

(November 24, 2004)

# Free modules, finitely-generated modules

Paul Garrett <garrett@math.umn.edu>

EDIT: ... draft... more later...

- Free modules
  - Finitely-generated modules over domains
  - PIDs are UFDs
  - Structure theorem
- 

## 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  $i : S \rightarrow M$  such that, for any  $R$ -module  $N$  and any set map  $f : S \rightarrow N$ , there is a unique  $R$ -module homomorphism  $\tilde{f} : M \rightarrow N$  such that

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

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

**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  $F : M \rightarrow M$  such that  $F \circ i = i$  is the identity map. Indeed, by definition,<sup>[1]</sup> given  $i : S \rightarrow M$  there is a *unique*  $\tilde{i} : M \rightarrow M$  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  $i' : S \rightarrow M'$  as in the definition. By the defining property of  $(M, i)$ , there is a unique  $\tilde{i}' : M \rightarrow M'$  such that  $\tilde{i}' \circ i = i'$ . Similarly, there is a unique  $\tilde{i}$  such that  $\tilde{i} \circ i' = i$ . Thus,

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

Similarly,

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

From the first remark of this proof, this shows that

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

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

So  $\tilde{i}'$  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] Letting letting  $i : S \rightarrow M$  take the role of  $f : S \rightarrow N$  in the definition.

**Proposition:** A free  $R$ -module  $M$  on generators  $i : S \rightarrow M$  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  $f : S \rightarrow M/N$  by  $f(s) = 0$  for all  $s \in S$ . Let  $\zeta : M \rightarrow M/N$  be the 0 map. Certainly  $\zeta \circ i = f$ . If  $M/N \neq 0$ , then the quotient map  $q : M \rightarrow M/N$  is not the zero map  $\zeta$ , 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  $R$ ).

**Proposition:** Let  $M$  be a free  $R$ -module on generators  $i : S \rightarrow M$ . 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  $f : S \rightarrow R$  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  $\tilde{f} : M \rightarrow R$ . Then

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

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

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

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

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

*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  $j : C \rightarrow B$  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  $f(C) \cap \ker f$  is trivial.

[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*.

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.

**Theorem:** Let  $F$  be a free  $R$ -module on generators  $i : S \rightarrow F$ , where  $R$  is a commutative ring with 1. Suppose that  $F$  is also a free  $R$ -module on generators  $j : T \rightarrow F$ . 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  $q : F \rightarrow V$ . 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  $q \circ i : S \rightarrow V$ , 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.

To show that  $V$  is free over  $k$ , consider a set map  $f : S \rightarrow W$  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  $\tilde{f} : F \rightarrow W$  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,  $\bar{f} : V \rightarrow W$  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  $\bar{f} : V \rightarrow W$  such that  $\bar{f} \circ (q \circ i) = f$ , let  $\tilde{f} = \bar{f} \circ q$ . Since there is a unique  $\tilde{f} : F \rightarrow W$  with  $\tilde{f} \circ i = f$ , there is at most one  $\bar{f}$ . ///

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

---

[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.

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  $i : S \rightarrow M$  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.

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

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

*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  $F : M \rightarrow N$  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. ///

**Remark:** For finite generator sets often one takes

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

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.

**Theorem:** Let  $R$  be a principal ideal domain. Let  $M$  be a free  $R$ -module on generators  $i : S \rightarrow M$ . Let  $N$  be an  $R$ -submodule. Then  $N$  is a free  $R$ -module on at most  $|S|$  generators.<sup>[5]</sup>

*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  $p : R^m \rightarrow R^{m-1}$  be the map

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

<sup>[4]</sup> 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.

<sup>[5]</sup> 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.

The image  $p(N)$  is free on  $\leq m - 1$  generators, by induction. From the previous section, there is always a section  $j : p(N) \rightarrow N$  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  $i_1 : S_1 \rightarrow M_1$  and  $i_2 : S_2 \rightarrow M_2$  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. ///

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

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

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

is a module homomorphism from the direct sum to  $N$  with  $\tilde{f} \circ i = f$ . On the other hand, given any map  $g : M \rightarrow N$  such that  $g \circ i = f$ , by the uniqueness on the summands  $M_1$  and  $M_2$  inside  $M$ , it 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**  $\text{Ann}_R(m)$  of  $m$  in  $R$  is

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

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**  $M^{\text{tors}}$  of  $M$  is

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

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

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

*Proof:* For torsion elements  $m, n$  in  $M$ , let  $x$  be a non-zero element of  $\text{Ann}_R(m)$  and  $y$  a non-zero element of  $\text{Ann}_R(n)$ . 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  $M/M^{\text{tors}}$  is torsion free, suppose  $r \cdot (m + M^{\text{tors}}) \in M^{\text{tors}}$  for  $r \neq 0$ . Then  $rm \in M^{\text{tors}}$ . 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  $m + M^{\text{tors}} = M^{\text{tors}}$ , which is 0 in the quotient. ///

[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  $i_\alpha : M_\alpha \rightarrow M$  such that, for every family of homomorphisms  $f_\alpha : M_\alpha \rightarrow N$  to another module  $N$ , there is a unique  $f : M \rightarrow N$  such that every  $f_\alpha$  **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.

