^D$.

If we look at $V \otimes V^D$, we see that the weights are the linear forms $L_i - L_j$, with $i \neq j$, and the highest weight is $L_1 - L_3$. A highest weight vector associated with $L_1 - L_3$ generates a subrepresentation of $V \otimes V^D$ isomorphic to $\Gamma_{1,1}$. More generallly, $\mathrm{Sym}^a V \otimes \mathrm{Sym}^b V^D$ contains a highest weight vector of weight $aL_1 - bL_2$, and thus a subrepresentation which is an irrep isomorphic to $\Gamma_{a,b}$, with $a, b \in \mathbb{N}$.

To find this irrep more explicitly, we can make use of the contraction map

$$\Theta_{a,b} \colon \mathrm{Sym}^a V \otimes \mathrm{Sym}^b V^D \to \mathrm{Sym}^{a-1} V \otimes \mathrm{Sym}^{b-1} V^D$$

given by

$$\Theta_{a,b}(w_1 \cdots w_a \otimes z_1^D \cdots z_b^D) = \sum_{i \neq j} z_j^D(w_i)(w_1 \cdots \widehat{w_i} \cdots w_a \otimes z_1^D \cdots \widehat{(z_j^D)} \cdots z_b^D).$$

The map $\Theta_{a,b}$ is a Lie algebra map and it can be shown that its kernel is $\Gamma_{a,b}$. Consequently, we have an exact sequence

$$0 \longrightarrow \Gamma_{a,b} \longrightarrow \mathrm{Sym}^a V \otimes \mathrm{Sym}^b V^D \longrightarrow \mathrm{Sym}^{a-1} V \otimes \mathrm{Sym}^{b-1} V^D \longrightarrow 0,$$

which yields an inductive description of the representation $\mathrm{Sym}^a V \otimes \mathrm{Sym}^b V^D$. □

Remark: The representation $V \otimes V^D$ of $\mathfrak{sl}(3, \mathbb{C})$ occurs in high energy physics, and has to do with quarks and antiquarks. The adjoint representation of $\mathfrak{sl}(3, \mathbb{C})$ has to do with baryons (feel the strong force) and mesons. Gell–Mann called it the "eight-fold way."

The representations of $\mathfrak{sl}(4, \mathbb{C}), \ldots, \mathfrak{sl}(n, \mathbb{C})$ are described in much the same way as the representations of $\mathfrak{sl}(3, \mathbb{C})$, using the notion of highest weight.

How about simply-connected Lie groups?

Say G is a simply-connected Lie group and let $\rho\colon \mathfrak{g} \to \mathrm{End}(V)$ be a representation of its Lie algebra. For a small enough open neighborhood U of 1 in G, the exponential map

$$\exp\colon \mathfrak{g} \to G$$

is a diffeomorphism. We can make a representation $\widetilde{\rho}$ of G as follows: for every $\sigma \in U$, we have $\sigma = \exp(X)$ for some unique $X \in \mathfrak{g}$, so $\rho(X) \in \mathfrak{gl}(n, \mathbb{C})$ and we set

$$\widetilde{\rho}(\sigma) = e^{\rho(X)},$$

where

$$e^{\rho(X)} = \sum_{k=0}^{\infty} \frac{\rho(X)^k}{k!}$$

is the matrix exponential. Since U generates G, the map $\widetilde{\rho}(\sigma)$ is defined for all $\sigma \in G$.

For more on the representation of groups, Lie groups, and Lie algebras, the reader should consult Fulton and Harris [5], Knapp [11], Serre [13, 15, 14], Bröcker, and tom Dieck [2] and Humphreys [9].

Chapter 2

Numerical Linear Algebra

2.1 Some Elementary Numerical Analysis. Some Bad Examples. "Algorithms"

In a computer, the reals cannot be embedded. We put it as a discrete substitute, "floating point computations."

Fix a number b, the *base* ($b = 2, 4, 8, 16$), fix s, the *number of places*, and two integers m and M, the min and max *exponent*; then $\mathrm{fl}(\mathbb{R})$ consists in numbers

$$\pm .d_1 \cdots d_s \, b^e, \quad \text{where } m \leq e \leq M,\ d_j \in \mathbb{N}, \text{ with } 0 \leq d_j \leq b-1 \text{ if } j \geq 2 \text{ and } 1 \leq d_1 \leq b-1.$$

Zero is represented by

$$+ .0 \cdots 0 \, b^m.$$

Examples. In old and big IBM machines, $b = 16$, $m = -63$, $M = 64$, $s = 6$ for ordinary arithmetic, and $s = 14$ for double precision arithmetic.

If x, y are two real numbers, when do we think that $\mathrm{fl}(x)$ and $\mathrm{fl}(y)$ are the same? The convention is that

$$\frac{|x-y|}{|x|} \leq \frac{1}{2} b^s \stackrel{\text{def}}{=} \epsilon_{\text{machine}}.$$

Let $*$ be a binary operation on the real numbers. Then

$$\mathrm{fl}(x * y) = (x * y)(1+\epsilon), \quad \text{where } \epsilon \leq \epsilon_{\text{machine}}.$$

Problems and Algorithms

We have a vector space of data, D, and we have a vector space of solutions, S. A *problem* is a function $f\colon D \to S$. An *algorithm* for a problem f consists in

(1) Making D into $\mathrm{fl}(D) \subseteq D$.

(2) A naive notion of an algorithm: a discrete well-defined process that always terminates.

(3) A program to run an algorithm on a computer.

(4) The output of the algorithm is of the form $\mathrm{fl}(S) \subseteq S$.

Let us denote by $\widetilde{f}$ an algorithm for f. The following property is desired:

$$\frac{\|\widetilde{f}(x) - f(x)\|}{\|f(x)\|} = O(\epsilon_{\text{machine}}). \tag{$\dagger$}$$

Recall that in analysis, we write (assuming $h(\xi) \geq 0$)

$$g(\xi) = O(h(\xi)) \text{ as } \xi \mapsto L$$

iff there is a constant $C > 0$ such that

$$|g(\xi)| \leq Ch(\xi) \text{ near } L. \tag{$*$}$$

If g is one of a family of functions, say $g_s(t)$, where $s \in \mathcal{S}$, then $(*)$ might mean

$$|g_s(\xi)| \leq C(s)h(\xi) \text{ near } L,$$

or

$$|g_s(\xi)| \leq Ch(\xi) \text{ near } L.$$

In the second case, we say that g is *uniformly* $O(h)$ *near* L . We always want uniformity in $(\dagger)$ if f depends on a parameter.

Some problems are "bad," or ill -posed (Hadamard), ill-conditioned, chaotic: this means that a small change in x (say from x to $\widetilde{x} = \mathrm{fl}(x)$) can make a *very large* difference in $f(x)$, and so in $\widetilde{f}(x)$.

A *stable algorithm* is one for which

$$\frac{\|\widetilde{f}(x) - f(\widetilde{x})\|}{\|f(\widetilde{x})\|} = O(\epsilon_{\text{machine}})$$

if

$$\frac{\|\widetilde{x} - x\|}{\|x\|} = O(\epsilon_{\text{machine}}).$$

That is, the algorithm gives "nearly the right answer to nearly the right question." It would be better if whenever

$$\frac{\|\widetilde{x} - x\|}{\|x\|} = O(\epsilon_{\text{machine}}),$$

then

$$\|\widetilde{f}(x) - f(\widetilde{x})\| = 0,$$

that is, the algorithm gives "exactly the right answer to nearly the right question." Such an algorithn is called *backwardly stable*.

Bad examples

(1) Moler's Example.

$$\begin{aligned} 0.778x + 0.563y &= 0.217 \\ 0.913x + 0.659y &= 0.254. \end{aligned} \tag{E}$$

The first proposed "solution" is:

$$\begin{aligned} x &= 0.999 \\ y &= -1.001, \end{aligned}$$

and the second proposed "solution" is

$$\begin{aligned} x &= 0.341 \\ y &= -0.087. \end{aligned}$$

To check how "good" these solutions are, we substitute them in the error expressions

$$\begin{aligned} &0.778x + 0.563y - 0.217 \\ &0.913x + 0.659y - 0.254. \end{aligned}$$

For the first solution, we get

$$\begin{aligned} &- 0.001243 \\ &- 0.001572, \end{aligned}$$

and for the second solution we get

$$\begin{aligned} &- 0.000001 \\ &0. \end{aligned}$$

By this measurement, it looks like we should choose the second solution. However, the exact solution is

$$\begin{aligned} x &= 1 \\ y &= -1. \end{aligned}$$

Which solution we pick depends on the criterion chosen. If we wish to minimize the error term, then we should pick the second solution, although it is not as "close" to the exact solution as the first solution. Note that if we use Gaussian elimination, then

$$\delta = \frac{913}{780} = 1.17050$$

and then

$$.563\,\delta = .65899$$
$$.217\,\delta = .253999.$$

(2) Polynomial Equations

Consider the quadratic equation

$$x^2 - 4x + 4 = 0,$$

whose solution is $x = 2$, a double root. Make a small change:

$$x^2 - 4x + 3.9999999 = 0.$$

The new solutions are

$$x = \begin{cases} 1.9996838 \\ 2.0003162 \end{cases}$$

We changed the data of the problem by 10^{-7} and the solution changed by 3×10^{-4}, a ratio of 3000.

This bad behavior can be explained as follows: we changed the equation

$$(x-2)^2 = 0$$

to

$$(x-2) - \epsilon = 0,$$

for some $\epsilon > 0$. The new solutions are

$$x = 2 \pm \sqrt{\epsilon}.$$

But, if ϵ is small, then $\sqrt{\epsilon} \gg \epsilon$.

As a general rule, if in a computation small numbers appear, avoid forming powers $(\text{number})^a$ if $0 < a < 1$.

(3) Hilbert's Problem.

Given a continuous function $f \in \mathcal{C}([0,1])$, the problem is to approximate f by a polynomial of degree $n-1$,

$$p(t) = x_1 + x_2 t + \cdots + x_n t^{n-1},$$

in the unknowns $x_1, \ldots, x_n$. By Gauss, the best approximation is by least squares, that is, $p(t)$ minimizes

$$\|f(t) - p(t)\|_2 .$$

Therefore, we wish to minimize

$$\Phi(x_1, \ldots, x_n) = \int_0^1 (f(t) - p(t))^2 dt.$$

It is easy to see that there is a unique solution obtained by setting

$$\frac{\partial \Phi}{\partial x_i} = 0, \quad i = 1, \ldots, n.$$

This yields a systems of n linear equations in $x_1, \ldots, x_n$,

$$Ax = b, \tag{††}$$

whose matrix $A = (a_{ij})$ is given by

$$a_{ij} = \frac{1}{i + j - 1}$$

and with

$$b_i = \int_0^1 f(t) t^{i-1} dt.$$

The matrix

$$A = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots & \frac{1}{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n} & \frac{1}{n+1} & \frac{1}{n+2} & \cdots & \frac{1}{2n-1} \end{pmatrix}$$

is the nth *Hilbert matrix*, denoted by H_n. Here are some facts about the Hilbert matrix:

(1) The matrix H_n is invertible. I fact, it is symmetric, positive, definite (as the matrix of inner products (t^{i-1}, t^{j-1})).

(2) The inverse matrix H_n^{-1} has integer coefficients.

(3) The determinant of H_n is ridiculously small.

(4) For any $n \times n$ matrix $A = (a_{ij})$, if we let

$$\|A\|_\infty = \max |a_{ij}|,$$

then we have the following table:

n	$\|H_n^{-1}\|_\infty$
2	12
3	192
4	6,480
5	1.79×10^5
6	4.41×10^6
7	1.33×10^8
8	4.25×10^9
9	1.22×10^{11}
10	3.48×10^{12}

The linear system (††) cannot be solved in s-place floating point arithmetic with base b if $\|H_n^{-1}\|_\infty \gg b^s$.

(4) Wilkinson's Example

This is the polynomial

$$P(x) = \prod_{j=1}^{20}(x-j) = x^{20} - 210x^{19} + \cdots + 20!.$$

The roots of this polynomials are the integers $j = 1, \ldots, 20$, all real and well separated. Say we use $b = 2$, $s = 30$ for floating point. So, we enter the data into the computer ($\widetilde{x}$ in D) by rounding to 30 significant bits (base 2). Now, make a small change in *only one* of the twenty coefficients, and make this change *only in the* 30*th significant bit*. What happens?

Wilkinson changed the coefficient of x^{19} and computed roots for

$$P(x) - 2^{-23}x^{19} = 0,$$

using $b = 2$, but $s = 90$. Here are the answers for the 20 roots: 10 remain real, 10 are now complex:

1.00000 0000	$10.09526\,6145 \pm 0.64350\,0904i$
2.00000 0000	$11.79363\,3881 \pm 1.65232\,9728i$
3.00000 0000	$13.99235\,8137 \pm 2.51883\,0070i$
4.00000 0000	$16.73073\,7466 \pm 2.81262\,4894i$ $\Longleftarrow$
6.00000 6944	$19.50243\,9400 \pm 1.94033\,0347i$
8.00726 7603	
8.91725 0249	
20.84690 8101	

Note that the zeros for $1, 2, \ldots, 10$ remain real, as well as the zero for 20, but the zeros for $10, 11, 12, \ldots, 19$ become complex, and two of them (indicated by a left arrow) are shifted 2.81 units off the real axis.

(5) Forsythe's Example

If A is a square matrix and if there is some matrix X such that $AX = I$, then we know that $XA = I$. So fix A and vary X. If $AX - I$ is "small," by continuity $XA - I$ should also be "small." Let

$$A = \begin{pmatrix} 9999 & 9998 \\ 10000 & 9999 \end{pmatrix}.$$

The determinant of A is nonzero but "small." Let

$$\begin{pmatrix} 9999.9999 & -9997.0001 \\ -10001 & 9998 \end{pmatrix}.$$

A real computation (with no roundoff) yields

$$AX - I = \begin{pmatrix} .001 & .0001 \\ 0 & 0 \end{pmatrix},$$

but

$$XA - I = \begin{pmatrix} 19997.0001 & 19995.0003 \\ -19999 & -19995 \end{pmatrix}.$$

We will now describe a method for computing the eigenvalues of a matrix using complex analysis. Unfortunately it is not practical.

