11. Finitely-generated modules

1. *Free modules*

The following definition is an example of defining things by *mapping properties*, that is, by the way the object relates to other objects, rather than by internal structure. The first proposition, which says that there is at most one such thing, is typical, as is its proof.

Let R be a commutative ring with 1. Let S be a set. A **free R-module** M on **generators** S is an R-module M and a set map $i : S \longrightarrow M$ such that, for any R-module N and any set map $f : S \longrightarrow N$, there is a unique R-module homomorphism $\tilde{f} : M \longrightarrow N$ such that

$$\tilde{f} \circ i = f : S \longrightarrow N$$

The elements of $i(S)$ in M are an R-**basis** for M.

[1.0.1] Proposition: If a free R-module M on generators S exists, it is unique up to unique isomorphism.

Proof: First, we claim that the only R-module homomorphism $F : M \longrightarrow M$ such that $F \circ i = i$ is the identity map. Indeed, by definition,[1] given $i : S \longrightarrow M$ there is a *unique* $\tilde{i} : M \longrightarrow M$ such that $\tilde{i} \circ i = i$. The identity map on M certainly meets this requirement, so, by uniqueness, $\tilde{i}$ can only be the identity.

Now let M' be another free module on generators S, with $i' : S \longrightarrow M'$ as in the definition. By the defining property of (M, i), there is a unique $\widetilde{i'} : M \longrightarrow M'$ such that $\widetilde{i'} \circ i = i'$. Similarly, there is a unique $\tilde{i}$ such that $\tilde{i} \circ i' = i$. Thus,

$$i = \tilde{i} \circ i' = \tilde{i} \circ \widetilde{i'} \circ i$$

[1] Letting letting $i : S \longrightarrow M$ take the role of $f : S \longrightarrow N$ in the definition.

Similarly,

$$i' = \widetilde{i'} \circ i = \widetilde{i'} \circ \tilde{i} \circ i'$$

From the first remark of this proof, this shows that

$$\tilde{i} \circ \widetilde{i'} = \text{ identity map on } M$$

$$\widetilde{i'} \circ \tilde{i} = \text{ identity map on } M'$$

So $\widetilde{i'}$ and $\tilde{i}$ are mutual inverses. That is, M and M' are isomorphic, and in a fashion that respects the maps i and i'. Further, by uniqueness, there is no *other* map between them that respects i and i', so we have a *unique* isomorphism. ///

Existence of a free module remains to be demonstrated. We should be relieved that the uniqueness result above assures that any successful construction will invariably yield the same object. Before proving existence, and, thus, before being burdened with irrelevant internal details that arise as artifacts of the construction, we prove the basic facts about free modules.

[1.0.2] **Proposition:** A free R-module M on generators $i : S \longrightarrow M$ is *generated by* $i(S)$, in the sense that the only R-submodule of M containing the image $i(S)$ is M itself.

Proof: Let N be the submodule generated by $i(S)$, that is, the intersection of all submodules of M containing $i(S)$. Consider the quotient M/N, and the map $f : S \longrightarrow M/N$ by $f(s) = 0$ for all $s \in S$. Let $\zeta : M \longrightarrow M/N$ be the 0 map. Certainly $\zeta \circ i = f$. If $M/N \neq 0$, then the quotient map $q : M \longrightarrow M/N$ is not the zero map ζ, and also $q \circ i = f$. But this would contradict the uniqueness in the definition of M. ///

For a set X of elements of an R-module M, if a relation

$$\sum_{x \in X} r_x \, x = 0$$

with $r_x \in R$ and $x \in M$ (with all but finitely-many coefficients r_x being 0) implies that *all* coefficients r_x are 0, say that the elements of X are **linearly independent** (over R).

[1.0.3] **Proposition:** Let M be a free R-module on generators $i : S \longrightarrow M$. Then any relation (with finitely-many non-zero coefficients $r_s \in R$)

$$\sum_{s \in S} r_s \, i(s) = 0$$

must be trivial, that is, all coefficients r_s are 0. That is, the elements of $i(S)$ are *linearly independent.*

Proof: Suppose $\sum_s r_s \, i(s) = 0$ in the free module M. To show that every coefficient r_s is 0, fix $s_o \in S$ and map $f : S \longrightarrow R$ itself by

$$f(s) = \begin{cases} 0 & (s \neq s_o) \\ 1 & (s = s_o) \end{cases}$$

Let $\tilde{f}$ be the associated R-module homomorphism $\tilde{f} : M \longrightarrow R$. Then

$$0 = \tilde{f}(0) = \tilde{f}(\sum_s r_s \, i(s)) = r_{s_o}$$

This holds for each fixed index s_o, so any such relation is trivial. ///

[1.0.4] **Proposition:** Let $f : B \longrightarrow C$ be a *surjection* of R-modules, where C is free on generators S with $i : S \longrightarrow C$. Then there is an injection $j : C \longrightarrow B$ such that [2]

$$f \circ j = 1_C \quad \text{and} \quad B = (\ker f) \oplus j(C)$$

[1.0.5] **Remark:** The map $j : C \longrightarrow B$ of this proposition is a **section** of the surjection $f : B \longrightarrow C$.

