Homework V (due December 9), Math 602, Fall 2002. (GJSZ)

B III.(d) First, we need to recall that if M is a Γ-module, then, viewing M as a $\mathbb{Z}$-module, the $\mathbb{Z}$-module $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$ is made into a Γ-module by defining the (left) action of Γ on $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$ as follows: For any $\gamma \in \Gamma$ and any $f \in \mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$, we define γf as the $\mathbb{Z}$-linear map given by

$$(\gamma f)(\lambda) = f(\lambda\gamma), \quad \text{for all } \lambda \in \Gamma.$$

We have

$$(\gamma(f + f'))(\lambda) = (f + f')(\lambda\gamma) = f(\lambda\gamma) + f'(\lambda\gamma) = (\gamma f)(\lambda) + (\gamma f')(\lambda),$$

and

$$(\alpha(\gamma f))(\lambda) = (\gamma f)(\lambda\alpha) = f(\lambda\alpha\gamma) = ((\alpha\gamma)f)(\lambda),$$

confirming that $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$ is indeed a Γ-module with this action.

Let F be a free abelian group (a $\mathbb{Z}$-module).

Proposition 1.1 *If F is a free $\mathbb{Z}$-module, then $F^D = \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z})$ is an injective $\mathbb{Z}$-module.*

Proof. Since F is a free $\mathbb{Z}$-module, $F = \coprod_S \mathbb{Z}$, for some index set, S. So,

$$F^D = \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(\coprod_S \mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \prod_S \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \prod_S \mathbb{Q}/\mathbb{Z}.$$

However, $\mathbb{Q}$ is obviously divisible, and and factors of divisible are divisible. Thus, $\mathbb{Q}/\mathbb{Z}$ is a divisible abelian group; but we proved in class that a divisible abelian group is injective, so, $\mathbb{Q}/\mathbb{Z}$ is injective. We also proved in class that any product of injectives is injective. Therefore, $\prod_S \mathbb{Q}/\mathbb{Z}$ is injective, and so, F^D is also injective. $\square$

Given a $\mathbb{Z}$-module, M, we define a natural $\mathbb{Z}$-linear map, $m \mapsto \widehat{m}$, from M to $M^{DD} = \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}), \mathbb{Q}/\mathbb{Z})$, as follows: For every $m \in M$ and every $f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$,

$$\widehat{m}(f) = f(m).$$

It is clear that such a map is $\mathbb{Z}$-linear.

Proposition 1.2 *For every $\mathbb{Z}$-module, M, the natural map $M \longrightarrow M^{DD}$ is injective.*

Proof. It is enough to show that $m \neq 0$ implies that $\widehat{m} \neq 0$, i.e., there is some $f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ so that $f(m) \neq 0$.

Consider the cyclic subgroup, $\langle m \rangle$, of M generated by m. We define a $\mathbb{Z}$-linear map, $f\colon \langle m \rangle \to \mathbb{Q}/\mathbb{Z}$, as follows: If m has infinite order, let $f(km) = k/2 \pmod{\mathbb{Z}}$, and if m has finite order, n, let $f(km) = k/n \pmod{\mathbb{Z}}$. Since $0 \longrightarrow \langle m \rangle \longrightarrow M$ is exact and $\mathbb{Q}/\mathbb{Z}$ is injective, the map $f\colon \langle m \rangle \to \mathbb{Q}/\mathbb{Z}$ extends to a map $f\colon M \to \mathbb{Q}/\mathbb{Z}$, with $f(m) \neq 0$, as claimed. $\square$

Theorem 1.3 *For every $\mathbb{Z}$-module, M, there is some injective $\mathbb{Z}$-module, P, and an injection $M \longrightarrow P$.*

Proof. Consider the $\mathbb{Z}$-module, M^D. We know that there is some free $\mathbb{Z}$-module, F, so that the sequence

$$F \longrightarrow M^D \longrightarrow 0 \quad \text{is exact.}$$

Since $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z},)$ is left-exact, we get the exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(M^D, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z}),$$

i.e.,

$$0 \longrightarrow M^{DD} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z}).$$

Thus, we have an injection $M^{DD} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z})$. However, by Proposition 1.1, the $\mathbb{Z}$-module $\mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z})$ is injective and by Proposition 1.2, we have an injection $M \longrightarrow M^{DD}$. Therefore, composing these injections, we get an injection $M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z})$, with $\mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z})$ injective, as desired. $\square$

B III.(e) Recall from B III.(d) that for any $\mathbb{Z}$-module, M, the module $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$ is a Γ-module.