Say $z \mapsto f(z)$ is holomorphic on region Ω in $\mathbb{C}$. Then, it turns out that

$$\frac{1}{2\pi i} \int_{\partial\Omega} \frac{f'(z)}{f(z)} dz$$

is the number of zeros of f in Ω (an integer).

If A is an $n \times n$ matrix and if its characteristic polynomial is

$$\chi(A)(z) = z^n + a_1 z^{n-1} + \cdots + a_n,$$

we would like to know where to look for the roots of $\chi(A)$. If we let

$$K = |a_1| + \cdots + |a_n| + 1,$$

complex analysis shows that $z^n = 0$ and $\chi(A)(z) = 0$ have the same number of roots in any disk $|z| \leq B$, with $B \geq K$. This shows that $\chi(A)$ has all its roots in the disk $|z| \leq K$. We design a bisection algorithm that works as follows:

(1) First, draw the square enclosing the disk $|z| \leq K$.

(2) Bisect the square (say vertically); see Figure 2.1. Build in a subroutine for computing

$$\int_L R(z)dz,$$

where L is a line segment parallel to the x or y axis, and $R(z)$ is a rational function, up to $1/10$.

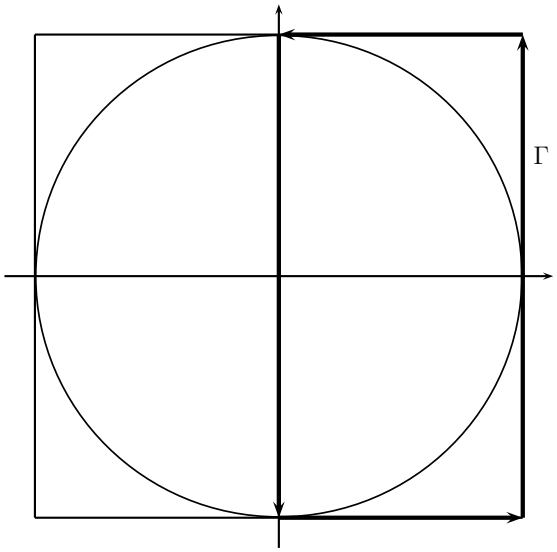


Figure 2.1: Bisection method to find roots of a polynomial

(3) Compute

$$\int_\Gamma \frac{\chi(A)'(z)}{\chi(A)(z)}dz,$$

along the polygonal boundary Γ of the current rectangle; see Figure 2.1. The error will be at at most $4/10 < 1/2$. Since the value of the integral is an integer, we will have the real answer. If the answer is ≥ 1, bisect horizontally, and if the answer is 0 ($< 1/2$), then bisect the left-hand rectangle horizontally.

(4) Repeat this process.

Critique.

1. $\chi(A)(z)$ has roundoff error problems.
2. Too many steps may be needed (2^r).

2.2 Square Matrices, Eigenvalues, QR-Factorization, and the QR-Algorithm

Let A be an $n \times n$ real invertible matrix. In order to find the eigenvalues of A, we try to find matrices Q and R so that

(1) $A = QR$.

(2) Q is orthogonal.

(3) R is upper triangular.

When $A = QR$ as above, we say that we have a *QR-factorization*. Write A_j for the jth column of A and Q_j for the jth column of Q. Given any $v \in \mathbb{R}^n$, let

$$\|v\| = \|v\|_2 = \sqrt{v_1^2 + \cdots + v_n^2}.$$

If we write out the equations given by $A = QR$ we get

$$\begin{aligned} C_1 &= r_{11}Q_1 \\ Q_2 &= r_{22}Q_2 + r_{12}Q_1 \\ &\vdots \\ C_n &= r_{nn}Q_n + r_{n-1n}Q_{n-1} + \cdots + r_{1n}Q_1, \end{aligned} \tag{$*_1$}$$

and since Q is orthogonal,

$$Q_i^\top Q_j = \delta_{ij}. \tag{$*_2$}$$

We show that Q and R satisfying the above equations can be obtained using the Gram–Schmidt orthonormalization procedure.

We begin by setting

$$Q_1' = C_1, \quad r_{11} = \|C_1\|,$$

and

$$Q_1 = \frac{1}{r_{11}} Q_1'.$$

This way, Q_1 is a unitary vector such that

$$C_1 = r_{11}.Q_1$$

Next, since

$$C_2 = r_{22}Q_2 + xQ_1,$$

if we want Q_1 and Q_2 to be orthogonal, we must have

$$Q_1^\top C_2 = r_{22}Q_1^\top Q_2 + xQ_1^\top Q_1 = x,$$

and so

$$x = Q_1^\top C_2.$$

Then, we get

$$r_{22}Q_2 = C_2 - (Q_1^\top C_2)Q_1,$$

and if we write

$$Q_2' = C_2 - (Q_1^\top C_2)Q_1, \quad r_{2,2} = \|Q_2'\|,$$

then

$$Q_2 = \frac{1}{r_{22}}Q_2'.$$

In general, we want Q_j orthogonal to $Q_1, \ldots, Q_{j-1}$, so we get

$$Q_j' = C_j - ((C_j^\top Q_{j-1})Q_{j-1} + \cdots + (C_j^\top Q_1)Q_1), \quad r_{jj} = \left\|Q_j'\right\|,$$

and

$$Q_j = \frac{1}{r_{jj}}Q_j'.$$

Note that

$$\mathrm{Span}(C_1, \ldots, C_j) = \mathrm{Span}(Q_1, \ldots, Q_j).$$

Therefore, Gram-Schmidt yields the desired QR-decomposition. Furthermore, it is easy to see that if the diagonal elements of R are required to be positive, then Q and R are unique.

Observe that

$$C_j = Q_j' + \underbrace{(C_j^\top Q_1)Q_1 + \cdots + (C_j^\top Q_{j-1})Q_{j-1}},$$

where the term in the underbrace is the Fourier series for C_j over $(Q_1, \ldots, Q_{j-1})$, and

$$Q_j = \frac{Q_j'}{\left\|Q_j'\right\|}.$$

Oberve that Q_j is the orthogonal projection of C_j onto the subspace spanned by $Q_1, \ldots, Q_{j-1}$. It turns out that in computing this projection P_j there are roundoff errors. A modified version of Gram–Schmidt has less roundoff errors.

Write $P(\perp v)$ for the orthogonal projection onto the orthogonal complement of $\mathrm{Span}(v)$. Observe that

$$P_j = P(\perp Q_{j-1}) \circ P(\perp Q_{j-2}) \circ \cdots \circ P(\perp Q_1).$$

The $P(\perp Q_i)$ are easier to compute and we obtain Q_j by the following iterative process:

$$\begin{aligned} Q_j^{(1)} &= P(\perp Q_1)C_j \\ Q_j^{(2)} &= P(\perp Q_2)Q_j^{(1)} \\ &\vdots \\ Q_j^{(j-1)} &= P(\perp Q_{j-1})Q_j^{(j-2)}, \end{aligned}$$

and $Q_j = Q_j^{(j-1)}$.

We now go back to our original problem: Given an invertible matrix A, find its eigenvalues. The *QR algorithm* due to JR Francis and Vera Kublanoskaya, independently (1960-1961), is one of the most remarkable algorithms and goes as follows:

(1) Factor A as $A = A_0 = Q_1 R_1$ (the QR factorization of A).

(2) Make
$$A_1 = R_1 Q_1,$$
and then compute a QR-factorization of A_1,
$$A_1 = Q_2 R_2$$

(3) Repeat step (2): Using $A_{i-1} = Q_i R_i$, make
$$A_i = R_i Q_i$$
and QR-factor A_i as
$$A_i = Q_{i+1} R_{i+1}.$$

Remarks:

(1) From $A_i = R_i Q_i$ we get $R_i = A_i Q_i^*$, and from $A_{i-1} = Q_i R_i$, we get
$$A_{i-1} = Q_i A_i Q_i^* = Q_i A_i Q_i^{-1}.$$
Therefore, A_i and A_{i-1} are similar, and thus A and A_i are similar for all i. Consequently, A_i has the same eigenvalues as A, including multiplicities.

(2) If A_i becomes upper triangular, then the eigenvalues of A are the diagonal elements of A_i.

(3) The method does not always converge. For example, if A is a unitary matrix, the method loops forever (in this case, $R = I$). Therefore, certain conditions on A are needed to ensure that the method converges. We will investigate this matter later on.

We now briefly review some basics about eigenvalues and eigenvectors. Our main goal is to prove that every (complex) matrix A can be factored as UTU^*, where U is unitary and T is upper triangular (the Schur form).

Eigenvalues and Eigenvectors

Given an $n \times n$ matrix A, the set of all the eigenvalues of A is the *spectrum* of A, denoted by $\mathrm{sp}(A)$. We let
$$\rho(A) = \max\{|\lambda| \mid \lambda \in \mathrm{sp}(A)\}$$

be the *spectral radius* of A. Given any eigenvalue λ of A, write

$$E_\lambda = \{v \in \mathbb{C}^n \mid Av = \lambda v\},$$

the *eigenspace* associated with λ. Except for the zero vector, all vectors in E_λ are eigenvectors for the eigenvalue λ. The dimension of E_λ, denoted by $\mathrm{geo}(\lambda)$, is the *geometric multiplicity* of λ.

The spectrum of A is the set of zeros of the characteristic polynomial of A,

$$\chi(A)(z) = \det(zI - A).$$

We have

$$\chi(A)(z) = z^n - \mathrm{tr}(A)z^{n-1} + \cdots + (-1)^n \det(A).$$

If we factor $\chi(A)(z)$, then we get

$$\chi(A)(z) = \prod_{\lambda \in \mathrm{sp}(A)} (z - \lambda)^{r(\lambda)},$$

where each $r(\lambda)$ is some positive integer called the *algebraic multiplicity* of λ. We also denote $r(\lambda)$ by $\mathrm{alg}(\lambda)$.

Proposition 2.1. *(Fundamental Inequality) If A is a square matrix, then for every eigenvalue $\lambda \in \mathrm{sp}(A)$, we have*

$$\mathrm{geo}(\lambda) \leq \mathrm{alg}(\lambda).$$

Proof. Pick any eigenvalue λ_1 of A and consider E_{λ_1}. Pick a basis of E_{λ_1} and extend it to a basis of $\mathbb{C}^n$. Let Q be the change of basis matrix (from the canonical basis). Then, with respect to this new basis, the matrix A becomes

$$Q^{-1}AQ = \begin{pmatrix} \lambda I & X \\ 0 & Y \end{pmatrix}.$$

Furthermore, we have

$$\begin{aligned} \chi(A)(z) &= \chi(Q^{-1}AQ)(z) \\ &= \det(zI - Q^{-1}AQ) \\ &= (z - \lambda_1)^{\mathrm{geo}(\lambda_1)} \det(zI - Y) \\ &= (z - \lambda_1)^{\mathrm{geo}(\lambda_1)} \chi(Y)(z). \end{aligned}$$

It follows that $(z - \lambda_1)^{\mathrm{geo}(\lambda_1)}$ divides $\chi(A)(z)$, which shows that $\mathrm{geo}(\lambda_1) \leq \mathrm{alg}(\lambda_1)$. □

Proposition 2.1 has the following useful consequences:

(I) If $\mathrm{alg}(\lambda) = 1$ for all $\lambda \in \mathrm{sp}(A)$, then A is diagonalizable.

This is because in this case, $\mathrm{geo}(\lambda) = \mathrm{alg}(\lambda)$ for all λ. But $\sum_\lambda \mathrm{alg}(\lambda) = n = \dim(A)$, so $\sum_\lambda \mathrm{geo}(\lambda) = n$ and then

$$\dim\Big(\coprod_\lambda E_\lambda\Big) = n,$$

which implies that

$$\mathbb{C}^n = \coprod_\lambda E_\lambda.$$

(II) If $\mathrm{geo}(\lambda) = \mathrm{alg}(\lambda)$ for all $\lambda \in \mathrm{sp}(A)$, then A is diagonalizable (the converse is clearly true).

The proof is the same as in case (I).

Question: Say Q is unitary and $Q^*AQ = D$ is diagonal. What can we say about A?

From $Q^*AQ = D$, we get $A = QDQ^*$, and because Q is unitary, we have

$$AA^* = QDQ^*QD^*Q^* = QDD^*Q^*,$$

and

$$A^*A = QD^*Q^*QDQ^* = QD^*DQ^*.$$

However, both D and D^* are diagonal matrices, so $DD^* = D^*D$, and we get

$$AA^* = A^*A.$$

In this case, we say that A is a *normal matrix*. Conversely, every normal matrix A can be diagonalized as $A = QDQ^*$, where Q is unitary. This is the *spectral theorem*.

As a special case, if A is Hermitian, which means that $A = A^*$, then A is diagonalizable. Furthermore, all the eigenvalues of A are real. This is because, from $A = QDQ^*$ we get

$$QDQ^* = A = A^* = QD^*Q^*,$$

which implies that $D = D^* = \overline{D}$, that is, D is real.

Unfortunately not every square matrix can be diagonalized, but if we relax the requirement of obtaining a similar diagonal matrix to obtaining a similar upper triangular matrix, then this is possible. In fact, Schur proved that for every complex matrix A, there is a unitary matrix U and an upper triangular matrix T such that

$$A = UTU^*.$$

This is called a *Schur factorization* of A.