Proof: Let $\{b_s : s \in S\}$ be any set of elements of B such that $f(b_s) = i(s)$. Invoking the universal property of the free module, given the choice of $\{b_x\}$ there is a unique R-module homomorphism $j : C \longrightarrow B$ such that $(j \circ i)(s) = b_s$. It remains to show that $jC \oplus \ker f = B$. The intersection $jC \cap \ker f$ is trivial, since for $\sum_s r_s\, j(s)$ in the kernel (with all but finitely-many r_s just 0)

$$C \ni 0 = f\left(\sum_s r_s\, j(s)\right) = \sum_s r_s\, i(s)$$

We have seen that any such relation must be trivial, so the intersection $f(C) \cap kerf$ is trivial.

Given $b \in B$, let $f(b) = \sum_s r_s\, i(s)$ (a finite sum), using the fact that the images $i(s)$ generate the free module C. Then

$$f(b - j(f(b))) = f(b - \sum_s r_s b_s) == f(b) - \sum_s r_s f(b_s) = \sum_s r_s i(s) - \sum_s r_s i(s) = 0$$

Thus, $j(C) + \ker f = B$. ///

We have one more basic result before giving a construction, and before adding any hypotheses on the ring R.

The following result uses an interesting trick, reducing the problem of counting generators for a free module F over a commutative ring R with 1 to counting generators for vector spaces over a field R/M, where M is a maximal proper ideal in R. We see that the number of generators for a free module over a commutative ring R with unit 1 has a well-defined cardinality, the **R-rank** of the free module.

[1.0.6] **Theorem:** Let F be a free R-module on generators $i : S \longrightarrow F$, where R is a commutative ring with 1. Suppose that F is also a free R-module on generators $j : T \longrightarrow F$. Then $|S| = |T|$.

Proof: Let M be a maximal proper ideal in R, so $k = R/M$ is a field. Let

$$E = M \cdot F = \text{ collection of finite sums of elements } mx,\ m \in M, x \in F$$

and consider the quotient

$$V = F/E$$

with quotient map $q : F \longrightarrow V$. This quotient has a canonical k-module structure

$$(r + M) \cdot (x + M \cdot F) = rx + M \cdot F$$

We claim that V is a *free* k-module on generators $q \circ i : S \longrightarrow V$, that is, is a vector space on those generators. Lagrange's replacement argument shows that the cardinality of the number of generators for a *vector space* over a field is well-defined, so a successful comparison of generators for the original module and this vector space quotient would yield the result.

[2] The property which we are about to prove is enjoyed by free modules is the *defining* property of **projective** modules. Thus, in these terms, we are proving that *free modules are projective.*

To show that V is free over k, consider a set map $f : S \longrightarrow W$ where W is a k-vectorspace. The k-vectorspace W has a natural R-module structure compatible with the k-vectorspace structure, given by

$$r \cdot (x + M \cdot F) = rx + M \cdot F$$

Let $\tilde{f} : F \longrightarrow W$ be the unique R-module homomorphism such that $\tilde{f} \circ i = f$. Since $m \cdot w = 0$ for any $m \in M$ and $w \in W$, we have

$$0 = m \cdot f(s) = m \cdot \tilde{f}(i(s)) = \tilde{f}(m \cdot i(s))$$

so

$$\ker \tilde{f} \supset M \cdot F$$

Thus, $\bar{f} : V \longrightarrow W$ defined by

$$\bar{f}(x + M \cdot F) = \tilde{f}(x)$$

is *well*-defined, and $\bar{f} \circ (q \circ i) = f$. This proves the existence part of the defining property of a free module.

For uniqueness, the previous argument can be reversed, as follows. Given $\bar{f} : V \longrightarrow W$ such that $\bar{f} \circ (q \circ i) = f$, let $\tilde{f} = \bar{f} \circ q$. Since there is a unique $\tilde{f} : F \longrightarrow W$ with $\tilde{f} \circ i = f$, there is at most one $\bar{f}$. ///

Finally, we *construct* free modules, as a proof of existence. [3]

Given a non-empty set S, let M be the set of R-valued functions on S which take value 0 outside a finite subset of S (which may depend upon the function). Map $i : S \longrightarrow M$ by letting $i(s)$ be the function which takes value 1 at $s \in S$ and is 0 otherwise. Add functions value-wise, and let R act on M by value-wise multiplication.