Define the map, $j \colon M \to \mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$, as follows: For every $m \in M$ and every $\gamma \in \Gamma$,

$$j(m)(\gamma) = \gamma m.$$

Proposition 1.4 *If M is a Γ-module, the map $j \colon M \to \mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$ is a Γ-linear injection.*

Proof. We have

$$j(m + m')(\gamma) = \gamma(m + m') = \gamma m + \gamma m' = j(m)(\gamma) + j(m')(\gamma),$$

for all $\gamma \in \Gamma$ and all $m, m' \in M$. We also have

$$j(\lambda m)(\gamma) = \gamma(\lambda m) = (\gamma\lambda)m,$$

for all $m \in M$ and all $\gamma, \lambda \in \Gamma$, and by definition of the Γ-action on $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$, we have

$$(\lambda j(m))(\gamma) = j(m)(\gamma\lambda) = (\gamma\lambda)m,$$

for all $m \in M$ and all $\gamma, \lambda \in \Gamma$. Thus, $j(m)$ is Γ-linear for all $m \in M$. If $j(m) = 0$, then $j(m)(\gamma) = 0$ for all $\gamma \in \Gamma$, and in particular, for $\gamma = 1$. So, $j(m)(1) = 1m = m = 0$, and the map j is injective. $\square$

Recall from B III.(c) that if N is an injective $\mathbb{Z}$-module, then the Γ-module $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, N)$ is injective.

We finally get the main theorem of this problem.

Theorem 1.5 *For every* Γ*-module,* M*, there is some injective* Γ*-module,* P*, and an injection* $M \longrightarrow P$*.*

Proof. If we view M as a $\mathbb{Z}$-module, by Theorem 1.3, there is an injective $\mathbb{Z}$-module, N, and an injection, $M \longrightarrow N$. So, we have the exact sequence

$$0 \longrightarrow M \longrightarrow N,$$

and since $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, -)$ is left-exact, we get the exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma, N).$$

Thus, we have an injection $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma, N)$, and by Proposition 1.4, there is an injection $M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma, M)$, so we get an injection $M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma, N)$. But, since N is $\mathbb{Z}$-injective, by B III.(c), the Γ-module $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, N)$ is injective, and our result is proved. $\square$

Remark: A proof of Theorem 1.5 not using the existence of injectives in **Ab** can be given, following Godement.

Recall that if M is a Γ-module and N is any $\mathbb{Z}$-module, then $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ is a Γ^{op}-module under the right Γ-action given by: For any $f \in \mathrm{Hom}_{\mathbb{Z}}(M, N)$,

$$(f\gamma)(m) = f(\gamma m),$$

for all $m \in M$ and all $\gamma \in \Gamma$. Similarly, if M is a Γ^{op}-module and N is any $\mathbb{Z}$-module, then $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ is a Γ-module under the left Γ-action given by: For any $f \in \mathrm{Hom}_{\mathbb{Z}}(M, N)$,

$$(\gamma f)(m) = f(m\gamma),$$

for all $m \in M$ and all $\gamma \in \Gamma$. Then, $M^D = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is a Γ^{op}-module if M is a Γ-module (resp. a Γ-module is M is Γ^{op}-module). Furthermore, Proposition 1.2 holds, i.e., there is a Γ-injection, $M \longrightarrow M^{DD}$. The new ingredient is the following proposition:

Proposition 1.6 *If* M *is a projective* Γ^{op}*-module, then* M^D *is an injective* Γ*-module.*

Proof. Consider the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & X & \longrightarrow & X' \\ & & \big\downarrow{\scriptstyle \varphi} & & \\ & & M^D & & \end{array}$$

where the row is exact. To prove that M^D is injective, we need to prove that φ extends to a map $\varphi'\colon X' \to M^D$. The map φ yields the map $\mathrm{Hom}_{\mathbb{Z}}(M^D, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z})$, i.e.,