Remark: The eigenvalue problem is equivalent with the problem of finding the roots of a polynomial. Since the eigenvalues of a matrix A are the zeros of its characteristic polynomial $\chi_A(z)$, a solution to the second problem obviously yields a solution of the first problem. Conversely, if $P(z)$ is any polynomial of degree n, we may assume that the leading coefficient is 1 so that

$$P(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_{n-1} z + a_n,$$

then we can make the *companion matrix*

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & -a_2 \\ 0 & 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

and a simple computation shows that the characteristic polynomial $\chi_A(z) = \det(zI - A)$ is equal to $P(z)$. Therefore, a method for finding the eigenvalues of the matrix A can be used to find the zeros of the polynomial $P(z) = \chi_A(z)$.

In 1819, NH Abel proved that for a "generic" quintic equation with coefficients in $\mathbb{Q}$, there exists a root which cannot be expressed as a finite combination of the coefficients using the operations $+, -, *, /$ and $\sqrt[k]{}$ (solution by radicals). Then, E. Galois (1832) gave a criterion for polynomials of degree n for when they could be solved by radicals. Galois associated to each P (of degree n) a subgroup $\mathrm{Gal}(P)$ of $\mathfrak{S}_n$ (in a canonical way) called the *Galois group* of P.

Galois's criterion: A polynomial $P(z)$ is solvable by radicals iff $\mathrm{Gal}(P)$ is a solvable group.

Abel showed that for $n = 5$, any generic P has $\mathrm{Gal}(P) = \mathfrak{S}_5$, but $\mathfrak{S}_5$ is not solvable. The conclusion is that the eigenvalue problem is not solvable by formulae involving radicals.

We now return to the Schur normal form.

Proposition 2.2. *Every square complex matrix A has a Schur decomposition*

$$A = UTU^*,$$

with U unitary and T upper triangular.

Proof. We proceed by induction on the dimension of A. The case $n = 1$ is trivial. If $n > 1$, let $\lambda_1 \in \mathbb{C}$ be any eigenvalue of A (it exists since $\mathbb{C}$ is algebraically closed). Using Gram-Schmidt, we can find an orthonormal basis consisting of a basis of the eigenspace E_{λ_1} and a basis of $E_{\lambda_1}^{\perp}$. Thus, there is a unitary matrix U_1 such that

$$U_1^* A U_1 = \begin{pmatrix} \lambda I & X \\ 0 & Y \end{pmatrix}.$$

By the induction hypothesis applied to Y, there is a unitary matrix U_2 such that

$$U_2^* Y U_2 = T_2$$

is an upper triangular matrix. Then, we have

$$\begin{pmatrix} I & 0 \\ 0 & U_2^* \end{pmatrix} \begin{pmatrix} \lambda I & X \\ 0 & Y \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & U_2 \end{pmatrix} = \begin{pmatrix} \lambda I & X \\ 0 & U_2^* Y \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & U_2 \end{pmatrix} = \begin{pmatrix} \lambda I & XU_2 \\ 0 & U_2^* Y U_2 \end{pmatrix} = \begin{pmatrix} \lambda I & XU_2 \\ 0 & T_2 \end{pmatrix}$$

Thus, if we let

$$U_3 = \begin{pmatrix} I & 0 \\ 0 & U_2 \end{pmatrix},$$

we have

$$U_3^* \begin{pmatrix} \lambda I & X \\ 0 & Y \end{pmatrix} U_3 = U_3^* U_1^* A U_1 U_3 = \begin{pmatrix} \lambda I & XU_2 \\ 0 & T_2 \end{pmatrix},$$

an upper triangular matrix. If we write $U = U_1 U_3$ and

$$T = \begin{pmatrix} \lambda I & XU_2 \\ 0 & T_2 \end{pmatrix},$$

we get

$$U^* A U = T,$$

with U unitary and T upper triangular, as claimed. □

Corollary 2.3. *(Spectral Theorem for Hermitian matrices) Every Hermitian matrix A can be diagonalized by a unitary matrix; that is*

$$A = UDU^*,$$

with U unitary and D diagonal. Furthermore, D is real.

Proof. Let $A = UTU^*$ be a Schur factorization of A. Since $A = A^*$, we get

$$UTU^* = UT^*U^*,$$

which implies $T = T^*$. However, since T is upper triangular, T^* is lower triangular, and the only way that $T = T^*$ is that T is a diagonal matrix D. Then $D = D^* = \overline{D}$, which shows that D is real. □

Let us go back to the QR factorization. We will show that there is a more stable way to obtain it using Householder reflections.

Observe that when we apply Gram–Schmidt (or modified Gram–Schmidt), we alter the columns seriatum leaving the previously altered ones alone. This means that we perform a

sequence of right multiplications by upper triangular matrices, and in the end we obtain a unitary matrix.

To avoid complications having to do with conjugation, let us consider real matrices. We can try to operate on the rows by orthogonal matrices. We would like to find an orthogonal matrix Q such that QA is upper triangular, and do this in a stepwise fashion. So, if we have a matrix A_k of the form

$$A_k = \begin{pmatrix} * & * & * & \cdots & * & u_1^k & \cdots & * \\ 0 & * & * & \cdots & * & u_2^k & \cdots & * \\ 0 & 0 & * & \cdots & * & u_3^k & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & * & u_{k-1}^k & \cdots & * \\ 0 & 0 & 0 & \cdots & 0 & u_k^k & \cdots & * \\ 0 & 0 & 0 & \cdots & 0 & u_{k+1}^k & \cdots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & u_n^k & \cdots & * \end{pmatrix}$$

where the left upper triangular block has size $(k-1) \times (k-1)$, we would like to multiply on the left by some orthogonal matrix to zero the entries $u_{k+1}^k, \ldots, u_n^k$ in the kth column and preserve the $k-1$ rows that we already have. This can be done using a hyperplane reflection, and such a method was found by Householder (1958).

If $u_{k+1}^k = \cdots = u_n^k = 0$, then $H_k = I$, else let

$$\begin{aligned} u_k'' &= (0, \ldots, 0, u_k^k, \ldots, u_n^k) \\ r_{kk} &= \|u_k''\|, \end{aligned}$$

and let H_k be the unique hyperplane reflection such that

$$H_k(u_k'') = r_{kk} e_k,$$

where $(e_1, \ldots, e_n)$ is the canonical basis of $\mathbb{R}^n$. The reflection H_k is uniquely determined by the hyperplane $\mathcal{H}_k$ orthogonal to $w_k = r_{kk} e_k - u_k''$. Since the first $k-1$ rows of A_k are linear combinations of $e_1, \ldots, e_{k-1}$, and since these vectors are orthogonal to w_k, they are invariant under the reflection H_k, as desired. Then, after n steps, we obtain

$$H_n H_{n-1} \cdots H_1 A = R,$$

where R is an upper triangular matrix and each H_i is a hyperplane reflection (or the identity). Observe that this works even if A is singular.

We claim that the hyperplane reflection H about a hyperplane orthogonal to a nonzero vector w is given by

$$H(u) = u - 2\frac{(u, w)}{\|w\|^2} w, \quad u \in \mathbb{R}^n.$$

We just need to find the orthogonal projection of u onto w. If we write

$$u = u' + \lambda w,$$

where u' is orthogonal to w, then we get

$$(u, w) = (u', w) + \lambda(w, w) = \lambda(w, w),$$

which yields

$$\lambda = \frac{(u, w)}{\|w\|^2}.$$

Then, it is geometrically obvious that

$$H(u) = u - 2\lambda w = u - 2\frac{(u, w)}{\|w\|^2}w.$$

The matrix corresponding to H is

$$H_w = I - 2\frac{ww^\top}{w^\top w},$$

since

$$H_w u = u - 2\frac{ww^\top}{w^\top w}u = u - 2\frac{w^\top u}{w^\top w}w.$$

The matrix $H_w = I - 2\frac{ww^\top}{w^\top w}$ is a *Householder reflection*. It is both orthogonal and symmetric.

Remark: Since the Householder reflection associated with w_k involves division by $\|w_k\|^2$, for numerical stability we want to make sure that $\|w_k\|$ is not too small, so it may be preferable to pick

$$w_k = r_{kk}e_k + u''_k$$

instead of $w_k = r_{kk}e_k - u''_k$ to maximize $\|w_k\|$. This amounts to picking

$$r_{kk} = -\|u''_k\|,$$

and in this case, some diagonal entries of R may be negative.

In the complex (Hermitian) case, we have the additional complication that if u and v are two distinct nonzero vectors such that $\|u\| = \|v\|$, unlike the Euclidean case, there may not be any reflection H such that $H(u) = v$. This is true only if the Hermitian inner product (u, v) is real. We can salvage the situation by multiplying by a suitable complex number. Specifically, if $(u, v) = e^{i\theta}|(u, v)|$ (and $\|u\| = \|v\|$), then the reflection H_w determined by the vector $w = v - e^{-i\theta}u$ has the property that

$$H_w(u) = e^{i\theta}v.$$

If we use this trick, we obtain a triangular matrix

$$R = H_n H_{n-1} \cdots H_1 A$$

whose diagonal entries are of the form $e^{i\theta_j} r_{jj}$, with $r_{jj} > 0$. We leave the details as an exercise.

Is it possible to achieve the Schur normal form of a matrix $A = QTQ^*$ using Householder reflections?

As a first attempt, use an orthogonal matrix Q to zero all entries below a_{11} in the first column of A. If

$$QA = \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & * \cdots & * \end{pmatrix},$$

then forming QAQ^* will change the first column, so this doesn not work. If we ask for less, namely, for $j = 1, \ldots, n$, to zero the entries a_{ij} for which $i \geq j+2$, then we succeed. Indeed, using a Householder reflection Q_1 we can zero all the entries below a_{21} obtaining

$$Q_1 A = \begin{pmatrix} * & * & \cdots & * \\ * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & * \cdots & * \end{pmatrix}.$$

This time, when we multiply on the right by Q_1^*, since Q_1 leaves the first row alone, Q_1^* leaves the first column alone, so we obtain a matrix of the form

$$Q_1 A Q_1^* = \begin{pmatrix} * & * & \cdots & * \\ * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & * \cdots & * \end{pmatrix}.$$

Next, we can use a Householder reflection Q_2 to zero all the entries in the second column for which $i \geq 4$, and since Q_2 leaves the first two rows alone, Q_2^* leaves the first two columns alone. We get a matrix of the form

$$Q_2 Q_1 A Q_1^* Q_2^* = \begin{pmatrix} * & * & \cdots & * \\ * & * & \cdots & * \\ 0 & * & \cdots & * \\ 0 & 0 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & * \cdots & * \end{pmatrix}.$$

Continuing in this fashion, we obtain a matrix R with

$$R = Q_{n-2}\cdots Q_2Q_1AQ_1^*Q_2^*\cdots Q_{n-2}^* = \begin{pmatrix} * & * & * & \cdots & * & * & * \\ * & * & * & \cdots & * & * & * \\ 0 & * & * & \cdots & * & * & * \\ 0 & 0 & * & \ddots & * & * & * \\ 0 & 0 & 0 & \ddots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & * & * \end{pmatrix},$$

such that $r_{ij} = 0$ for $j = 1, \ldots, n$ and $j + 2 \leq i \leq n$. In other words, R has zeros below the second diagonal. We say that R is a matrix in *Hessenberg form*. Thus, we showed that for every real matrix A, there is a sequence of Householder reflections whose composition Q yields

$$A = Q^*RQ,$$

with R a Hessenberg matrix. Observe that if A is a symmetric matrix, then R is a tridiagonal matrix.

2.3 More on Conditioning and Stability

Recall that a problem is a function $f\colon D \to S$, from the data space D to the problem space S. Say $x \in D$ and δx is a small perturbation of x. What happens to $f(x)$?

As in calculus, let

$$\delta f = f(x + \delta x) - f(x).$$

The numerical measure of changing the solution is

$$\lim_{\delta \mapsto 0} \sup_{\|\delta x\| \leq \delta} \frac{\|\delta f\|}{\|\delta x\|} = \kappa_f(x).$$

This quantity is the *conditioning number of the problem f at x*. In floating point arithmetic, we are interested in relative errors. So we divide by $\|f(x)\| / \|x\|$, and we get the *relative condition number of the problem f at x*,

$$\kappa_{f,\mathrm{rel}}(x) = \lim_{\delta \mapsto 0} \sup_{\|\delta x\| \leq \delta} \frac{\|\delta f\|}{\|f(x)\|} \Big/ \frac{\|\delta x\|}{\|x\|}.$$

Examples

(1) (Silly example) Let $D = S = \mathbb{C}$, and $f(x) = \lambda x$, for some $\lambda \in \mathbb{C}$. We have

$$\delta f = f(x + \delta x) - f(x) = \lambda x + \lambda\delta x - \lambda x = \lambda\delta x,$$

so

$$\frac{\|\delta f\|}{\|x\|} = |\lambda|,$$

and then

$$\kappa_f(x) = |\lambda|,$$

independently of x. We also have

$$\frac{\|\delta f\|}{\|f(x)\|} = \frac{|\lambda|\,\|\delta x\|}{|\lambda|\,\|x\|} = \frac{\|\delta x\|}{\|x\|},$$

which yields

$$\frac{\|\delta f\|}{\|f(x)\|} \Big/ \frac{\|\delta x\|}{\|x\|} = 1,$$

and so

$$\kappa_{f,\mathrm{rel}}(x) = 1,$$

independently of x.

(2) $D = S = \mathbb{C}$, $f(x) = \sqrt[k]{x}$.