[1.0.7] Proposition: The M and i just constructed is a free module on generators S. In particular, given a set map $f : S \longrightarrow N$ for another R-module N, for $m \in M$ define $\tilde{f}(m) \in N$ by [4]

$$\tilde{f}(m) = \sum_{s \in S} m(s) \cdot f(s)$$

Proof: We might check that the explicit expression (with only finitely-many summands non-zero) is an R-module homomorphism: that it respects addition in M is easy. For $r \in R$, we have

$$\tilde{f}(r \cdot m) = \sum_{s \in S} (r \cdot m(s)) \cdot f(s) = r \cdot \sum_{s \in S} m(s) \cdot f(s) = r \cdot \tilde{f}(m)$$

And there should be no *other* R-module homomorphism from M to N such that $\tilde{f} \circ i = f$. Let $F : M \longrightarrow N$ be another one. Since the elements $\{i(s) : s \in S\}$ generate M as an R-module, for an arbitrary collection $\{r_s \in R : s \in S\}$ with all but finitely-many 0,

$$F\left(\sum_{s \in S} r_s \cdot i(s)\right) = \sum_{s \in S} r_s \cdot F(i(s)) = \sum_{s \in S} r_s \cdot f(s) = \tilde{f}\left(\sum_{s \in S} r_s \cdot i(s)\right)$$

so necessarily $F = \tilde{f}$, as desired. ///

[3] Quite pointedly, the previous results did not use any explicit internal details of what a free module might be, but, rather, only invoked the external mapping properties.

[4] In this formula, the function m on S is non-zero only at finitely-many $s \in S$, so the sum is finite. And $m(s) \in R$ and $f(s) \in N$, so this expression is a finite sum of R-multiples of elements of N, as required.

[1.0.8] Remark: For finite generator sets often one takes

$$S = \{1, 2, \ldots, n\}$$

and then the construction above of the free module on generators S can be identified with the collection R^n of ordered n-tuples of elements of R, as usual.

---

2. *Finitely-generated modules over a domain*

In the sequel, the results will mostly require that R be a domain, or, more stringently, a principal ideal domain. These hypotheses will be carefully noted.

[2.0.1] Theorem: Let R be a principal ideal domain. Let M be a free R-module on generators $i : S \longrightarrow M$. Let N be an R-submodule. Then N is a free R-module on at most $|S|$ generators. [5]

Proof: Induction on the cardinality of S. We give the proof for *finite* sets S. First, for $M = R^1 = R$ a free module on a single generator, an R-submodule is an ideal in R. The hypothesis that R is a PID assures that every ideal in R needs at most one generator. This starts the induction.

Let $M = R^m$, and let $p : R^m \longrightarrow R^{m-1}$ be the map

$$p(r_1, r_2, r_3, \ldots, r_m) = (r_2, r_3, \ldots, r_m)$$

The image $p(N)$ is free on $\leq m - 1$ generators, by induction. From the previous section, there is always a *section* $j : p(N) \longrightarrow N$ such that $p \circ j = 1_{p(N)}$ and

$$N = \ker p|_N \oplus j(p(N))$$

Since $p \circ j = 1_{p(N)}$, necessarily j is an injection, so is an isomorphism to its image, and $j(p(N))$ is free on $\leq m-1$ generators. And $\ker p|_N$ is a submodule of R, so is free on at most 1 generator. We would be done if we knew that a direct sum $M_1 \oplus M_2$ of free modules M_1, M_2 on generators $i_1 : S_i \longrightarrow M_1$ and $i_2 : S_2 \longrightarrow M_2$ is a free module on the *disjoint* union $S = S_1 \cup S_2$ of the two sets of generators. We excise that argument to the following proposition. ///

[2.0.2] Proposition: A direct sum[6] $M = M_1 \oplus M_2$ of free modules M_1, M_2 on generators $i_1 : S_i \longrightarrow M_1$ and $i_2 : S_2 \longrightarrow M_2$ is a free module on the *disjoint* union $S = S_1 \cup S_2$ of the two sets of generators. [7]

Proof: Given another module N and a set map $f : S \longrightarrow N$, the restriction f_j of f to S_j gives a unique module homomorphism $\tilde{f}_j : M_j \longrightarrow M$ such that $\tilde{f}_j \circ i_j = f_j$. Then

$$\tilde{f}(m_1,\ m_2) = (f_1 m_1,\ f_2 m_2)$$

---

[5] The assertion of the theorem is false without some hypotheses on R. For example, even in the case that M has a *single* generator, to know that every submodule needs at most a single generator is exactly to assert that every ideal in R is principal.

[6] Though we will not use it at this moment, one can give a definition of *direct sum* in the same mapping-theoretic style as we have given for *free module*. That is, the direct sum of a family $\{M_\alpha : \alpha \in A\}$ of modules is a module M and homomorphisms $i_\alpha : M_\alpha \longrightarrow M$ such that, for every family of homomorphisms $f_\alpha : M_\alpha \longrightarrow N$ to another module N, there is a unique $f : M \longrightarrow N$ such that every f_α **factors through** f in the sense that $f_\alpha = f \circ i_\alpha$.