$M^{DD} \longrightarrow X^D$, and since we have an injection $M \longrightarrow M^{DD}$, we get a map $\theta \colon M \to X^D$. Now, since $\mathbb{Q}/\mathbb{Z}$ is injective, $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ maps the exact sequence

$$0 \longrightarrow X \longrightarrow X'$$

to the exact sequence

$$\mathrm{Hom}_{\mathbb{Z}}(X', \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0,$$

i.e.,

$$X'^D \longrightarrow X^D \longrightarrow 0.$$

So, we have the diagram

$$\begin{array}{ccccc} & & M & & \\ & & \big\downarrow{\scriptstyle \theta} & & \\ X'^D & \longrightarrow & X^D & \longrightarrow & 0, \end{array}$$

where the row is exact, and since M is projective, the map θ lifts to a map $\theta' \colon M \to X'^D$. Consequently, we get a map $X'^{DD} \longrightarrow M^D$, and since we have an injection $X' \longrightarrow X'^{DD}$, we get a map $X' \longrightarrow M^D$ extending φ, as desired. Therefore, M^D is injective. $\square$

We can now prove Theorem 1.5, but using the proof of Theorem 1.3. We consider the Γ^{op}-module M^D. We know that there is a free Γ^{op}-module, F, so that

$$F \longrightarrow M^D \longrightarrow 0 \quad \text{is exact.}$$

But, F being free, it is projective, and since $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is left-exact, we get the exact sequence

$$0 \longrightarrow M^{DD} \longrightarrow F^D.$$

By Proposition 1.6, the module F^D is injective. Composing the natural injection $M \longrightarrow M^{DD}$ with the injection $M^{DD} \longrightarrow F^D$, we obtain our injection, $M \longrightarrow F^D$, of M into an injective.

B V.(a) Let k be a field, and $f(X)$ be a monic polynomial of even degree in $k[X]$. Say

$$f(X) = X^{2m} + a_1 X^{2m-1} + \cdots + a_m X^m + a_{m+1} X^{m-1} + \cdots + a_{2m}.$$

We seek some polynomials $g(X)$ and $r(X)$ so that

$$f(X) = g(X)^2 + r(X), \quad \text{with} \quad \deg(r(X)) < m.$$

If $g(X)$ and $r(X)$ exist, then we must have $\deg(g(X)) = m$, say

$$g(X) = b_0 X^m + b_1 X^{m-1} + \cdots + b_m.$$

Now, we can easily compute the coefficients of $g(X)^2$. In fact, we only need the coefficients of the monomials X^k, where $m \leq k \leq 2m$. They are

$$
\begin{array}{rcl}
X^{2m} & : & b_0^2 \\
X^{2m-1} & : & 2b_0b_1 \\
X^{2m-2} & : & 2b_0b_2 + b_1^2 \\
X^{2m-3} & : & 2b_0b_3 + 2b_1b_2 \\
X^{2m-4} & : & 2b_0b_4 + 2b_1b_3 + b_2^2 \\
X^{2m-5} & : & 2b_0b_5 + 2b_1b_4 + 2b_2b_3 \\
\cdots\cdots & : & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
X^{2m-2k} & : & 2b_0b_{2k} + 2b_1b_{2k-1} + \cdots + 2b_{k-1}b_{k+1} + b_k^2 \\
X^{2m-2k-1} & : & 2b_0b_{2k+1} + 2b_1b_{2k} + \cdots + 2b_kb_{k+1} \\
\cdots\cdots & : & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}
$$

If we want to find $g(X)$ and $r(X)$ so that $f(X) = g(X)^2 + r(X)$, with $\deg(r(X)) < m$, we must solve the system of equations

$$
\begin{array}{rcl}
1 & = & b_0^2 \\
a_1 & = & 2b_0b_1 \\
a_2 & = & 2b_0b_2 + b_1^2 \\
a_3 & = & 2b_0b_3 + 2b_1b_2 \\
a_4 & = & 2b_0b_4 + 2b_1b_3 + b_2^2 \\
a_5 & = & 2b_0b_5 + 2b_1b_4 + 2b_2b_3 \\
\cdots\cdots & = & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
a_{2k} & = & 2b_0b_{2k} + 2b_1b_{2k-1} + \cdots + 2b_{k-1}b_{k+1} + b_k^2 \\
a_{2k+1} & = & 2b_0b_{2k+1} + 2b_1b_{2k} + \cdots + 2b_kb_{k+1} \\
\cdots\cdots & = & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
a_m & = & 2b_0b_m + 2b_1b_{m-1} + \cdots + 2b_{p-1}b_{p+1} + b_p^2 \quad \text{if } m = 2p, \text{ else} \\
a_m & = & 2b_0b_m + 2b_1b_{m-1} + \cdots + 2b_pb_{p+1} \quad \text{if } m = 2p+1.
\end{array}
$$

Observe that $b_0 = \pm 1$, but than once b_0 is determined, the coefficients $b_1, \ldots, b_m$ are uniquely determined. Therefore, $g(X)$ is uniquely determined, up to sign, and then, $r(X) = f(X) - g(X)^2$ is also uniquely determined.