The above is a particular example of a differentiable function f, so we consider this case. For δx small enough, we have

$$f(x + \delta x) = f(x) + Df_x(\delta x) + o(\delta x),$$

where Df_x is a linear map from D to S, that is,

$$\delta f = Df_x(\delta x) + o(\delta x).$$

From this, we deduce the inequalities

$$\|Df_x(\delta x)\| - \|o(\delta x)\| \leq \|\delta f\| \leq \|Df_x(\delta x)\| + \|o(\delta x)\|\,,$$

and so

$$\frac{\|Df_x(\delta x)\|}{\|\delta x\|} - \frac{\|o(\delta x)\|}{\|\delta x\|} \leq \frac{\|\delta f\|}{\|\delta x\|} \leq \frac{\|Df_x(\delta x)\|}{\|\delta x\|} + \frac{\|o(\delta x)\|}{\|\delta x\|}.$$

These inequalities are preserved by sup, which implies that when we take the limit

$$\lim_{\delta \mapsto 0} \sup_{\|\delta x\| \leq \delta}$$

we obtain

$$\kappa_f(x) = \lim_{\|\delta x\| \mapsto 0} \frac{\|Df_x(\delta x)\|}{\|\delta x\|}.$$

Now, if L is any linear map over a finite dimensional space, then L is continuous so the quantity

$$\sup_{\|x\|=1} \|L(x)\|$$

is well defined and is achieved for some x (by compactess of the unit sphere). For any $x \neq 0$, we have $x = \|x\| \widehat{x}$ with

$$\widehat{x} = \frac{x}{\|x\|},$$

a unit vector, which implies that for any $x \neq 0$,

$$\frac{\|L(x)\|}{\|x\|} = \|L(\widehat{x})\|,$$

and this shows that

$$\sup_{x \neq 0} \frac{\|L(x)\|}{\|x\|} = \sup_{\|x\|=1} \|L(x)\|.$$

The above quantity is the *operator norm* (or *subordinate norm*) of L, and it is denoted by $\|L\|$. Therefore, we proved that

$$\kappa_f(x) = \|Df_x\|.$$

It follows that

$$\kappa_{f,\mathrm{rel}}(x) = \|Df_x\| \Big/ \frac{\|f(x)\|}{\|x\|}.$$

Back to $f(x) = \sqrt[k]{x}$. We have

$$Df_x = f'(x) = \frac{1}{k} x^{\frac{1}{k}-1} = \frac{1}{k} \frac{\sqrt[k]{x}}{x},$$

and so

$$\kappa_f(x) = \frac{1}{k} \frac{\sqrt[k]{|x|}}{|x|}.$$

Observe that $\kappa_f(x)$ is very large if x is small. On the other hand,

$$\kappa_{f,\mathrm{rel}}(x) = \frac{1}{k} \frac{\sqrt[k]{|x|}}{|x|} \Big/ \frac{\sqrt[k]{|x|}}{|x|} = \frac{1}{k},$$

which is independent of x. In conclusion, $k_f(x)$ is ill-conditioned near 0, and $\kappa_{f,\mathrm{rel}}(x)$ is well conditioned for all x.

(3) $D = \mathbb{C}^2$, $S = \mathbb{C}$, $f(x_1, x_2) = x_1 - x_2$.

We have

$$Df(x) = (1, -1),$$

and so

$$\|Df(x)\| = \max \left| \frac{\partial f}{\partial x_j}(x_1, x_2) \right| \dim(D) = 2.$$

It follows that

$$\kappa_f(x) = 2,$$

and f is well-conditioned. On the other hand,

$$\kappa_{f,\mathrm{rel}}(x) = \frac{2\sqrt{x_1^2 + x_2^2}}{|x_1 - x_2|} = 2\frac{\|x\|_2}{|x_1 - x_2|}.$$

If $x_1 - x_2$ is very small, that is, $x_1 \approx x_2$, then $\kappa_{f,\mathrm{rel}}(x)$ is big. Thus, f is relatively ill-conditioned. This is a cancellation problem.

(4) Eigenvalue problems are ill-conditioned in general. Let

$$A = \begin{pmatrix} 1 & 1000 \\ 0 & 1 \end{pmatrix}.$$

The eigenvalues of A are both 1. Yet, if we change A a little bit to

$$B = \begin{pmatrix} 1 & 1000 \\ 0.001 & 1 \end{pmatrix},$$

then $\det(B) = 0$ and the eigenvalues are 0 and 2.

(5) Wilkinson's polynomial,

$$P(x) = \prod_{j=1}^{20}(x - j).$$

The sixteenth root is sensitive. Say

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Fact. If we change only the ith coefficient of P by δa_i, then the change in the jth root is

$$-\frac{(\delta a_i)x_j^i}{P'(x_j)}.$$

If $f(P) = j$th root of P, then

$$\kappa_f(P) = \frac{|\delta a_i||x_j|^i}{|P'(x_j)||\delta a_i|} = \frac{|x_j|^i}{|P'(x_j)|},$$

and

$$\kappa_{f,\mathrm{rel}}(P) = \frac{|x_j|^i}{|P'(x_j)|} \Big/ \frac{|x_j|}{\|P\|} = \frac{\|P\|}{|P'(x_j)|}|x_j|^{i-1}.$$

The quantity $\kappa_{f,\mathrm{rel}}(P)$ can be very large.

(6) The condition number of a matrix. Let A be an $m \times m$ complex matrix, let $D = \mathbb{C}^m$, $S = \mathbb{C}^m$. We have

$$A(x + \delta x) - Ax = A\delta x,$$

and so

$$\kappa_{A,\mathrm{rel}} = \lim_{\delta \mapsto 0} \sup_{\|\delta x\| \leq \delta} \frac{\|A\delta x\|}{\|\delta x\|} \Big/ \frac{\|Ax\|}{\|x\|} = \|A\| \frac{\|x\|}{\|Ax\|}.$$

If A^{-1} exists, then

$$x = A^{-1}Ax,$$

which implies that

$$\|x\| \leq \left\|A^{-1}\right\| \|Ax\|,$$

and so

$$\frac{\|x\|}{\|Ax\|} \leq \left\|A^{-1}\right\|.$$

Therefore, we get

$$\kappa_{A,\mathrm{rel}} \leq \|A\| \left\|A^{-1}\right\|.$$

The number $\kappa(A) = \|A\| \|A^{-1}\|$ is called the *condition number* of the matrix A. If A is not invertible, we agree that $\kappa(A) = \infty$.

Look at the two problems:

1. Given, x, find y such that $y = Ax$.
2. Given y, find x such that $Ax = y$, which is equivalent to $A^{-1}y = x$.

We find that

1. The first problem has condition number

$$\kappa_{\mathrm{rel}}(x) = \|A\| \frac{\|x\|}{\|y\|},$$

2. The second problem has condition number

$$\kappa_{\mathrm{rel}}(y) = \left\|A^{-1}\right\| \frac{\|y\|}{\|x\|}.$$

In both cases, we have

$$\kappa_{\mathrm{rel}} \leq \kappa(A).$$

For example, if $A = H_n$, the Hilbert matrix, then $\kappa(H_n)$ is enormous. In fact, the following proposition holds:

Proposition 2.4. *Suppose $f\colon D \to S$ is a problem and $\widetilde{f}$ is a backwardly stable algorithm to compute f. Then,*

$$\frac{\left\|\widetilde{f}(x) - f(x)\right\|}{\|f(x)\|} = O(\kappa_{f,\mathrm{rel}}(x) \cdot \epsilon_{\mathrm{machine}}).$$

Proof. Because $\widetilde{f}$ is backwardly stable, there is some $\widetilde{x}$ such that $f(\widetilde{x}) = \widetilde{f}(x)$, where

$$\frac{\|\widetilde{x} - x\|}{\|x\|} = O(\epsilon_{\text{machine}}).$$

Then, we have

$$\widetilde{f}(x) - f(x) = f(\widetilde{x}) - f(x) = \delta f,$$

and for $\|\widetilde{x} - x\| \leq \delta$,

$$\kappa_{f,\text{rel}}(x) = \lim_{\delta \mapsto 0} \sup_{\|\delta x\| \leq \delta} \frac{\|\delta f\|}{\|\delta x\|} \Big/ \frac{\|f(x)\|}{\|x\|} = \lim_{\delta \mapsto 0} \sup_{\|\delta x\| \leq \delta} \frac{\|\delta f\|}{\|f(x)\|} \Big/ \frac{\|x\|}{\|\delta x\|},$$

which implies that

$$\frac{\left\|\widetilde{f}(x) - f(x)\right\|}{\|f(x)\|} \leq (\kappa_{f,\text{rel}}(x) + o(1))(O(\epsilon_{\text{machine}})).$$

The righthand side is $O(\kappa_{f,\text{rel}}(x) \cdot \epsilon_{\text{machine}})$, as claimed. □

As an application of Proposition 2.4, consider the problem of computing $\sin(\frac{\pi}{2} - \delta)$ for $\delta > 0$ small. Let

$$x = \frac{\pi}{2} - \delta$$

and suppose that $\widetilde{f}(x) = \text{fl}(\sin x)$. Is the algorithm $\widetilde{f}$ backwardly stable?

If so, there is some $\widetilde{x}$ such that $\widetilde{f}(x) = f(\widetilde{x})$ with

$$\frac{\|\widetilde{x} - x\|}{\|x\|} = O(\epsilon_{\text{machine}}).$$

Using calculus, we have

$$f(\widetilde{x}) - f(x) = f'(x)(\widetilde{x} - x) + O((\widetilde{x} - x)^2).$$

Since

$$f'(x) = \cos x = \cos\left(\frac{\pi}{2} - \delta\right)$$

and

$$\cos\left(\frac{\pi}{2} - \delta\right) = cos\frac{\pi}{2}\cos\delta + \sin\frac{\pi}{2}\sin\delta = \sin\delta \approx \delta,$$

we get

$$f(\widetilde{x}) - f(x) \approx \delta(\widetilde{x} - x) + O((\widetilde{x} - x)^2). \qquad (*)$$

By assumption, $f(\widetilde{x}) = \widetilde{f}(x) = \text{fl}(\sin x)$ and $f(x) = \sin x$. This implies that

$$\|f(\widetilde{x}) - f(x)\| = O(\epsilon_{\text{machine}}),$$

and if we divide $(*)$ by δ, we get

$$\frac{\left\|\widetilde{f}(x) - f(x)\right\|}{\delta} = \|\widetilde{x} - x\| + \text{small error}.$$

The lefthand side is $O(\epsilon_{\text{machine}})/\delta$. Thus, if δ is small, then

$$\|\widetilde{x} - x\| \neq O(\epsilon_{\text{machine}})\,\|x\|\,,$$

a contradiction. Therefore, $\widetilde{f}$ is not backwardly stable.

2.4 Rayleigh Quotient and Power Iteration

In this section, we assume that A is a square, real, symmetric matrix. In this case, A has real eigenvalues that can be ordered according to their absolute values,

$$|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_n|,$$

and A can be diagonalized with respect to an orthornormal basis of eigenvectors $(e_1, \ldots, e_n)$.

Definition 2.1. The *Rayleigh quotient of A at x ($x \neq 0$)* is

$$r(x) = \frac{x^\top Ax}{x^\top x} = \frac{(Ax, x)}{(x, x)}.$$

The following properties hold:

(1) $r(\lambda x) = r(x)$, for all $\lambda \neq 0$. Consequently, we may assume that $\|x\| = 1$.

(2) If y is an eigenvector of A for λ, then $(Ay, y) = \lambda(y, y)$, and so

$$r(y) = \lambda.$$

We can consider r as a function on the unit sphere S^{n-1}. The function r is smooth on S^{n-1}. Pick x on S^{n-1} and look at $r(x)$ near x. We need $Dr(x)$, the derivative of r at x. Thus, we need to compute the partial derivatives, $\partial r/\partial x_j$. We have

$$\frac{\partial r}{\partial x_j} = \frac{(x, x)\frac{\partial (Ax, x)}{\partial x_j} - \frac{\partial (x, x)}{\partial x_j}(Ax, x)}{(x, x)^2}.$$

Say $x = \sum_{j=1}^n x_j e_j$, then

$$Ax = \sum_{j=1}^n x_j Ae_j,$$

and

$$\begin{aligned}\frac{\partial(Ax,x)}{\partial x_j} &= \left(\frac{\partial Ax}{\partial x_j},x\right)+\left(Ax,\frac{\partial x}{\partial x_j}\right)\\ &= (Ae_j,x)+(Ax,e_j)\\ &= 2(Ax,e_j).\end{aligned}$$

Since the basis is orthonormal, if $Ax=\sum_i a_i e_i$, we have

$$\frac{\partial(Ax,x)}{\partial x_j}=2a_j,$$

and we also have

$$\begin{aligned}\frac{\partial(x,x)}{\partial x_j} &= \left(\frac{\partial x}{\partial x_j},x\right)+\left(x,\frac{\partial x}{\partial x_j}\right)\\ &= (e_j,x)+(x,e_j)\\ &= 2(x,e_j)=2x_j.\end{aligned}$$

It follows that

$$\frac{\partial r}{\partial x_j}=\frac{2}{(x,x)}(a_j-x_j r(x)),$$

and thus

$$Dr(x)=\frac{2}{(x,x)}(Ax-r(x)x).$$

The critical points of r are given by $Dr(x)=0$, that is,

$$Ax=r(x)x,\quad x\neq 0.$$

Therefore, the critical points of r are the eigenvalues of A and the corresponding critical values are the corresponding eigenvalues (by (2) above).

The Taylor series of r near a critical point is given by

$$r(y)=r(x)+Dr(x)(y-x)+(y-x)^\top H(\xi)(y-x),$$

where $H(\xi)$ is the Hessian of r at some point ξ near x and y. In conclusion, near a critical point, we have

$$|r(y)-r(x)|=|r(y)-\lambda|=O(\|y-x\|^2).$$

Power Iteration

Given $x\neq 0$, look at the sequence

$$x,Ax,A^2x,\ldots,A^mx,\ldots,$$

and at the sequence of normalized vectors

$$\frac{A^m x}{\|A^m x\|}.$$

Nomenclatrure: The *kth Krylov subspace* from A and x, denoted by $K_k(A;x)$, is the subspace spanned by $(x, Ax, \ldots, A^k x)$.