[7] This does not need the assumption that R is a principal ideal domain.

is *a* module homomorphism from the direct sum to N with $\tilde{f} \circ i = f$. On the other hand, given any map $g : M \longrightarrow N$ such that $g \circ i = f$, by the uniqueness on the summands M_1 and M_2 inside M, if must be that $g \circ i_j = f_j$ for $j = 1, 2$. Thus, this g is $\tilde{f}$. ///

For an R-module M, for $m \in M$ the **annihilator** $\mathrm{Ann}_R(m)$ of m in R is

$$\mathrm{Ann}_R(m) = \{r \in R : rm = 0\}$$

It is easy to check that the annihilator is an ideal in R. An element $m \in M$ is a **torsion element** of M if its annihilator is not the 0 ideal. The **torsion submodule** M^{tors} of M is

$$M^{\mathrm{tors}} = \{m \in M : \mathrm{Ann}_R(m) \neq \{0\}\}$$

A module is **torsion free** if its torsion submodule is trivial.

[2.0.3] **Proposition:** For a domain R, the torsion submodule M^{tors} of a given R-module M is an R-submodule of M, and M/M^{tors} is torsion-free.

Proof: For torsion elements m, n in M, let x be a non-zero element of $\mathrm{Ann}_R(m)$ and y a non-zero element of $\mathrm{Ann}_(n)$. Then $xy \neq 0$, since R is a domain, and

$$(xy)(m + n) = y(xm) + x(yn) = y \cdot 0 + x \cdot 0 = 0$$

And for $r \in R$,

$$x(rm) = r(xm) = r \cdot 0 = 0$$

Thus, the torsion submodule *is* a submodule.

To show that the quotient M/M^{tors} is torsion free, suppose $r \cdot (m + M^{\mathrm{tors}}) \subset M^{\mathrm{tors}}$ for $r \neq 0$. Then $rm \in M^{\mathrm{tors}}$. Thus, there is $s \neq 0$ such that $s(rm) = 0$. Since R is a domain, $rs \neq 0$, so m itself is torsion, so $m + M^{\mathrm{tors}} = M^{\mathrm{tors}}$, which is 0 in the quotient. ///

An R-module M is **finitely generated** if there are finitely-many $m_1, \ldots, m_n$ such that $\sum_i Rm_i = M$. [8]

[2.0.4] **Proposition:** Let R be a domain. [9] Given a finitely-generated [10] R-module M, there is a (not necessarily unique) maximal free submodule F, and M/F is a torsion module.

Proof: Let X be a set of generators for M, and let S be a maximal subset of X such that (with inclusion $i : S \longrightarrow M$) the submodule generated by S is free. To be careful, consider why there is such a maximal subset. First, for ϕ not to be maximal means that there is $x_1 \in X$ such that $Rx_1 \subset M$ is free on generator $\{x_1\}$. If $\{x_1\}$ is not maximal with this property, then there is $x_2 \in X$ such that $Rx_1 + Rx_2$ is free on generators $\{x_1, x_2\}$. Since X is finite, there is no issue of infinite ascending unions of free modules. Given $x \in X$ but not in S, by the maximality of S there are coefficients $0 \neq r \in R$ and $r_s \in R$ such that

$$rx + \sum_{s \in S} r_s \cdot i(s) = 0$$

[8] This is equivalent to saying that the m_i *generate* M in the sense that the intersection of submodules containing all the m_i is just M itself.

[9] The hypothesis that the ring R is a domain assures that if $r_i x_i = 0$ for $i = 1, 2$ with $0 \neq r_i \in R$ and x_i in an R-module, then not only $(r_1 r_2)(x_1 + x_2) = 0$ but *also* $r_1 r_2 \neq 0$. That is, the notion of *torsion module* has a simple sense over domains R.

[10] The conclusion is false in general without an assumption of finite generation. For example, the $\mathbb{Z}$-module $\mathbb{Q}$ is the ascending union of the free $\mathbb{Z}$-modules $\frac{1}{N} \cdot \mathbb{Z}$, but is itself not free.

so M/F is torsion. ///

[2.0.5] **Theorem:** Over a principal ideal domain R a finitely-generated torsion-free module M is free.

Proof: Let X be a finite set of generators of M. From the previous proposition, let S be a maximal subset of X such that the submodule F generated by the inclusion $i : S \longrightarrow M$ is free. Let $x_1, \ldots, x_n$ be the elements of X not in S, and since M/F is torsion, for each x_i there is $0 \neq r_i \in R$ be such that $r_i x_i \in F$. Let $r = \prod_i r_i$. This is a finite product, and is non-zero since R is a domain. Thus, $r \cdot M \subset F$. Since F is free, rM is free on at most $|S|$ generators. Since M is torsion-free, the multiplication by r map $m \longrightarrow rm$ has trivial kernel in M, so $M \approx rM$. That is, M is free. ///

[2.0.6] **Corollary:** Over a principal ideal domain R a finitely-generated module M is expressible as

$$M \approx M^{\mathrm{tors}} \oplus F$$

where F is a free module and M^{tors} is the torsion submodule of M.