B V.(b) We now assume that $k = \mathbb{Q}$ and that $f(X)$ has integer coefficients and is not the square of a polynomial in $\mathbb{Q}[X]$. We still assume that $f(X)$ is monic of even degree, since the result we wish to prove is *false* otherwise! Indeed, if say $f(X) = X^3$, then $Y^2 = X^3$ is satisfied whenever X is a square.

The key is this: If n is a positive integer and $r \in \mathbb{Z}$, then

$$n^2 + r \text{ is } \textit{not} \text{ a square if either } 0 < r \leq 2n \text{ or } -2n + 2 \leq r < 0.$$

Indeed, $(n+1)^2 = n^2+2n+1$, and if $0 < r \leq 2n$, then $n^2 < n^2+r < (n+1)^2$, so n^2+r is not a square. Similarly, $(n-1)^2 = n^2-2n+1$, and if $-2n+2 \leq r < 0$, then $(n-1)^2 < n^2+r < n^2$, so $n^2 + r$ is not a square.

For a numerical example, consider $f(X) = X^4+X^3+1$. Clearly $f(X)$ is a perfect square for

$$\begin{aligned} X = -2; &\quad f(-2) &= 9 \\ X = -1; &\quad f(-1) &= 1 \\ X = 0; &\quad f(0) &= 1 \\ X = 2; &\quad f(2) &= 25. \end{aligned}$$

Also, $f(-3) = 81 - 9 + 1 = 73$, not a square. We claim that these are the only solutions. For this, we express $f(X)$ as $g(X)^2 + r(X)$, as above. We get

$$f(X) = X^4 + X^3 + 1 = \frac{1}{64}((8X^2 + 4X - 1)^2 + 8X + 63).$$

Clearly, if $(8X^2 + 4X - 1)^2 + 8X + 63$ is not a square, then $f(X)$ is not a square, and we claim that this is the case for $X \leq -4$ or $X \geq 3$.

If $X \geq 3$ then $8X^2 + 4X - 1 > 0$ and $8X + 63 > 0$, and by the criterion stated above, if

$$8X + 63 \leq 2(8X^2 + 4X - 1)$$

then $(8X^2 + 4X - 1)^2 + 8X + 63$ is not a square. This will be the case if

$$8X + 63 \leq 16X^2 + 8X - 2,$$

that is, if $16X^2 \geq 65$, which holds if $X \geq 3$.

If $X \leq -4$, then $8X^2 + 4X - 1 > 0$ and $8X + 63 < 0$, by the criterion stated above, if

$$-2(8X^2 + 4X - 1) + 2 \leq 8X + 63$$

then $(8X^2 + 4X - 1)^2 + 8X + 63$ is not a square. This will be the case if

$$-16X^2 - 8X + 4 \leq 8X + 63,$$

that is, if $16X^2 \geq -16X - 59$, which holds if $X \leq -4$.

Now, in general, we claim that there is some (possible large) $K > 0$ so that for $|X| \geq K$, $f(X)$ is not a square.

We use a slightly modified version our criterion that allows us to treat the cases $r < 0$ and $r > 0$ uniformly. Recall that we showed that if n is a positive integer and $r \in \mathbb{Z}$, then

$$n^2 + r \text{ is } \textit{not} \text{ a square if either } 0 < r \leq 2n \text{ or } -2n + 2 \leq r < 0.$$

It follows that if n is a positive integer and $r \in \mathbb{Z}$, then

$$n^2 + r \text{ is } \textit{not} \text{ a square if either } 0 < r \leq 2n - 2 \text{ or } 0 < -r \leq 2n - 2.$$

From B V.(a), we may write

$$f(X) = \frac{g(X)^2 + r(X)}{N},$$

where $h(X), r(X) \in \mathbb{Z}[X]$, $N \in \mathbb{N}$, $\deg(g(X)) = m$ and $\deg(r(X)) = p < m$. We want to show that for $|X|$ large enough, $g(X)^2 + r(X)$ is not a square. We can write $g(X) = aX^m + O(X^{m-1})$ and $r(X) = bX^p + O(X^{p-1})$, where $O(X^{m-1})$ stands for a polynomial of degree at most $m - 1$ (and similarly for $r(X)$). Now, for $|X|$ large, $g(X) \approx aX^m$ and $r(X) \approx aX^p$.