Assume that $|\lambda_1| > |\lambda_2| \geq \cdots \geq |\lambda_n|$. Compute $A^k x$ using a basis of eigenvectors $(e_1, \ldots, e_n)$. If $x = \sum_j a_j e_j$, then

$$Ax = \sum_j a_j \lambda_j e_j,$$

and we get

$$A^m x = \sum_j a_j \lambda_j^m e_j,$$

which yields

$$\begin{aligned}\frac{A^m x}{\|A^m x\|} &= \frac{\frac{1}{\lambda_1^m} A^m x}{\frac{1}{\lambda_1^m}\|A^m x\|} \\ &= \frac{\sum_j a_j \left(\frac{\lambda_j}{\lambda_1}\right)^m e_j}{\sqrt{\sum_j a_j^2 \left(\frac{\lambda_j}{\lambda_1}\right)^{2m}}},\end{aligned}$$

and as m goes to infinity, since $|\lambda_1| > |\lambda_j|$ for $j = 2, \ldots, n$, the limit is

$$a_1 \frac{e_1}{|a_1|} = \pm e_1.$$

We can also estimate the rate of convergence. If we let

$$x_k = \frac{A^k x}{\|A^k x\|},$$

then the above implies that

$$\left\|A^k x\right\| = |a_1||\lambda_1|^k O\left(\left|\frac{\lambda_2}{\lambda_1}\right|^k\right),$$

and so

$$\|x_k - \pm e_1\| = O\left(\left|\frac{\lambda_2}{\lambda_1}\right|^k\right), \qquad (*)$$

and finally

$$|r(x^k) - \lambda_1| = O\left(\left|\frac{\lambda_2}{\lambda_1}\right|^{2k}\right). \qquad (**)$$

The next question is: what do we do to improve the speed of convergence of power iteration?

Here is an idea: pick a number μ and suppose that it is close to an eigenvalue λ of A. If μ is distinct from all the eigenvalues of A, then $A - \mu I$ is invertible, so let $B = (A - \mu I)^{-1}$. Say x is an eigenvector of B for some eigenvalue $\xi \neq 0$. If so, $Bx = \xi x$, that is,

$$x = (A - \mu)\xi x,$$

which yields

$$(1 + \mu\xi)x = \xi A x.$$

It follows that x is an eigenvector of A for the eigenvalue

$$\lambda = \frac{1 + \mu\xi}{\xi},$$

and then

$$1 + \mu\xi = \lambda\xi,$$

so

$$\xi = \frac{1}{\lambda - \mu}.$$

In summary: The eigenvectors of B are equal to those of A, and if λ is an eigenvalue of A, then $1/(\lambda - \mu)$ is an eigenvalue of B. Also, if μ is close to λ, then $1/(\lambda - \mu)$ is large, and if μ is closest to λ than to any other eigenvalue λ' of A, then

$$|\lambda - \mu| < |\lambda' - \mu| \quad \text{for all } \lambda' \neq \lambda,$$

so

$$\frac{1}{|\lambda - \mu|} > \frac{1}{|\lambda' - \mu|} \quad \text{for all } \lambda' \neq \lambda,$$

and then power iteration applied to $B = (A - \mu I)^{-1}$ converges to an eigenvector e corresponding to λ. We also have

$$\left\|x^k - \pm e\right\| = O\left(\left|\frac{\lambda - \mu}{\lambda' - \mu}\right|^{k}\right),$$

and

$$|r(x^k) - \lambda| = O\left(\left|\frac{\lambda - \mu}{\lambda' - \mu}\right|^{2k}\right).$$

The above method is the *inverse power iteration method*.

Power iteration and inverse power iteration can be used together to yield an effective iterative method for computing eigenvalues and eigenvectors. Look at the diagram in Figure 2.2:

Repeat these steps seriatum alternately; use $r(x^{k-1})$ instead of the previous guess of eigenvalue when doing iteration and use the better vectors starting vector in either itreration steps.

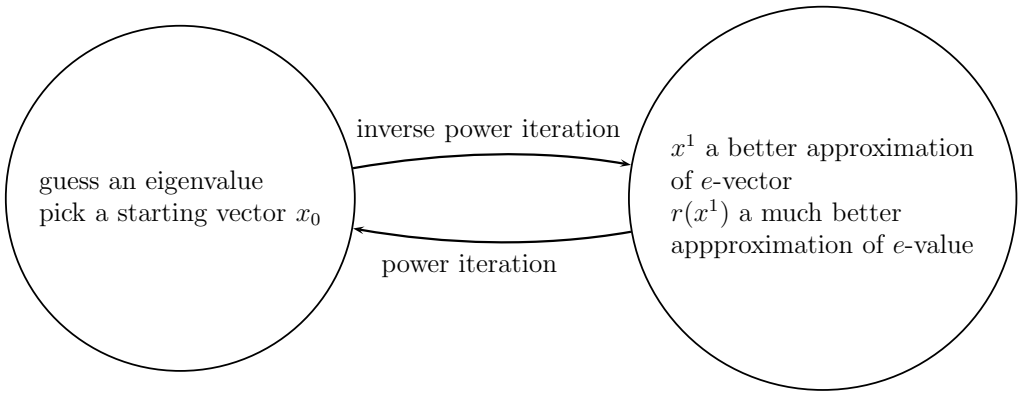


Figure 2.2: Rayleigh quotient iteration

Remark: To compute x^1 we apply $B = (A - \mu I)^{-1}$, that is, we solve

$$(A - \mu I)x^1 = x^0$$

for x^1. This is ill conditioned if μ is close to λ. Remarkably, in practice this does not matter! Also, if

$$\left\|x^k - \pm e\right\| = O(\epsilon),$$

then

$$|r(x^k) - \lambda| = O(\epsilon^2).$$

From $(*)$ and $(**)$, it can be shown that if the iteration converges, then

$$\left\|x^{k+1} - \pm e\right\| = O(\left\|x^k - \pm e\right\|^3)$$

and

$$\left\|r(x^{k+1}) - \lambda\right\| = O(\left\|r(x^k) - \lambda\right\|^3).$$

This is a very fast convergence rate.

2.5 Back to the QR-Algorithm

Recall the QR algorithm for finding the eigenvalues of a (symmetric) matrix: First, factor $A^{(0)} = A$ as

$$A^{(0)} = Q^{(1)}R^{(1)}$$

(say by Householder reflection) and then make

$$A^{(1)} = R^{(1)}Q^{(1)}.$$

In general, factor $A^{(k)}$ as

$$A^{(k)} = Q^{(k+1)}R^{(k+1)}$$

and make

$$A^{(k+1)} = R^{(k+1)}Q^{(k+1).}$$

Since, $Q^{(k+1)} = A^{(k)}(R^{(k+1)})^*$, we have

$$A^{(k+1)} = R^{(k+1)}A^{(k)}(R^{(k+1)})^*,$$

which shows that $A^{(k)}$ and $A^{(k+1)}$ have the same spectrum, and thus that A and $A^{(k)}$ have the same spectrum for all k.

The "practical algorithm" consists of the following steps:

(0) Use Householder reflections to convert A to Hessenberg form (tridiagonal if A is Hermitian); call this matrix $A^{(0)}$.

(1) Pick a good *shift* μ_1, and QR factor $A^{(0)} - \mu_1 I$ as

$$A^{(0)} - \mu_1 I = Q^{(1)}R^{(1)}.$$

(2) Make

$$A^{(1)} = R^{(1)}Q^{(1)} + \mu_1 I.$$

Repeat (1) and (2). Usually, we pick $\mu_k = A^{(k)}_{mm}$. Observe that

$$Q^{(1)}A^{(1)}(Q^{(1)})^* = Q^{(1)}(R^{(1)}Q^{(1)} + \mu_1 I)(Q^{(1)})^* = Q^{(1)}R^{(1)} + \mu_1 I = A^{(0)},$$

which shows that $A^{(0)}$ and $A^{(1)}$ have the same spectrum, and similarly $A^{(0)}$ and $A^{(k)}$ have the same spectrum for all k.

(3) (Deflation) If $A^{(k)}$ has some very small lower off diagonal entry $A^{(k)}_{j+1j}$, then replace $A^{(k)}$ by the matrix which has $A^{(k)}_{j+1j} = 0$ to get a new matrix of the form

$$\begin{pmatrix} B & * \\ 0 & C \end{pmatrix}$$

and run the shifted QR algorithm separately on B and C.

The above method is the QR algorithm with shift.

To analyze the convergence of the above method, assume that A is Hermitian and forget about the shifts. Let $(e_1, \ldots, e_m)$ be an orthonormal basis of eigenvectors for A. Let $X^{(0)}$ be an invertible $m \times m$ matrix whose jth column is a vector of the form

$$x_j^{(0)} = \sum_{i=1}^{m} a_{ij} e_i.$$

Write Q for the matrix whose columns are $e_1, \ldots, e_m$ and look at $Q^\top X^{(0)}$. Observe that

$$(Q^\top x_j^{(0)})_l = (e_l, x_j^{(0)}) = a_{lj}.$$

Recall that the principal k minor of a $m \times m$ matrix $A = (a_{ij})$ is the matrix (a_{ij}), with $1 \leq i, j \leq k$ and $1 \leq k \leq m$.

Theorem 2.5. *If A is a real symmetric matrix, Q is an orthogonal matrix consisting of an orthonormal basis of eigenvectors of A, and if*

(1) $X^{(0)}$ is any matrix such that $Q^\top X^{(0)}$ and all its principal minors are nonsingular

(2) $|\lambda_1| > |\lambda_2| > \cdots > |\lambda_m|$, where $\lambda_1, \ldots, \lambda_m$ are the eigenvalues of A, and if

$$A^{(k)} X^{(0)} = Q^{(k)} R^{(k)},$$

is a QR decomposition of $A^{(k)} X^{(0)}$,

then the sequence $(Q^{(k)})$ converges linearly to Q and the diagonal entries of $R^{(k)}$ converge linearly to the eigenvalues of A.

Sketch of proof. We have $A = Q\Lambda Q^\top$ where Λ is a diagonal matrix and Q is orthogonal. It follows that

$$A^k = Q\Lambda^k Q^\top.$$

Let $l \leq m$ and for any $m \times m$ matrix B write B_l for the principal l-minor of B augmented by 1s down the diagonal. We have

$$A^k X^{(0)} = Q\Lambda^k Q^\top X^{(0)},$$

and so

$$\begin{aligned}
(A^k X^{(0)})_l &= Q_l \Lambda_l^k (Q^\top X^{(0)})_l, \\
&= (Q\Lambda^k)_l Q_l^\top X^{(0)} + O(\lambda_{l+1}^k) \\
&= (Q\Lambda^k)_l Q_l^\top X^{(0)} + O(\lambda_{l+1}^k)(Q_l^\top X^{(0)})^{-1} Q_l^\top X^{(0)} \\
&= [(Q\Lambda^k)_l + O(\lambda_{l+1}^k)] Q_l^\top X^{(0)}.
\end{aligned}$$

Since $Q_l^\top X^{(0)}$ is nonsingular, the column space of $(A^k X^{(0)})_l$ is the same as the column space of $(Q\Lambda^k)_l + O(\lambda_{l+1}^k)$. Let

$$C = \max\left\{\left|\frac{\lambda_{j+1}}{\lambda_j}\right|, j = 1, \ldots, m-1\right\}.$$

By hypothesis, $C < 1$. For $l = 1$, the column space of $(A^k X^{(0)})_1 + O(|\lambda_2|^k)$ converges to the first column of Q in $O(C)$. By induction, all the column spaces of $Q\Lambda^k$ converge those of $A^k X^{(0)}$ in $O(C)$ as k goes to infinity. But, $Q\Lambda^k$ has the same column space as Q, so

$$\left\|(A^k X^{(0)})_j - \pm e_j\right\| = O(C).$$

□

In practice, there are too many roundoff errors so we normalize at each stage. Start with $X^{(0)}$, compute

$$X^{(1)} = AX^{(0)} = Q^{(1)}R^{(1)}.$$

Since A is invertible, so is $R^{(1)}$, thus $X^{(1)}$ and $Q^{(1)}$ have the same column space. Replace $X^{(1)}$ by $Q^{(1)}$. Keep going: let

$$AQ^{(k-1)} = Q^{(k)}R^{(k)}$$

and get $Q^{(k)}$. This method is the *simultaneous power iteration method* (SPI). It turns out that QR iteration is equivalent to simultaneous iteration applied to the identity matrix. To show this, we need to introduce some notation. Define the matrices $A^{(k)}$, $X^{(k)}$, $Q^{(k)}$, $\mathbf{Q}^{(k)}$ and $\mathbf{R}^{(k)}$ as follows:

$$\begin{aligned} A^{(0)} &= A \\ A^{(k-1)} &= Q^{(k)}R^{(k)} \\ A^{(k)} &= R^{(k)}Q^{(k)} \\ X^{(0)} &= \mathbf{Q}^{(0)} = I \\ AQ^{(k-1)} &= \mathbf{Q}^{(k)}\mathbf{R}^{(k)} \\ X^{(k)} &= \mathbf{Q}^{(k)}. \end{aligned}$$

We also define the matrices $\mathcal{A}^{(k)}$ and $\mathcal{R}^{(k)}$ by

$$\begin{aligned} \mathcal{A}^{(k)} &= \mathbf{Q}^{(k)}A(\mathbf{Q}^{(k)})^\top \\ \mathcal{R}^{(k)} &= \mathbf{R}^{(k)}\mathbf{R}^{(k-1)}\cdots\mathbf{R}^{(1)}. \end{aligned}$$

Proposition 2.6. *The following properties hold:*

1. $A^k = \mathbf{Q}^{(k)}\mathbf{R}^{(k)}$.
2. $\mathcal{A}^{(k)} = A^{(k)}$.
3. $\mathcal{R}^{(k)} = R^{(1)}\cdots R^{(k)}$.
4. $\mathbf{Q}^{(k)} = Q^{(1)}\cdots Q^{(k)}$.