Proof: We saw above that M/M^{tors} is torsion-free, so (being still finitely-generated) is free. The quotient map $M \longrightarrow M/M^{\mathrm{tors}}$ admits a section $\sigma : M/M^{\mathrm{tors}} \longrightarrow M$, and thus

$$M = M^{\mathrm{tors}} \oplus \sigma(M/M^{\mathrm{tors}}) = M^{\mathrm{tors}} \oplus \ \ \text{free}$$

as desired. ///

[2.0.7] **Corollary:** Over a principal ideal domain R, a submodule N of a finitely-generated R-module M is finitely-generated.

Proof: Let F be a finitely-generated free module which surjects to M, for example by choosing generators S for M and then forming the free module on S. The inverse image of N in F is a submodule of a free module on finitely-many generators, so (from above) needs at most that many generators. Mapping these generators forward to N proves the finite-generation of N. ///

[2.0.8] **Proposition:** Let R be a principal ideal domain. Let $e_1, \ldots, e_k$ be elements of a finitely-generated free R-module M which are linearly independent over R, and such that

$$M/(Re_1 + \ldots + Re_k) \quad \text{is torsion-free, hence free}$$

Then this collection can be extended to an R-basis for M.

Proof: Let N be the submodule $N = Re_1 + \ldots + Re_k$ generated by the e_i. The quotient M/N, being finitely-generated and torsion-less, is free. Let $e_{k+1}, \ldots, e_n$ be elements of M whose images in M/N are a basis for M/N. Let $q : M \longrightarrow M/N$ be the quotient map. Then, as above, q has a *section* $\sigma : M/N \longrightarrow M$ which takes $q(e_i)$ to e_i. And, as above,

$$M = \ker q \oplus \sigma(M/N) = N \oplus \sigma(M/N)$$

Since $e_{k+1}, \ldots, e_n$ is a basis for M/N, the collection of *all* $e_1, \ldots, e_n$ is a basis for M. ///

---

3. *PIDs are UFDs*

We have already observed that *Euclidean* rings are unique factorization domains and are principal ideal domains. The two cases of greatest interest are the ordinary integers $\mathbb{Z}$ and polynomials $k[x]$ in one variable over a field k. But, also, we do have

[3.0.1] Theorem: A principal ideal domain is a unique factorization domain.

Before proving this, there are relatively elementary remarks that are of independent interest, and useful in the proof. Before anything else, keep in mind that in a *domain* R (with identity 1), for $x, y \in R$,

$$Rx = Ry \quad \text{if and only if} \quad x = uy \ \text{ for some unit } u \in R^\times$$

Indeed, $x \in Ry$ implies that $x = uy$, while $y \in Rx$ implies $y = vx$ for some v, and then $y = uv \cdot y$ or $(1 - uv)y = 0$. Since R is a domain, either $y = 0$ (in which case this discussion was trivial all along) or $uv = 1$, so u and v are units, as claimed.

Next recall that divisibility $x|y$ is inclusion-reversion for the corresponding ideals, that is

$$Rx \supset Ry \quad \text{if and only if} \quad x|y$$

Indeed, $y = mx$ implies $y \in Rx$, so $Ry \subset Rx$. Conversely, $Ry \subset Rx$ implies $y \in Rx$, so $y = mx$ for some $m \in R$.

Next, given x, y in a PID R, we claim that $g \in R$ such that

$$Rg = Rx + Ry$$

is a greatest common divisor for x and y, in the sense that for any $d \in R$ dividing both x and y, also d divides g (and g itself divides x and y). Indeed, $d|x$ gives $Rx \subset Rd$. Thus, since Rd is closed under addition, any common divisor d of x and y has

$$Rx + Ry \subset Rd$$

Thus, $g \in Rg \subset Rd$, so $g = rd$ for some $r \in R$. And $x \in Rg$ and $y \in Rg$ show that this g does divide both x and y.

Further, note that since a *gcd* $g = \gcd(x, y)$ of two elements x, y in the PID R is a generator for $Rx + Ry$, this *gcd* is expressible as $g = rx + sy$ for some $r, s \in R$.

In particular, a point that starts to address unique factorization is that an *irreducible* element p in a PID R is *prime*, in the sense that $p|ab$ implies $p|a$ or $p|b$. Indeed, the proof is the same as for integers, as follows. If p does *not* divide a, then the irreducibility of p implies that $1 = \gcd(p, a)$, since (by definition of *irreducible*) p has no proper divisors. Let $r, s \in R$ be such that $1 = rp + sa$. Let $ab = tp$. Then

$$b = b \cdot 1 = b \cdot (rp + sa) = br \cdot p + s \cdot ab = p \cdot (br + st)$$

and, thus, b is a multiple of p.