First, assume $X >> 0$ (i.e., $X > 0$ and large). We may assume that $g(X) > 0$ and $r(X) > 0$, since otherwise we use $-g(X)$ and $-r(X)$ in the above criterion. So, we must have $a, b > 0$, and the condition

$$bX^p \leq 2aX^m - 2$$

can certainly be fulfilled for $X > 0$ large enough, since $p < m$.

Now, assume $X << 0$. Again, we may assume that $g(X) > 0$ and $r(X) > 0$. Then, either m is even and $a > 0$, or m is odd and $a < 0$. So, we can replace X by $-X$ and in the second case, a by $-a$, and we are back to the case where $X >> 0$ and $a > 0$. We can do the same thing with bX^p, and again, the condition

$$bX^p \leq 2aX^m - 2$$

is fulfilled for $X > 0$ large enough, since $p < m$.

B VI. We have to prove that the $\mathbb{Z}$-module

$$M = \prod_{\mathbb{N}} \mathbb{Z}$$

is not projective (even though, each factor, $\mathbb{Z}$, is projective).

To do so, we will use the following lemma, whose proof is given a little later.

Lemma 1.7 *Every submodule of a free module over a P.I.D. is free.*

Lemma 1.7 implies that every projective module over a P.I.D. is free. Indeed, for every projective module, P, there is some (projective) module, $\widetilde{P}$, so that $P \coprod \widetilde{P} \cong F$, where F is a free module. So, the projective module, P, is a submodule of a free module, F (over a P.I.D.), and by Lemma 1.7, it is free.

Consequently, to prove that a module, M, over a P.I.D. is not projective, it is enough to prove that M has some submodule that is not free. This is because, as we just proved, over a P.I.D., any projective module is free, and by Lemma 1.7, again, every submodule of a free module is free.

It turns out that Lemma 1.7 follows from a more general proposition (whose proof is not harder than the proof of Lemma 1.7).

Proposition 1.8 *Let R be a ring and assume that every (left) ideal $\mathfrak{A} \neq (0)$ is projective. Then, every submodule of a free R-module is isomorphic to a coproduct of ideals (in R).*

Proof. Let F be a free R-module, and let $\{e_\lambda\}_{\lambda\in\Lambda}$ be a basis of F. Consider any submodule, M, of F, and for any nonempty subset, I, of Λ, let $F_I = \coprod_{i\in I} Re_i$ be the free module generated by the family of basis vectors, $\{e_i\}_{i\in I}$, and let $M_I = M \cap F_I$. Define $\mathcal{S}$ as the collection

$$\mathcal{S} = \left\{(I, \{\mathfrak{A}_j\}_{j\in J}) \mid J \subseteq I \subseteq \Lambda,\ J \neq \emptyset,\ \mathfrak{A}_j \text{ is an ideal in } R \text{ and } M_I \cong \coprod_{j\in J} \mathfrak{A}_j\right\}.$$

Observe that $\mathcal{S}$ is nonempty, since $(\{\lambda\}, R) \in \mathcal{S}$, for every $\lambda \in \Lambda$. Partially order $\mathcal{S}$ as follows:

$$(I, \{\mathfrak{A}_j\}_{j\in J}) \leq (I', \{\mathfrak{A}'_k\}_{k\in J'})$$

iff $I \subseteq I'$, $J \subseteq J'$, and $\mathfrak{A}_j = \mathfrak{A}'_j$ for all $j \in J$.

It is immediately checked that $\mathcal{S}$ is inductive (because every element of a coproduct of modules only has finitely many nonzero components). Thus, by Zorn's lemma, the set $\mathcal{S}$ has a maximal element, say $(I, \{\mathfrak{A}_j\}_{j\in J})$.

We claim that $I = \Lambda$, which establishes the lemma, since $M_\Lambda = M \cap F_\Lambda = M \cap F = M$.