Proof. By induction. □

2.6 Singular Value Decomposition (SVD)

Let A be a $p \times q$ complex matrix, and let S^{2q-1} be the unit sphere in $\mathbb{C}^q$, given by

$$S^{2q-1} = \{(z_1, \ldots, z_q) \in \mathbb{C}^q \mid |z_1|^2 + \cdots + |z_q|^2 = 1\}.$$

Recall that (for any norms on $\mathbb{C}^p$ and $\mathbb{C}^q$)

$$\|A\| = \sup_{\|x\|=1} \|Ax\|.$$

Because S^{2q-1} is compact, there is some $x \in \mathbb{C}^q$ such that

$$\|A\| = \|Ax\|,$$

and the image of S^{2q-1} under A is also compact, so geometrically AS^{2q-1} is an ellipsoid. Because A may not have full rank, this ellipsoid may be flat in certain directions. This can be easily handled using some linear algebra.

First, we prove that every square real matrix has an SVD. Stronger results can be obtained if we first consider the polar form and then derive the SVD from it (there are uniqueness properties of the polar decomposition). For our purposes, uniqueness results are not as important so we content ourselves with existence results, whose proofs are simpler. Readers interested in a more general treatment are referred to [6].

The early history of the singular value decomposition is described in a fascinating paper by Stewart [16]. The SVD is due to Beltrami and Camille Jordan independently (1873, 1874). Gauss is the grandfather of all this, for his work on least squares (1809, 1823) (but Legendre also published a paper on least squares!). Then come Sylvester, Schmidt, and Hermann Weyl. Sylvester's work was apparently "opaque." He gave a computational method to find an SVD. Schmidt's work really has to do with integral equations and symmetric and asymmetric kernels (1907). Weyl's work has to do with perturbation theory (1912). Autonne came up with the polar decomposition (1902, 1915). Eckart and Young extended SVD to rectangular matrices (1936, 1939).

Theorem 2.7. *(Singular value decomposition) For every real $n \times n$ matrix A there are two orthogonal matrices U and V and a diagonal matrix D such that $A = VDU^\top$, where D is of the form*

$$D = \begin{pmatrix} \sigma_1 & & \ldots & \\ & \sigma_2 & \ldots & \\ \vdots & \vdots & \ddots & \vdots \\ & & \ldots & \sigma_n \end{pmatrix},$$

where $\sigma_1, \ldots, \sigma_r$ are the singular values of f, i.e., the (positive) square roots of the nonzero eigenvalues of $A^\top A$ and $A\,A^\top$, and $\sigma_{r+1} = \cdots = \sigma_n = 0$. The columns of U are eigenvectors of $A^\top A$, and the columns of V are eigenvectors of $A\,A^\top$.

Proof. Since $A^\top A$ is a symmetric matrix, in fact, a positive semidefinite matrix, there exists an orthogonal matrix U such that

$$A^\top A = UD^2U^\top,$$

with $D = \mathrm{diag}(\sigma_1, \ldots, \sigma_r, 0, \ldots, 0)$, where $\sigma_1^2, \ldots, \sigma_r^2$ are the nonzero eigenvalues of $A^\top A$, and where r is the rank of A; that is, $\sigma_1, \ldots, \sigma_r$ are the singular values of A. It follows that

$$U^\top A^\top AU = (AU)^\top AU = D^2,$$

and if we let f_j be the jth column of AU for $j = 1, \ldots, n$, then we have

$$\langle f_i, f_j \rangle = \sigma_i^2 \delta_{ij}, \quad 1 \leq i, j \leq r$$

and

$$f_j = 0, \quad r+1 \leq j \leq n.$$

If we define $(v_1, \ldots, v_r)$ by

$$v_j = \sigma_j^{-1} f_j, \quad 1 \leq j \leq r,$$

then we have

$$\langle v_i, v_j \rangle = \delta_{ij}, \quad 1 \leq i, j \leq r,$$

so complete $(v_1, \ldots, v_r)$ into an orthonormal basis $(v_1, \ldots, v_r, v_{r+1}, \ldots, v_n)$ (for example, using Gram–Schmidt). Now, since $f_j = \sigma_j v_j$ for $j = 1 \ldots, r$, we have

$$\langle v_i, f_j \rangle = \sigma_j \langle v_i, v_j \rangle = \sigma_j \delta_{i,j}, \quad 1 \leq i \leq n,\ 1 \leq j \leq r$$

and since $f_j = 0$ for $j = r+1, \ldots, n$,

$$\langle v_i, f_j \rangle = 0 \quad 1 \leq i \leq n,\ r+1 \leq j \leq n.$$

If V is the matrix whose columns are $v_1, \ldots, v_n$, then V is orthogonal and the above equations prove that

$$V^\top AU = D,$$

which yields $A = VDU^\top$, as required.

The equation $A = VDU^\top$ implies that

$$A^\top A = UD^2U^\top, \quad AA^\top = VD^2V^\top,$$

which shows that $A^\top A$ and $AA^\top$ have the same eigenvalues, that the columns of U are eigenvectors of $A^\top A$, and that the columns of V are eigenvectors of $AA^\top$. □

Theorem 2.7 suggests the following definition.

Definition 2.2. A triple (U, D, V) such that $A = VDU^\top$, where U and V are orthogonal and D is a diagonal matrix whose entries are nonnegative (it is positive semidefinite) is called a *singular value decomposition (SVD) of* A.

The proof of Theorem 2.7 shows that there are two orthonormal bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, where $(u_1, \ldots, u_n)$ are eigenvectors of $A^\top A$ and $(v_1, \ldots, v_n)$ are eigenvectors of $AA^\top$. Furthermore, $(u_1, \ldots, u_r)$ is an orthonormal basis of $\operatorname{Im} A^\top$, $(u_{r+1}, \ldots, u_n)$ is an orthonormal basis of $\operatorname{Ker} A$, $(v_1, \ldots, v_r)$ is an orthonormal basis of $\operatorname{Im} A$, and $(v_{r+1}, \ldots, v_n)$ is an orthonormal basis of $\operatorname{Ker} A^\top$.

If we denote the columns of U by $u_1, \ldots, u_n$ and the columns of V by $v_1, \ldots, v_n$, then we can write

$$A = V D U^\top = \sigma_1 v_1 u_1^\top + \cdots + \sigma_r v_r u_r^\top.$$

As a consequence, if r is a lot smaller than n (we write $r \ll n$), we see that A can be reconstructed from U and V using a much smaller number of elements. This idea will be used to provide "low-rank" approximations of a matrix. The idea is to keep only the k top singular values for some suitable $k \ll r$ for which $\sigma_{k+1}, \ldots \sigma_r$ are very small.

Remarks:

(1) In Strang [18] the matrices U, V, D are denoted by $U = Q_2$, $V = Q_1$, and $D = \Sigma$, and an SVD is written as $A = Q_1 \Sigma Q_2^\top$. This has the advantage that Q_1 comes before Q_2 in $A = Q_1 \Sigma Q_2^\top$. This has the disadvantage that A maps the columns of Q_2 (eigenvectors of $A^\top A$) to multiples of the columns of Q_1 (eigenvectors of $A\,A^\top$).

(2) Algorithms for actually computing the SVD of a matrix are presented in Golub and Van Loan [7], Demmel [4], and Trefethen and Bau [19], where the SVD and its applications are also discussed quite extensively.

(3) The SVD also applies to complex matrices. In this case, for every complex $n \times n$ matrix A, there are two unitary matrices U and V and a diagonal matrix D such that

$$A = V D U^*,$$

where D is a diagonal matrix consisting of real entries $\sigma_1, \ldots, \sigma_n$, where $\sigma_1, \ldots, \sigma_r$ are the singular values of A, i.e., the positive square roots of the nonzero eigenvalues of A^*A and $A\,A^*$, and $\sigma_{r+1} = \ldots = \sigma_n = 0$.

A notion closely related to the SVD is the polar form of a matrix.

Definition 2.3. A pair (R, S) such that $A = RS$ with R orthogonal and S symmetric positive semidefinite is called a *polar decomposition of* A.

Theorem 2.7 implies that for every real $n \times n$ matrix A, there is some orthogonal matrix R and some positive semidefinite symmetric matrix S such that

$$A = RS.$$

This is easy to show and we will prove it below. Furthermore, R, S are unique if A is invertible, but this is harder to prove.

For example, the matrix

$$A = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

is both orthogonal and symmetric, and $A = RS$ with $R = A$ and $S = I$, which implies that some of the eigenvalues of A are negative.

Remark: In the complex case, the polar decomposition states that for every complex $n \times n$ matrix A, there is some unitary matrix U and some positive semidefinite Hermitian matrix H such that

$$A = UH.$$

It is easy to go from the polar form to the SVD, and conversely.

Given an SVD decomposition $A = V D U^\top$, let $R = V U^\top$ and $S = U D U^\top$. It is clear that R is orthogonal and that S is positive semidefinite symmetric, and

$$RS = V U^\top U D U^\top = V D U^\top = A.$$

Going the other way, given a polar decomposition $A = R_1 S$, where R_1 is orthogonal and S is positive semidefinite symmetric, there is an orthogonal matrix R_2 and a positive semidefinite diagonal matrix D such that $S = R_2 D R_2^\top$, and thus

$$A = R_1 R_2 D R_2^\top = V D U^\top,$$

where $V = R_1 R_2$ and $U = R_2$ are orthogonal.

The eigenvalues and the singular values of a matrix are typically not related in any obvious way. For example, the $n \times n$ matrix

$$A = \begin{pmatrix} 1 & 2 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 2 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 2 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & 2 \\ 0 & 0 & \dots & 0 & 0 & 0 & 1 \end{pmatrix}$$

has the eigenvalue 1 with multiplicity n, but its singular values, $\sigma_1 \geq \cdots \geq \sigma_n$, which are

the positive square roots of the eigenvalues of the matrix $B = A^\top A$ with

$$B = \begin{pmatrix} 1 & 2 & 0 & 0 & \dots & 0 & 0 \\ 2 & 5 & 2 & 0 & \dots & 0 & 0 \\ 0 & 2 & 5 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 2 & 5 & 2 & 0 \\ 0 & 0 & \dots & 0 & 2 & 5 & 2 \\ 0 & 0 & \dots & 0 & 0 & 2 & 5 \end{pmatrix}$$

have a wide spread, since

$$\frac{\sigma_1}{\sigma_n} = \mathrm{cond}_2(A) \geq 2^{n-1}.$$

If A is a complex $n \times n$ matrix, the eigenvalues $\lambda_1, \dots, \lambda_n$ and the singular values $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n$ of A are not unrelated, since

$$\sigma_1^2 \cdots \sigma_n^2 = \det(A^* A) = |\det(A)|^2$$

and

$$|\lambda_1| \cdots |\lambda_n| = |\det(A)|,$$

so we have

$$|\lambda_1| \cdots |\lambda_n| = \sigma_1 \cdots \sigma_n.$$

More generally, Hermann Weyl proved the following remarkable theorem:

Theorem 2.8. *(Weyl's inequalities, 1949) For any complex $n \times n$ matrix, A, if $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ are the eigenvalues of A and $\sigma_1, \dots, \sigma_n \in \mathbb{R}_+$ are the singular values of A, listed so that $|\lambda_1| \geq \cdots \geq |\lambda_n|$ and $\sigma_1 \geq \cdots \geq \sigma_n \geq 0$, then*

$$\begin{aligned} &|\lambda_1| \cdots |\lambda_n| = \sigma_1 \cdots \sigma_n \quad \textit{and} \\ &|\lambda_1| \cdots |\lambda_k| \leq \sigma_1 \cdots \sigma_k, \quad \textit{for} \quad k = 1, \dots, n-1. \end{aligned}$$

A proof of Theorem 2.8 can be found in Horn and Johnson [8], Chapter 3, Section 3.3, where more inequalities relating the eigenvalues and the singular values of a matrix are given.

Theorem 2.7 can be easily extended to rectangular $m \times n$ matrices, as we show in the next section (for various versions of the SVD for rectangular matrices, see Strang [18] Golub and Van Loan [7], Demmel [4], and Trefethen and Bau [19]).

2.7 Singular Value Decomposition for Rectangular Matrices

Here is the generalization of Theorem 2.7 to rectangular matrices.

Theorem 2.9. *(Singular value decomposition) For every real $m \times n$ matrix A, there are two orthogonal matrices U $(n \times n)$ and V $(m \times m)$ and a diagonal $m \times n$ matrix D such that $A = V D U^\top$, where D is of the form*

$$D = \begin{pmatrix} \sigma_1 & & \dots & \\ & \sigma_2 & \dots & \\ \vdots & \vdots & \ddots & \vdots \\ & & \dots & \sigma_n \\ 0 & \vdots & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \vdots & \dots & 0 \end{pmatrix} \quad or \quad D = \begin{pmatrix} \sigma_1 & & \dots & & 0 & \dots & 0 \\ & \sigma_2 & \dots & & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \vdots & 0 \\ & & \dots & \sigma_m & 0 & \dots & 0 \end{pmatrix},$$

where $\sigma_1, \dots, \sigma_r$ are the singular values of f, i.e. the (positive) square roots of the nonzero eigenvalues of $A^\top A$ and $A A^\top$, and $\sigma_{r+1} = \dots = \sigma_p = 0$, where $p = \min(m, n)$. The columns of U are eigenvectors of $A^\top A$, and the columns of V are eigenvectors of $A A^\top$.