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

**Proposition:** Let  $R$  be a domain.<sup>[9]</sup> Given a finitely-generated<sup>[10]</sup>  $R$ -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  $i : S \rightarrow M$ ) the submodule generated by  $S$  is free. To be careful, consider why there is such a maximal subset. First, for  $\phi$  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

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

so  $M/F$  is torsion. ///

**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  $i : S \rightarrow M$  is free. Let  $x_1, \dots, x_n$  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  $m \rightarrow rm$  has trivial kernel in  $M$ , so  $M \approx rM$ . That is,  $M$  is free. ///

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

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

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

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

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

as desired. ///

**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  $N$ . ///

[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  $\mathbf{Z}$ -module  $\mathbf{Q}$  is the ascending union of the free  $\mathbf{Z}$ -modules  $\frac{1}{N} \cdot \mathbf{Z}$ , but is itself not free.

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

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

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

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

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

Since  $e_{k+1}, \dots, e_n$  is a basis for  $M/N$ , the collection of all  $e_1, \dots, e_n$  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  $\mathbf{Z}$  and polynomials  $k[x]$  in one variable over a field  $k$ . But, also, we do have

**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  $x, y \in R$ ,

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

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  $p$ .

**Corollary:** (*of proof*) Any ascending chain

$$I_1 \subset I_2 \subset \dots$$

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

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

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

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

$$I_1 \subset I_2 \subset \dots$$

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,

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

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

$$Rr \subset Ry_1 \subset Ry_2 \subset \dots$$

with all inclusions *strict*. This is impossible, by the Noetherian-ness property just proven. <sup>[11]</sup> 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

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

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

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

[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.

**Theorem:** Let  $R$  be a principal ideal domain. Let  $M$  be a finitely-generated free module over  $R$ , and  $N$  an  $R$ -submodule of  $M$ . Then there are elements<sup>[12]</sup>  $d_1 | \dots | d_t$  of  $R$ , uniquely determined up to  $\mathbf{R}^\times$ , and an  $R$ -module basis  $m_1, \dots, m_t$  of  $M$ , such that  $d_1 e_1, \dots, d_t e_t$  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  $q : M \rightarrow (M/N)/T$  be the quotient map. Let  $\sigma : F \rightarrow M$  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<sup>[13]</sup>  $\sigma(F)$  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).

For  $\lambda$  in the set of  $R$ -linear *functionals*  $\text{Hom}_R(M, R)$  on  $M$ , the image  $\lambda(M)$  is an ideal in  $R$ , as is the image  $\lambda(N)$ . Let  $\lambda$  be such that  $\lambda(N)$  is *maximal* among all ideals occurring as  $\lambda(N)$ .<sup>[14]</sup> 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  $\mu_i \in \text{Hom}_R(M, R)$  by

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

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  $\mu \in \text{Hom}_R(M, R)$ . 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  $\mu_i$  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

<sup>[12]</sup> Elementary divisors.

<sup>[13]</sup> 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.

<sup>[14]</sup> 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.

$m_1, \dots, m_t$  of  $M$  and  $x_1, \dots, x_t$  in  $R$  such that  $n_i = x_i m_i$  is a basis for  $N$ , using functional  $\lambda_i$  whose kernel is  $Rm_{i+1} + \dots + Rm_t$ , and  $\lambda_i(n_i) = x_i$ .

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

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

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

$$\begin{aligned} (r\lambda_i + s\lambda_{i+1})(n_i + n_{i+1}) &= r \cdot \lambda_i(n_i) + r \cdot \lambda_i(n_{i+1}) + s \cdot \lambda_{i+1}(n_i) + s \cdot \lambda_{i+1}(n_{i+1}) \\ &= r \cdot x_i + 0 + 0 + s \cdot x_{i+1} = \gcd(x_i, x_{i+1}) \end{aligned}$$

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. To prove *uniqueness*, first note that we have already shown that the cardinality of a basis of a free module is well-defined.

**EDIT: ... uniqueness perhaps better proven by introduction of a further idea...**

---

## 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 structure theorem for finitely-generated modules as a corollary, as follows.

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

$$q : M \rightarrow F$$

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.<sup>[16]</sup>

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  $m_1, \dots, m_t$  and there are uniquely determined<sup>[17]</sup>  $r_1 | r_2 | \dots | r_t \in R$  such that  $r_1 m_1, \dots, r_t m_t$  is a basis for  $N$ . Then

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

since

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

by

$$rm_i + Rr_im_i \rightarrow r + Rr_i$$

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

**Remark:** It is somewhat more clumsy to go in the opposite direction.

[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.