[3.0.2] Corollary: *(of proof)* Any ascending chain

$$I_1 \subset I_2 \subset \ldots$$

of ideals in a principal ideal domain is *finite*, in the sense that there is an index i such that

$$I_i = I_{i+1} = I_{i+2} = \ldots$$

That is, a PID is **Noetherian**.

Proof: First, prove the Noetherian property, that any ascending chain of proper ideals

$$I_1 \subset I_2 \subset \ldots$$

in R must be finite. Indeed, the union I is still a proper ideal, since if it contained 1 some I_i would already contain 1, which is not so. Further, $I = Rx$ for some $x \in R$, but x must lie in some I_i, so already $I = I_i$. That is,

$$I_i = I_{i+1} = I_{i+2} = \ldots$$

Let r be a non-unit in R. If r has no proper factorization $r = xy$ (with neither x nor y a unit), then r is irreducible, and we have factored r. Suppose r has no factorization into irreducibles. Then r itself is *not* irreducible, so factors as $r = x_1 y_1$ with neither x_1 nor y_1 a unit. Since r has no factorization into irreducibles, one of x_1 or y_1, say y_1, has no factorization into irreducibles. Thus, $y_1 = x_2 y_2$ with neither x_2 nor y_2 a unit. Continuing, we obtain a chain of inclusions

$$Rr \subset Ry_1 \subset Ry_2 \subset \ldots$$

with all inclusions *strict*. This is impossible, by the Noetherian-ness property just proven. [11] That is, all ring elements have factorizations into irreducibles.

The more serious part of the argument is the *uniqueness* of the factorization, up to changing irreducibles by units, and changing the ordering of the factors. Consider

$$p_1^{e_1} \ldots p_m^{e_m} = (\text{unit}) \cdot q_1^{f_1} \ldots q_n^{f_n}$$

where the p_i and q_j are irreducibles, and the exponents are positive integers. The fact that $p_1 | ab$ implies $p_1 | a$ or $p_1 | b$ (from above) shows that p_1 must differ only by a unit from one of the q_j. Remove this factor from both sides and continue, by induction. ///

---

4. *Structure theorem, again*

The form of the following theorem is superficially stronger than our earlier version, and is more useful.

[4.0.1] **Theorem:** Let R be a principal ideal domain, M a finitely-generated free module over R, and N an R-submodule of M. Then there are elements [12] $d_1 | \ldots | d_t$ of R, uniquely determined up to $\mathbb{R}^\times$, and an R-module basis $m_1, \ldots, m_t$ of M, such that $d_1 e_1, \ldots, d_t e_t$ is an R-basis of N (or $d_i e_i = 0$).

Proof: From above, the quotient M/N has a well-defined torsion submodule T, and $F = (M/N)/T$ is free. Let $q : M \longrightarrow (M/N)/T$ be the quotient map. Let $\sigma : F \longrightarrow M$ be a section of q, such that

$$M = \ker q \oplus \sigma(F)$$

Note that $N \subset \ker q$, and $(\ker q)/N$ is a torsion module. The submodule $\ker q$ of M is canonically defined, though the free complementary submodule [13] $\sigma(F)$ is not. Since $\sigma(F)$ can be described as a sum of a uniquely-determined (from above) number of copies $R/\langle 0 \rangle$, we see that this free submodule in M complementary to $\ker q$ gives the 0 elementary divisors. It remains to treat the finitely-generated torsion module $(\ker q)/N$. Thus, without loss of generality, suppose that M/N is torsion (finitely-generated).

[11] Yes, this proof actually shows that in *any* Noetherian commutative ring with 1 every element has a factorization into irreducibles. This does not accomplish much, however, as the *uniqueness* is far more serious than *existence* of factorization.

[12] Elementary divisors.

[13] Given a submodule A of a module B, a **complementary submodule** A' to A in B is another submodule A' of B such that $B = A \oplus A'$. In general, submodules do not admit complementary submodules. Vector spaces over fields are a marked exception to this failure.

For λ in the set of R-linear *functionals* $\mathrm{Hom}_R(M,R)$ on M, the image $\lambda(M)$ is an ideal in R, as is the image $\lambda(N)$. Let λ be such that $\lambda(N)$ is *maximal* among all ideals occurring as $\lambda(N)$. [14] Let $\lambda(N) = Rx$ for some $x \in R$. We claim that $x \neq 0$. Indeed, express an element $n \in N$ as $n = \sum_i r_i e_i$ for a basis e_i of M with $r_i \in R$, and with respect to this basis define dual functionals $\mu_i \in \mathrm{Hom}_R(M,R)$ by

$$\mu_i(\sum_j s_j\, e_j) = e_i \quad \text{(where } s_j \in R)$$

If $n \neq 0$ then some coefficient r_i is non-zero, and $\mu_i(n) = r_i$. Take $n \in N$ such that $\lambda(n) = x$.