Proof. As in the proof of Theorem 2.7, since $A^\top A$ is symmetric positive semidefinite, there exists an $n \times n$ orthogonal matrix U such that

$$A^\top A = U \Sigma^2 U^\top,$$

with $\Sigma = \mathrm{diag}(\sigma_1, \dots, \sigma_r, 0, \dots, 0)$, where $\sigma_1^2, \dots, \sigma_r^2$ are the nonzero eigenvalues of $A^\top A$, and where r is the rank of A. Observe that $r \leq \min\{m, n\}$, and AU is an $m \times n$ matrix. It follows that

$$U^\top A^\top A U = (AU)^\top AU = \Sigma^2,$$

and if we let $f_j \in \mathbb{R}^m$ be the jth column of AU for $j = 1, \dots, n$, then we have

$$\langle f_i, f_j \rangle = \sigma_i^2 \delta_{ij}, \quad 1 \leq i, j \leq r$$

and

$$f_j = 0, \quad r + 1 \leq j \leq n.$$

If we define $(v_1, \dots, v_r)$ by

$$v_j = \sigma_j^{-1} f_j, \quad 1 \leq j \leq r,$$

then we have

$$\langle v_i, v_j \rangle = \delta_{ij}, \quad 1 \leq i, j \leq r,$$

so complete $(v_1, \dots, v_r)$ into an orthonormal basis $(v_1, \dots, v_r, v_{r+1}, \dots, v_m)$ (for example, using Gram–Schmidt).

Now, since $f_j = \sigma_j v_j$ for $j = 1 \dots, r$, we have

$$\langle v_i, f_j \rangle = \sigma_j \langle v_i, v_j \rangle = \sigma_j \delta_{i,j}, \quad 1 \leq i \leq m,\ 1 \leq j \leq r$$

and since $f_j = 0$ for $j = r+1, \ldots, n$, we have

$$\langle v_i, f_j \rangle = 0 \quad 1 \leq i \leq m,\ r+1 \leq j \leq n.$$

If V is the matrix whose columns are $v_1, \ldots, v_m$, then V is an $m \times m$ orthogonal matrix and if $m \geq n$, we let

$$D = \begin{pmatrix} \Sigma \\ 0_{m-n} \end{pmatrix} = \begin{pmatrix} \sigma_1 & & \ldots & \\ & \sigma_2 & \ldots & \\ \vdots & \vdots & \ddots & \vdots \\ & & \ldots & \sigma_n \\ 0 & \vdots & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \vdots & \ldots & 0 \end{pmatrix},$$

else if $n \geq m$, then we let

$$D = \begin{pmatrix} \sigma_1 & & \ldots & & 0 & \ldots & 0 \\ & \sigma_2 & \ldots & & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \vdots & 0 \\ & & \ldots & \sigma_m & 0 & \ldots & 0 \end{pmatrix}.$$

In either case, the above equations prove that

$$V^\top A U = D,$$

which yields $A = VDU^\top$, as required.

The equation $A = VDU^\top$ implies that

$$A^\top A = UD^\top DU^\top = U \mathrm{diag}(\sigma_1^2, \ldots, \sigma_r^2, \underbrace{0, \ldots, 0}_{n-r}) U^\top$$

and

$$AA^\top = VDD^\top V^\top = V \mathrm{diag}(\sigma_1^2, \ldots, \sigma_r^2, \underbrace{0, \ldots, 0}_{m-r}) V^\top,$$

which shows that $A^\top A$ and $AA^\top$ have the same nonzero eigenvalues, that the columns of U are eigenvectors of $A^\top A$, and that the columns of V are eigenvectors of $AA^\top$. □

A triple (U, D, V) such that $A = VDU^\top$ is called a *singular value decomposition (SVD) of* A.

Even though the matrix D is an $m \times n$ rectangular matrix, since its only nonzero entries are on the descending diagonal, we still say that D is a diagonal matrix.

If we view A as the representation of a linear map $f\colon E \to F$, where $\dim(E) = n$ and $\dim(F) = m$, the proof of Theorem 2.9 shows that there are two orthonormal bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_m)$ for E and F, respectively, where $(u_1, \ldots, u_n)$ are eigenvectors of $f^* \circ f$ and $(v_1, \ldots, v_m)$ are eigenvectors of $f \circ f^*$. Furthermore, $(u_1, \ldots, u_r)$ is an orthonormal basis of $\operatorname{Im} f^*$, $(u_{r+1}, \ldots, u_n)$ is an orthonormal basis of $\operatorname{Ker} f$, $(v_1, \ldots, v_r)$ is an orthonormal basis of $\operatorname{Im} f$, and $(v_{r+1}, \ldots, v_m)$ is an orthonormal basis of $\operatorname{Ker} f^*$.

The SVD of matrices can be used to define the pseudo-inverse of a rectangular matrix; we do so in the nexg section. The reader may also consult Strang [18], Demmel [4], Trefethen and Bau [19], and Golub and Van Loan [7].

The polar form has applications in continuum mechanics. Indeed, in any deformation it is important to separate stretching from rotation. This is exactly what QS achieves. The orthogonal part Q corresponds to rotation (perhaps with an additional reflection), and the symmetric matrix S to stretching (or compression). The real eigenvalues $\sigma_1, \ldots, \sigma_r$ of S are the stretch factors (or compression factors) (see Marsden and Hughes [12]). The fact that S can be diagonalized by an orthogonal matrix corresponds to a natural choice of axes, the principal axes.

The SVD has applications to data compression, for instance in image processing. The idea is to retain only singular values whose magnitudes are significant enough. The SVD can also be used to determine the rank of a matrix when other methods such as Gaussian elimination produce very small pivots. One of the main applications of the SVD is the computation of the pseudo-inverse. Pseudo-inverses are the key to the solution of various optimization problems, in particular the method of least squares. This topic is discussed in the next section. Applications of the material of this section can be found in Strang [18, 17]; Ciarlet [3]; Golub and Van Loan [7], which contains many other references; Demmel [4]; and Trefethen and Bau [19].

2.8 Least Squares Problems and the Pseudo-Inverse

> De tous les principes qu'on peut proposer pour cet objet, je pense qu'il n'en est pas de plus général, de plus exact, ni d'une application plus facile, que celui dont nous avons fait usage dans les recherches précédentes, et qui consiste à rendre *minimum* la somme des carrés des erreurs. Par ce moyen il s'établit entre les erreurs une sorte d'équilibre qui, empêchant les extrêmes de prévaloir, est très propre à faire connaitre l'état du système le plus proche de la vérité.
>
> —**Legendre, 1805,** *Nouvelles Méthodes pour la détermination des Orbites des Comètes*

This section and the next present several applications of SVD. The first one is the pseudo-inverse, which plays a crucial role in solving linear systems by the method of least squares. The second application is data compression.

The method of least squares is a way of "solving" an overdetermined system of linear equations

$$Ax = b,$$

i.e., a system in which A is a rectangular $m \times n$ matrix with more equations than unknowns (when $m > n$). Historically, the method of least squares was used by Gauss and Legendre to solve problems in astronomy and geodesy. The method was first published by Legendre in 1805 in a paper on methods for determining the orbits of comets. However, Gauss had already used the method of least squares as early as 1801 to determine the orbit of the asteroid Ceres, and he published a paper about it in 1810 after the discovery of the asteroid Pallas. Incidentally, it is in that same paper that Gaussian elimination using pivots is introduced.

The reason why more equations than unknowns arise in such problems is that repeated measurements are taken to minimize errors. This produces an overdetermined and often inconsistent system of linear equations. For example, Gauss solved a system of eleven equations in six unknowns to determine the orbit of the asteroid Pallas. As a concrete illustration, suppose that we observe the motion of a small object, assimilated to a point, in the plane. From our observations, we suspect that this point moves along a straight line, say of equation $y = dx + c$. Suppose that we observed the moving point at three different locations (x_1, y_1), (x_2, y_2), and (x_3, y_3). Then we should have

$$\begin{aligned} c + dx_1 &= y_1, \\ c + dx_2 &= y_2, \\ c + dx_3 &= y_3. \end{aligned}$$

If there were no errors in our measurements, these equations would be compatible, and c and d would be determined by only two of the equations. However, in the presence of errors, the system may be inconsistent. Yet we would like to find c and d!

The idea of the method of least squares is to determine (c, d) such that it minimizes the sum of the squares of the errors, namely,

$$(c + dx_1 - y_1)^2 + (c + dx_2 - y_2)^2 + (c + dx_3 - y_3)^2.$$

In general, for an overdetermined $m \times n$ system $Ax = b$, what Gauss and Legendre discovered is that there are solutions x minimizing

$$\|Ax - b\|_2^2$$

(where $\|u\|_2^2 = u_1^2 + \cdots + u_n^2$, the square of the Euclidean norm of the vector $u = (u_1, \ldots, u_n)$), and that these solutions are given by the square $n \times n$ system

$$A^\top Ax = A^\top b,$$

called the *normal equations*. Furthermore, when the columns of A are linearly independent, it turns out that $A^\top A$ is invertible, and so x is unique and given by

$$x = (A^\top A)^{-1} A^\top b.$$

Note that $A^\top A$ is a symmetric matrix, one of the nice features of the normal equations of a least squares problem. For instance, the normal equations for the above problem are

$$\begin{pmatrix} 3 & x_1+x_2+x_3 \\ x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} y_1+y_2+y_3 \\ x_1y_1+x_2y_2+x_3y_3 \end{pmatrix}.$$

In fact, given any real $m \times n$ matrix A, there is always a unique x^+ of minimum norm that minimizes $\|Ax-b\|_2^2$, even when the columns of A are linearly dependent. How do we prove this, and how do we find x^+?

Theorem 2.10. *Every linear system $Ax = b$, where A is an $m \times n$ matrix, has a unique least squares solution x^+ of smallest norm.*

Proof. Geometry offers a nice proof of the existence and uniqueness of x^+. Indeed, we can interpret b as a point in the Euclidean (affine) space $\mathbb{R}^m$, and the image subspace of A (also called the column space of A) as a subspace U of $\mathbb{R}^m$ (passing through the origin). Then, it is clear that

$$\inf_{x\in\mathbb{R}^n} \|Ax-b\|_2^2 = \inf_{y\in U} \|y-b\|_2^2,$$

with $U = \operatorname{Im} A$, and we claim that x minimizes $\|Ax-b\|_2^2$ iff $Ax = p$, where p the orthogonal projection of b onto the subspace U.

Recall that the orthogonal projection $p_U \colon U \oplus U^\perp \to U$ is the linear map given by

$$p_U(u+v) = u,$$

with $u \in U$ and $v \in U^\perp$. If we let $p = p_U(b) \in U$, then for any point $y \in U$, the vectors $\overrightarrow{py} = y - p \in U$ and $\overrightarrow{bp} = p - b \in U^\perp$ are orthogonal, which implies that

$$\|\overrightarrow{by}\|_2^2 = \|\overrightarrow{bp}\|_2^2 + \|\overrightarrow{py}\|_2^2,$$

where $\overrightarrow{by} = y - b$. Thus, p is indeed the unique point in U that minimizes the distance from b to any point in U.

Thus, the problem has been reduced to proving that there is a unique x^+ of minimum norm such that $Ax^+ = p$, with $p = p_U(b) \in U$, the orthogonal projection of b onto U. We use the fact that

$$\mathbb{R}^n = \operatorname{Ker} A \oplus (\operatorname{Ker} A)^\perp.$$

Consequently, every $x \in \mathbb{R}^n$ can be written uniquely as $x = u + v$, where $u \in \operatorname{Ker} A$ and $v \in (\operatorname{Ker} A)^\perp$, and since u and v are orthogonal,

$$\|x\|_2^2 = \|u\|_2^2 + \|v\|_2^2.$$

Furthermore, since $u \in \operatorname{Ker} A$, we have $Au = 0$, and thus $Ax = p$ iff $Av = p$, which shows that the solutions of $Ax = p$ for which x has minimum norm must belong to $(\operatorname{Ker} A)^\perp$.

However, the restriction of A to $(\operatorname{Ker} A)^\perp$ is injective. This is because if $Av_1 = Av_2$, where $v_1, v_2 \in (\operatorname{Ker} A)^\perp$, then $A(v_2 - v_2) = 0$, which implies $v_2 - v_1 \in \operatorname{Ker} A$, and since $v_1, v_2 \in (\operatorname{Ker} A)^\perp$, we also have $v_2 - v_1 \in (\operatorname{Ker} A)^\perp$, and consequently, $v_2 - v_1 = 0$. This shows that there is a unique x^+ of minimum norm such that $Ax^+ = p$, and that x^+ must belong to $(\operatorname{Ker} A)^\perp$. By our previous reasoning, x^+ is the unique vector of minimum norm minimizing $\|Ax - b\|_2^2$. □

The proof also shows that x minimizes $\|Ax - b\|_2^2$ iff $\overrightarrow{pb} = b - Ax$ is orthogonal to U, which can be expressed by saying that $b - Ax$ is orthogonal to every column of A. However, this is equivalent to

$$A^\top(b - Ax) = 0, \quad \text{i.e.,} \quad A^\top Ax = A^\top b.$$

Finally, it turns out that the minimum norm least squares solution x^+ can be found in terms of the pseudo-inverse A^+ of A, which is itself obtained from any SVD of A.

Definition 2.4. Given any $m \times n$ matrix A, if $A = VDU^\top$ is an SVD of A with

$$D = \operatorname{diag}(\lambda_1, \ldots, \lambda_r, 0, \ldots, 0),$$

where D is an $m \times n$ matrix and $\lambda_i > 0$, if we let

$$D^+ = \operatorname{diag}(1/\lambda_1, \ldots, 1/\lambda_r, 0, \ldots, 0),$$

an $n \times m$ matrix, the *pseudo-inverse* of A is defined by

$$A^+ = UD^+V^\top.$$

Actually, it seems that A^+ depends on the specific choice of U and V in an SVD (U, D, V) for A, but the next theorem shows that this is not so.