If $I \neq \Lambda$, there is some $k \in \Lambda$ so that $k \notin I$; write $K = I \cup \{k\}$. We can't have $M_K = M_I$, since this would contradict the maximality of I. Thus, $M_K \neq M_I$. Then,

$$M_K = M_{I\cup\{k\}} = M \cap F_{I\cup\{k\}} = M \cap \left(F_I \coprod Re_k\right) = M_I \coprod M \cap (Re_k),$$

and we can define the homomorphism $\varphi\colon M_K \to R$ by projecting the second summand of $M_K = M_I \coprod M \cap (Re_k)$ onto R. If we let $\mathfrak{A}_k = \mathrm{Im}\,\varphi$, we see that $\mathfrak{A}_k$ is a nonzero ideal in R, since $M_K \neq M_I$ and, obviously, we have the exact sequence

$$0 \longrightarrow M_I \longrightarrow M_K \longrightarrow \mathfrak{A}_k \longrightarrow 0.$$

However, by the hypothesis on the ring R, the ideal $\mathfrak{A}_k$ is projective, so, the above sequence splits, i.e., we have

$$M_K \cong M_I \coprod \mathfrak{A}_k.$$

But, by definition of $\mathcal{S}$, we have $M_I \cong \coprod_{j\in J} \mathfrak{A}_j$, for some subset, J, of I. Therefore, we get

$$M_K \cong M_I \coprod \mathfrak{A}_k \cong \coprod_{j\in J\cup\{k\}} \mathfrak{A}_j,$$

contradicting the maximality of $(I, \{\mathfrak{A}_j\}_{j\in J})$. Therefore, we must have $I = \Lambda$, and we are done. $\square$

If R is a P.I.D., every nonzero ideal, $\mathfrak{A}$, in R is of the form Ra, for some $a \in R$; so, $\mathfrak{A} \cong R$, via the isomorphism $\lambda \in R \mapsto \lambda a \in \mathfrak{A}$, and $\mathfrak{A}$ is obviously projective. Then, Proposition 1.8 shows that every submodule, M, of a free module, F, over a P.I.D. is isomorphic to a coproduct, $\coprod_{i\in\Lambda} R$, i.e., M is free: This proves Lemma 1.7

Let K be the submodule of $M = \prod_{\mathbb{N}} \mathbb{Z}$ defined by

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

Our goal is to prove that K is *not* free. We will need the following standard proposition:

Proposition 1.9 *Given a commutative ring, R, if M is a left R-module and $\mathfrak{A}$ is an ideal in R, then $M/\mathfrak{A}M$ is a left $R/\mathfrak{A}$-module. In particular, if $\mathfrak{A}$ is a maximal ideal, then $M/\mathfrak{A}M$ is a vector space over the field $R/\mathfrak{A}$, and if M is a free module, then the cardinality of any basis for M is equal to the dimension the vector space $M/\mathfrak{A}M$. Thus, if M is a free module, any two bases of M have the same cardinality, called the rank of M.*

Proof. For instance, see *Algebra*, by Lang, or *Introduction to Homological Algebra*, by Rotman. $\square$

Observe that

$$(k_1 2, k_2 2^2, k_3 2^3, \ldots, k_n 2^n, \ldots) \in K$$

for all $(k_1, k_2, \ldots, k_n, \ldots) \in \mathbb{Z}^{\mathbb{N}}$, and so, $\#(K)$ is an uncountable cardinal. Now, if K were free, its rank would be uncountable, because if it were countable, we would have

$$K = \coprod_{\mathbb{N}} \mathbb{Z},$$

a countable union of countable sets, which is countable, a contradiction. Also observe that $2K$ is a submodule of K, and so, by Proposition 1.9, the factor module $K/2K$ is a vector space over $\mathbb{Z}/2\mathbb{Z}$, of the same dimension as K. Thus, $\dim(K/2K)$ would be uncountable. However, it is countable, as we will prove next. Thus, we get a contradiction and K is not free, and a fortiori, not projective.

Let $\overline{\xi}$ denote the image in $K/2K$ of any $\xi \in K$. If $\xi \in K$, by definition, there is some finite number, n, so that $2 \mid \xi_j$ for all $j > n$. Thus, we can write

$$\xi = (k_1, \ldots, k_n, 0, \ldots, 0) + 2\eta,$$

where we also have $\eta \in K$. Then,

$$\overline{\xi} = (k_1 \pmod 2)e_1 + \cdots + (k_n \pmod 2)e_n,$$

where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0, \ldots)$, with 1 in the ith slot, and this shows that $K/2K$ is generated by countably many vectors, as claimed.