Claim $\mu(n) \in Rx$ for any $\mu \in \mathrm{Hom}_R(M,R)$. Indeed, if not, let $r, s \in R$ such that $r\lambda(n) + s\mu(n)$ is the *gcd* of the two, and $(r\lambda + s\mu)(N)$ is a strictly larger ideal than Rx, contradiction.

Thus, in particular, $\mu_i(n) \in Rx$ for all dual functionals μ_i for a given basis e_i of M. That is, $n = xm$ for some $m \in M$. Then $\lambda(m) = 1$. And

$$M = Rm \oplus \ker \lambda$$

since for any $m' \in M$

$$\lambda(m' - \lambda(m')m) = \lambda(m') - \lambda(m') \cdot 1 = 0$$

Further, for $n' \in N$ we have $\lambda(n') \in Rx$. Let $\lambda(n') = rx$. Then

$$\lambda(n' - r \cdot n) = \lambda(n') - r \cdot \lambda(n) = \lambda(n') - rx = 0$$

That is,

$$N = Rn \oplus \ker \lambda|_N$$

Thus,

$$M/N \approx Rm/Rn \oplus (\ker \lambda)/(\ker \lambda|_N)$$

with $n = xm$. And

$$Rm/Rn = Rm/Rxn \approx R/Rx = R/\langle x \rangle$$

The submodule $\ker \lambda$ is free, being a submodule of a free module over a PID, as is $\ker \lambda|_N$. And the number of generators is reduced by 1 from the number of generators of M. Thus, by induction, we have a basis $m_1, \ldots, m_t$ of M and $x_1, \ldots, x_t$ in R such that $n_i = x_i m_i$ is a basis for N, using functional λ_i whose kernel is $Rm_{i+1} + \ldots + Rm_t$, and $\lambda_i(n_i) = x_i$.

We claim that the above procedure makes $x_i | x_{i+1}$. By construction,

$$n_{i+1} \in \ker \lambda_i \quad \text{and } n_i \in \ker \lambda_{i+1}$$

Thus, with $r, s \in R$ such that $rx_i + sx_{i+1}$ is the greatest common divisor $g = \gcd(x_i, x_{i+1})$, we have

$$(r\lambda_i + s\lambda_{i+1})(n_i + n_{i+1}) = r \cdot \lambda_i(n_i) + r \cdot \lambda_i(n_{i+1}) + + s \cdot \lambda_{i+1}(n_i) + s \cdot \lambda_{i+1}(n_{i+1})$$

$$= r \cdot x_i + 0 + + 0 + s \cdot x_{i+1} = \gcd(x_i, x_{i+1})$$

That is, $Rg \supset Rx_i$ and $Rg \supset Rx_{i+1}$. The maximality property of Rx_i requires that $Rx_i = Rg$. Thus, $Rx_{i+1} \subset Rx_i$, as claimed.

This proves *existence* of a decomposition as indicated. Proof of *uniqueness* is far better treated after introduction of a further idea, namely, *exterior algebra*. Thus, for the moment, we will *not* prove uniqueness, but will defer this until the later point when we treat exterior algebra.

[14] At this point it is not clear that this maximal ideal is unique, but by the end of the proof we will see that it is. The fact that any ascending chain of proper ideals in a PID has a maximal element, that is, that a PID is *Noetherian*, is proven along with the proof that a PID is a unique factorization domain.

5. *Recovering the earlier structure theorem*

The above structure theorem on finitely-generated free modules M over PIDs R and submodules $N \subset M$ gives the structure theorem for finitely-generated modules as a corollary, as follows.

Let F be a finitely-generated R-module with generators[15] $f_1, \ldots, f_n$. Let $S = \{f_1, \ldots, f_n\}$, and let M be the free R-module on generators $i : S \longrightarrow M$. Let

$$q : M \longrightarrow F$$

be the unique R-module homomorphism such that $q(i(f_k)) = f_k$ for each generator f_k. Since $q(M)$ contains all the generators of F, the map q is surjective. [16]

Let $N = \ker q$, so by a basic isomorphism theorem

$$F \approx M/N$$

By the theorem of the last section, M has a basis $m_1, \ldots, m_t$ and there are uniquely determined [17] $r_1|r_2|\ldots|r_t \in R$ such that $r_1 m_1, \ldots, r_t m_t$ is a basis for N. Then

$$F \approx M/N \approx (Rm_1/Rr_1m_1) \oplus \ldots \oplus (Rm_t/Rrm_t) \approx R/\langle r_1 \rangle \oplus \ldots R/\langle r_t \rangle$$

since

$$Rm_i/Rr_im_i \approx R/\langle r_i \rangle$$

by

$$rm_i + Rr_im_i \longrightarrow r + Rr_i$$

This gives an expression for F of the sort desired. ///

6. *Submodules of free modules*

Let R be a principal ideal domain. Let A be a well-ordered set, and M a free module on generators e_α for $\alpha \in A$. Let N be a submodule of M.