Theorem 2.11. *The least squares solution of smallest norm of the linear system $Ax = b$, where A is an $m \times n$ matrix, is given by*

$$x^+ = A^+b = UD^+V^\top b.$$

Proof. First, assume that A is a (rectangular) diagonal matrix D, as above. Then, since x minimizes $\|Dx - b\|_2^2$ iff Dx is the projection of b onto the image subspace F of D, it is fairly obvious that $x^+ = D^+b$. Otherwise, we can write

$$A = VDU^\top,$$

where U and V are orthogonal. However, since V is an isometry,

$$\|Ax - b\|_2 = \|VDU^\top x - b\|_2 = \|DU^\top x - V^\top b\|_2.$$

Letting $y = U^\top x$, we have $\|x\|_2 = \|y\|_2$, since U is an isometry, and since U is surjective, $\|Ax - b\|_2$ is minimized iff $\|Dy - V^\top b\|_2$ is minimized, and we have shown that the least solution is

$$y^+ = D^+ V^\top b.$$

Since $y = U^\top x$, with $\|x\|_2 = \|y\|_2$, we get

$$x^+ = UD^+ V^\top b = A^+ b.$$

Thus, the pseudo-inverse provides the optimal solution to the least squares problem. □

By Proposition 2.11 and Theorem 2.10, $A^+ b$ is uniquely defined by every b, and thus A^+ depends only on A.

If A has full rank and $m \geq n$, then $A^\top A$ is invertible, in which case the pseudo inverse of A is given by

$$A^+ = (A^\top A)^{-1} A^\top.$$

Let $A = U\Sigma V^\top$ be an SVD for A. It is easy to check that

$$\begin{aligned} AA^+A &= A, \\ A^+AA^+ &= A^+, \end{aligned}$$

and both AA^+ and A^+A are symmetric matrices. In fact,

$$AA^+ = U\Sigma V^\top V\Sigma^+ U^\top = U\Sigma\Sigma^+ U^\top = U \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} U^\top$$

and

$$A^+A = V\Sigma^+ U^\top U\Sigma V^\top = V\Sigma^+\Sigma V^\top = V \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} V^\top.$$

We immediately get

$$\begin{aligned} (AA^+)^2 &= AA^+, \\ (A^+A)^2 &= A^+A, \end{aligned}$$

so both AA^+ and A^+A are orthogonal projections (since they are both symmetric). *We claim that AA^+ is the orthogonal projection onto the range of A and A^+A is the orthogonal projection onto* $\mathrm{Ker}(A)^\perp = \mathrm{Im}(A^\top)$*, the range of* $A^\top$.

Obviously, we have $\mathrm{range}(AA^+) \subseteq \mathrm{range}(A)$, and for any $y = Ax \in \mathrm{range}(A)$, since $AA^+A = A$, we have

$$AA^+ y = AA^+ Ax = Ax = y,$$

so the image of AA^+ is indeed the range of A. It is also clear that $\mathrm{Ker}(A) \subseteq \mathrm{Ker}(A^+A)$, and since $AA^+A = A$, we also have $\mathrm{Ker}(A^+A) \subseteq \mathrm{Ker}(A)$, and so

$$\mathrm{Ker}(A^+A) = \mathrm{Ker}(A).$$

Since A^+A is Hermitian, $\text{range}(A^+A) = \text{Ker}(A^+A)^\perp = \text{Ker}(A)^\perp$, as claimed.

It will also be useful to see that $\text{range}(A) = \text{range}(AA^+)$ consists of all vectors $y \in \mathbb{R}^n$ such that

$$U^\top y = \begin{pmatrix} z \\ 0 \end{pmatrix},$$

with $z \in \mathbb{R}^r$.

Indeed, if $y = Ax$, then

$$U^\top y = U^\top Ax = U^\top U\Sigma V^\top x = \Sigma V^\top x = \begin{pmatrix} \Sigma_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} V^\top x = \begin{pmatrix} z \\ 0 \end{pmatrix},$$

where Σ_r is the $r \times r$ diagonal matrix $\text{diag}(\sigma_1, \ldots, \sigma_r)$. Conversely, if $U^\top y = \left(\begin{smallmatrix} z \\ 0 \end{smallmatrix}\right)$, then $y = U\left(\begin{smallmatrix} z \\ 0 \end{smallmatrix}\right)$, and

$$\begin{aligned} AA^+y &= U \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} U^\top y \\ &= U \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} U^\top U \begin{pmatrix} z \\ 0 \end{pmatrix} \\ &= U \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} \begin{pmatrix} z \\ 0 \end{pmatrix} \\ &= U \begin{pmatrix} z \\ 0 \end{pmatrix} = y, \end{aligned}$$

which shows that y belongs to the range of A.

Similarly, we claim that $\text{range}(A^+A) = \text{Ker}(A)^\perp$ consists of all vectors $y \in \mathbb{R}^n$ such that

$$V^\top y = \begin{pmatrix} z \\ 0 \end{pmatrix},$$

with $z \in \mathbb{R}^r$.

If $y = A^+Au$, then

$$y = A^+Au = V \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} V^\top u = V \begin{pmatrix} z \\ 0 \end{pmatrix},$$

for some $z \in \mathbb{R}^r$. Conversely, if $V^\top y = \left(\begin{smallmatrix} z \\ 0 \end{smallmatrix}\right)$, then $y = V\left(\begin{smallmatrix} z \\ 0 \end{smallmatrix}\right)$, and so

$$\begin{aligned} A^+AV \begin{pmatrix} z \\ 0 \end{pmatrix} &= V \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} V^\top V \begin{pmatrix} z \\ 0 \end{pmatrix} \\ &= V \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix} \begin{pmatrix} z \\ 0 \end{pmatrix} \\ &= V \begin{pmatrix} z \\ 0 \end{pmatrix} = y, \end{aligned}$$

which shows that $y \in \text{range}(A^+A)$.

If A is a symmetric matrix, then in general, there is no SVD $U\Sigma V^\top$ of A with $U = V$. However, if A is positive semidefinite, then the eigenvalues of A are nonnegative, and so the nonzero eigenvalues of A are equal to the singular values of A and SVDs of A are of the form

$$A = U\Sigma U^\top.$$

If A is symmetric but not necessarily positive definite, since

$$A^*A = U\Sigma^2 U^\top,$$

we see that the singular values of A are $|\lambda_1|, \ldots, |\lambda_r|$, where $\lambda_1, \ldots, \lambda_r$ are the nonzero eigenvalues of A. Analogous results hold for complex matrices, but in this case, U and V are unitary matrices and AA^+ and A^+A are Hermitian orthogonal projections.

The following properties, due to Penrose, characterize the pseudo-inverse of a matrix. We have already proved that the pseudo-inverse satisfies these equations. For a proof of the converse, see Kincaid and Cheney [10].

Proposition 2.12. *Given any $m \times n$ matrix A (real or complex), the pseudo-inverse A^+ of A is the unique $n \times m$ matrix satisfying the following properties:*

$$\begin{aligned} AA^+A &= A, \\ A^+AA^+ &= A^+, \\ (AA^+)^\top &= AA^+, \\ (A^+A)^\top &= A^+A. \end{aligned}$$

If A is an $m \times n$ matrix of rank n (and so $m \geq n$), it is immediately shown that the QR-decomposition in terms of Householder transformations applies as follows:

There are n $m \times m$ matrices $H_1, \ldots, H_n$, Householder matrices or the identity, and an upper triangular $m \times n$ matrix R of rank n such that

$$A = H_1 \cdots H_n R.$$

Then, because each H_i is an isometry,

$$\|Ax - b\|_2 = \|Rx - H_n \cdots H_1 b\|_2,$$

and the least squares problem $Ax = b$ is equivalent to the system

$$Rx = H_n \cdots H_1 b.$$

Now, the system

$$Rx = H_n \cdots H_1 b$$

is of the form

$$\begin{pmatrix} R_1 \\ 0_{m-n} \end{pmatrix} x = \begin{pmatrix} c \\ d \end{pmatrix},$$

where R_1 is an invertible $n \times n$ matrix (since A has rank n), $c \in \mathbb{R}^n$, and $d \in \mathbb{R}^{m-n}$, and the least squares solution of smallest norm is

$$x^+ = R_1^{-1} c.$$

Since R_1 is a triangular matrix, it is very easy to invert R_1.

Hilbert's problem (given a function $f \in C[0,1]$, find a polynomial $P(x)$ of degree n so that $\int_0^1 |P(x) - f(x)|^2 dx$ is minimum) can be cast as a least square problem. Many other interpolation problems can be cast as least squares problems.

The method of least squares is one of the most effective tools of the mathematical sciences. There are entire books devoted to it. Readers are advised to consult Strang [18], Golub and Van Loan [7], Demmel [4], and Trefethen and Bau [19], where extensions and applications of least squares (such as weighted least squares and recursive least squares) are described. Golub and Van Loan [7] also contains a very extensive bibliography, including a list of books on least squares.

2.9 Data Compression and SVD

Among the many applications of SVD, a very useful one is *data compression*, notably for images. In order to make precise the notion of closeness of matrices, we use the notion of *matrix norm*.

Given an $m \times n$ matrix of rank r, we would like to find a best approximation of A by a matrix B of rank $k \leq r$ (actually, $k < r$) so that $\|A - B\|_2$ (or the Frobenius norm $\|A - B\|_F$) is minimized.

Proposition 2.13. *Let A be an $m \times n$ matrix of rank r and let $VDU^\top = A$ be an SVD for A. Write u_i for the columns of U, v_i for the columns of V, and $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_p$ for the singular values of A ($p = \min(m,n)$). Then a matrix of rank $k < r$ closest to A (in the $\| \ \|_2$ norm) is given by*

$$A_k = \sum_{i=1}^{k} \sigma_i v_i u_i^\top = V \mathrm{diag}(\sigma_1, \ldots, \sigma_k) U^\top$$

and $\|A - A_k\|_2 = \sigma_{k+1}$.

Proof. By construction, A_k has rank k, and we have

$$\|A - A_k\|_2 = \Big\| \sum_{i=k+1}^{p} \sigma_i v_i u_i^\top \Big\|_2 = \big\| V \mathrm{diag}(0, \ldots, 0, \sigma_{k+1}, \ldots, \sigma_p) U^\top \big\|_2 = \sigma_{k+1}.$$

It remains to show that $\|A - B\|_2 \geq \sigma_{k+1}$ for all rank-k matrices B. Let B be any rank-k matrix, so its kernel has dimension $p - k$. The subspace V_{k+1} spanned by $(v_1, \ldots, v_{k+1})$ has dimension $k + 1$, and because the sum of the dimensions of the kernel of B and of V_{k+1} is $(p - k) + k + 1 = p + 1$, these two subspaces must intersect in a subspace of dimension at least 1. Pick any unit vector h in $\mathrm{Ker}(B) \cap V_{k+1}$. Then since $Bh = 0$, we have

$$\|A - B\|_2^2 \geq \|(A - B)h\|_2^2 = \|Ah\|_2^2 = \left\|VDU^\top h\right\|_2^2 \geq \sigma_{k+1}^2 \left\|U^\top h\right\|_2^2 = \sigma_{k+1}^2,$$

which proves our claim. □

Note that A_k can be stored using $(m + n)k$ entries, as opposed to mn entries. When $k \ll m$, this is a substantial gain.

A nice example of the use of Proposition 2.13 in image compression is given in Demmel [4], Chapter 3, Section 3.2.3, pages 113–115; see the Matlab demo.

An interesting topic that we have not addressed is the actual computation of an SVD. This is a very interesting but tricky subject. Most methods reduce the computation of an SVD to the diagonalization of a well-chosen symmetric matrix (which is not $A^\top A$). Interested readers should read Section 5.4 of Demmel's excellent book [4], which contains an overview of most known methods and an extensive list of references.

Bibliography

[1] Marcel Berger. *Géométrie 1.* Nathan, 1990. English edition: Geometry 1, Universitext, Springer Verlag.

[2] T. Bröcker and T. tom Dieck. *Representation of Compact Lie Groups.* GTM, Vol. 98. Springer Verlag, first edition, 1985.

[3] P.G. Ciarlet. *Introduction to Numerical Matrix Analysis and Optimization.* Cambridge University Press, first edition, 1989. French edition: Masson, 1994.

[4] James W. Demmel. *Applied Numerical Linear Algebra.* SIAM Publications, first edition, 1997.

[5] William Fulton and Joe Harris. *Representation Theory, A first course.* GTM No. 129. Springer Verlag, first edition, 1991.

[6] Jean H. Gallier. *Geometric Methods and Applications, For Computer Science and Engineering.* TAM, Vol. 38. Springer, second edition, 2011.

[7] H. Golub, Gene and F. Van Loan, Charles. *Matrix Computations.* The Johns Hopkins University Press, third edition, 1996.

[8] Roger A. Horn and Charles R. Johnson. *Topics in Matrix Analysis.* Cambridge University Press, first edition, 1994.

[9] James E. Humphreys. *Introduction to Lie Algebras and Representation Theory.* GTM No. 9. Springer Verlag, first edition, 1972.

[10] D. Kincaid and W. Cheney. *Numerical Analysis.* Brooks/Cole Publishing, second edition, 1996.

[11] Anthony W. Knapp. *Lie Groups Beyond an Introduction.* Progress in Mathematics, Vol. 140. Birkhäuser, second edition, 2002.

[12] Jerrold E. Marsden and J.R. Hughes, Thomas. *Mathematical Foundations of Elasticity.* Dover, first edition, 1994.

[13] Jean-Pierre Serre. *Linear Representations of Finite Groups*. GTM No. 42. Springer, first edition, 1977.

[14] Jean-Pierre Serre. *Lie Algebras and Lie Groups*. Lecture Notes in Mathematics, No. 1500. Springer, second edition, 1992.

[15] Jean-Pierre Serre. *Complex Semisimple Lie Algebras*. Springer Monographs in Mathematics. Springer, first edition, 2000.

[16] G.W. Stewart. On the early history of the singular value decomposition. *SIAM review*, 35(4):551–566, 1993.

[17] Gilbert Strang. *Introduction to Applied Mathematics*. Wellesley-Cambridge Press, first edition, 1986.

[18] Gilbert Strang. *Linear Algebra and its Applications*. Saunders HBJ, third edition, 1988.

[19] L.N. Trefethen and D. Bau III. *Numerical Linear Algebra*. SIAM Publications, first edition, 1997.