For $\alpha \in A$, let

$$I_\alpha = \{r \in R : \text{ there exist } r_\beta,\ \beta < \alpha : r \cdot e_\alpha + \sum_{\beta<\alpha} r_\beta \cdot e_\beta \in N\}$$

Since R is a PID, the ideal I_α has a single generator ρ_α (which may be 0). Let $n_\alpha \in N$ be such that

$$n_\alpha = \rho_\alpha \cdot e_\alpha + \sum_{\beta<\alpha} r_\beta \cdot e_\beta$$

for some $r_\beta \in R$. This defines ρ_α and n_α for all $\alpha \in A$ by transfinite induction.

[6.0.1] **Theorem:** N is free on the (non-zero elements among) n_α.

---

[15] It does not matter whether or not this set is *minimal*, only that it be *finite*.

[16] We will have no further use for the generators f_k of F after having constructed the finitely-generated *free* module M which surjects to F.

[17] Uniquely determined up to units.

Proof: It is clear that I_α is an ideal in R, so at least one element n_α exists, though it may be 0. For any element $n \in N$ lying in the span of $\{e_\beta : \beta \le \alpha\}$, for some $r \in R$ the difference $n - rn_\alpha$ lies in the span of $\{e_\beta : \beta < \alpha\}$.

We claim that the n_α span N. Suppose not, and let $\alpha \in A$ be the first index such that there is $n \in N$ *not* in that span, with n expressible as $n = \sum_{\beta \le \alpha} r_\beta e_\beta$. Then $r_\alpha = r \cdot \rho_\alpha$ for some $r \in R$, and for suitable coefficients $s_\beta \in R$

$$n - rn_\alpha = \sum_{\beta<\alpha} s_\beta \cdot e_\beta$$

This element must still fail to be in the span of the n_γ's. Since that sum is finite, the supremum of the indices with non-zero coefficient is strictly less than α. This gives a contradiction to the minimality of α, proving that the n_α span N.

Now prove that the (non-zero) n_α's are linearly independent. Indeed, if we have a non-trivial (finite) relation

$$0 = \sum_\beta r_\beta \cdot n_\beta$$

let α be the highest index (among finitely-many) with $r_\alpha \ne 0$ and $n_\alpha \ne 0$. Since n_α is non-zero, it must be that $\rho_\alpha \ne 0$, and then the expression of n_α in terms of the basis $\{e_\gamma\}$ includes e_α with non-zero coefficient (namely, ρ_α). But no n_β with $\beta < \alpha$ needs e_α in its expression, so for suitable $s_\beta \in R$

$$0 = \sum_\beta r_\beta \cdot n_\beta = r_\alpha\, \rho_\alpha \cdot e_\alpha + \sum_{\beta<\alpha} s_\beta \cdot e_\beta$$

contradicting the linear independence of the e_α's. Thus, we conclude that the n_β's are linearly independent.
///

Exercises

11.[6.0.1] Find two integer vectors $x = (x_1, x_2)$ and $y = (y_1, y_2)$ such that $\gcd(x_1, x_2) = 1$ and $\gcd(y_1, y_2) = 1$, but $\mathbb{Z}^2/(\mathbb{Z}x + \mathbb{Z}y)$ has non-trivial torsion.

11.[6.0.2] Show that the $\mathbb{Z}$-module $\mathbb{Q}$ is torsion-free, but is *not* free.

11.[6.0.3] Let G be the group of positive rational numbers under multiplication. Is G a free $\mathbb{Z}$-module? Torsion-free? Finitely-generated?

11.[6.0.4] Let G be the quotient group $\mathbb{Q}/\mathbb{Z}$. Is G a free $\mathbb{Z}$-module? Torsion-free? Finitely-generated?

11.[6.0.5] Let $R = \mathbb{Z}[\sqrt{5}]$, and let $M = R \cdot 2 + R \cdot (1 + \sqrt{5}) \subset \mathbb{Q}(\sqrt{5})$. Show that M is *not* free over R, although it is torsion-free.

11.[6.0.6] Given an m-by-n matrix M with entries in a PID R, give an existential argument that there are matrices A (n-by-n) and B (m-by-m) with entries in R and with inverses with entries in R, such that AMB is *diagonal*.

11.[6.0.7] Describe an *algorithm* which, given a 2-by-3 integer matrix M, finds integer matrices A, B (with integer inverses) such that AMB is diagonal.

11.[6.0.8] Let A be a *torsion* abelian group, meaning that for every $a \in A$ there is $1 \leq n \in Z$ such that $n \cdot a = 0$. Let $A(p)$ be the subgroup of A consisting of elements a such that $p^\ell \cdot a = 0$ for some integer power p^ℓ of a prime p. Show that A is the direct sum of its subgroups $A(p)$ over primes p.

11.[6.0.9] (*) Let A be a subgroup of $\mathbb{R}^n$ such that in each ball there are finitely-many elements of A. Show that A is a free abelian group on at most n generators.