

.1 Classification of finitely generated modules over PID

Exercise .1.1. Let N, P be submodules of a module M , such that $N \cap P = \{0\}$ and $M = N + P$. Prove that $M \cong N \oplus P$. (This is a word-for-word repetition of Proposition IV.5.3 for modules.)

Solution. Consider the mapping

$$\varphi : N \oplus P \rightarrow N + P$$

defined by $\varphi(n, p) = n + p$. Certainly this is an R -module homomorphism. It is surjective since for all $m = n + p \in N + P$, we have $m = \varphi(n, p)$. Furthermore, the kernel of this mapping is

$$\ker \varphi = \{(n, p) \in N \oplus P \mid n + p = 0\}.$$

If $n + p = 0$ then $n = -p \in P$ so $n \in N \cap P$ and $n = 0$. Similarly, $p = 0$ so $\ker \varphi = \{0\}$ and the map is injective. Thus, this is an isomorphism and $M = N + P \cong N \oplus P$. \square

Exercise .1.2. Let R be an integral domain, and let M be a finitely generated R -module. Prove that M is torsion if and only if $\text{rk } M = 0$.

Solution. The rank of M is 0 if and only if for all $m \in M$, the set $\{m\}$ is linearly dependent. This occurs if and only if there exists $r \in R$ such that $rm = 0$, but this is true if and only if M is torsion. \square

Exercise .1.3. Complete the proof of Corollary 5.3.

Corollary 5.3. *Let R be a PID, let F be a finitely generated free module over R , and let $M \subseteq F$ be a submodule. Then there exists a basis (x_1, \dots, x_n) of F and nonzero elements a_1, \dots, a_m of R ($m \leq n$) such that (a_1x_1, \dots, a_mx_m) is a basis of M . Further, we may assume $a_1 \mid a_2 \mid \dots \mid a_m$.*

Solution. We only need to show the existence of the bases. By Lemma 5.2, there exists $x \in F$ such that

$$F = \langle x_1 \rangle \oplus F^{(1)}.$$

If $F^{(1)} = 0$, then (x_1) is a basis for F . Otherwise we may repeat this process. Since F is a finitely generated free module, this process terminates and yields a basis (x_1, \dots, x_n) for F . Lemma 5.2 also guarantees the existence of $y_1 = a_1x_1$ such that

$$M = \langle y_1 \rangle \oplus M^{(1)}.$$

If $M^{(1)} = 0$, then $(y_1) = (a_1x_1)$ is a basis for M . Otherwise we may repeat this process. Since M is a submodule of F , $\text{rk } M \leq \text{rk } F$ so this process also terminates at some $m \leq n$. \square

Exercise .1.4. Let R be an integral domain, and assume that $a, b \in R$ are such that $a \neq 0$, $b \notin (a)$, and $R/(a)$, $R/(a, b)$ are both integral domains.

- Prove that the Krull dimension of R is at least 2.
- Prove that if R satisfies the finiteness condition discussed in §5.2 for some n , then $n \geq 2$.

You can prove this second point by appealing to Proposition 5.4. For a more concrete argument, you should look for an R -module admitting a free resolution of length 2 which cannot be shortened.

- Prove that (a, b) is a regular sequence in R . (Exercise 4.13).
- Prove that the R -module $R/(a, b)$ has a free resolution of length exactly 2.

Can you see how to construct analogous situations with $n \geq 3$ elements a_1, \dots, a_n ?

Solution. Since $R/(a)$ and $R/(a, b)$ are integral domains, (a) and (a, b) are both prime ideals. Thus, we may construct the chain of prime ideals

$$(0) \subsetneq (a) \subsetneq (a, b)$$

in R , so the Krull dimension of R is at least 2.

Now suppose every finitely generated R -module M admits a free resolution of finite length n . To show that $n \geq 2$, it suffices to construct a free resolution of length 2 which cannot be shortened. Consider the R -module $M = R/(a, b)$. Then we have an exact sequence

$$0 \longrightarrow R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \xrightarrow{\pi} M \longrightarrow 0$$

where $d_2(r) = (-br, ar)$, $d_1(r, s) = ra + sb$, and π is the natural projection. It is easy to check that this is an exact sequence, and it cannot be shortened to $n = 1$. To see this, note that $\ker \pi = (a, b)$. Any morphism whose image is (a, b) must have domain R^2 since there are two degrees of choice in the image. Since the kernel of a map from $R^2 \rightarrow R$ must be nontrivial, there must be another copy of R before R^2 in the free resolution and the free resolution cannot be shortened. It also follows from the fact that the Krull dimension of a PID is at most 1.

Recall that a regular sequence is a tuple (a_1, a_2, \dots, a_n) where a_1 is not a zero-divisor of R , a_2 is not a zero-divisor of $R/(a_1)$, a_3 is not a zero-divisor of $R/(a_1, a_2)$ and so on. Since R is an integral domain, a is a non-zero-divisor of R . Furthermore, $b \notin (a)$ so $b \neq 0 \in R/(a)$. Then, since $R/(a)$ is an integral domain, b is not a zero divisor in $R/(a)$. Thus, (a, b) is a regular sequence in R .

The sequence constructed in part 2 of this exercise proves that $R/(a, b)$ has a free resolution of length 2. \square

Exercise .1.5. Recall (Exercise V.4.11) that a commutative ring is *local* if it has a single maximal ideal \mathfrak{m} . Let R be a local ring, and let M be a *direct summand* of a finitely generated free R -module: that is, there exists an R -module N such that $M \oplus N$ is a free R -module.

- Choose elements $m_1, \dots, m_r \in M$ whose cosets mod $\mathfrak{m}M$ are a basis of $M/\mathfrak{m}M$ as a vector space over the field R/\mathfrak{m} . By Nakayama's lemma, $M = \langle m_1, \dots, m_r \rangle$ (Exercise 3.10).
- Obtain a surjective homomorphism $\pi : F = R^{\oplus r} \rightarrow M$.
- Show that π splits, giving an isomorphism $F \cong M \oplus \ker \pi$. (Apply Exercise III.6.9 to the surjective homomorphism π and the free module $M \oplus N$ to obtain a splitting $M \rightarrow F$; then use Proposition III.7.5.)
- Show $\ker \pi / \mathfrak{m} \ker \pi = 0$. Use Nakayama's lemma (Exercise 3.8) to deduce that $\ker \pi = 0$.
- Conclude that $M \cong F$ is in fact free.

Summarizing, over a *local ring*, every *direct summand* of a finitely generated free R -module is free. Using the terminology we will introduce in Chapter VIII, we would say that ‘projective modules over local rings are free’. This result has strong implications in algebraic geometry, since it underlies the notion of vector bundle.

Contrast this fact with Proposition 5.1, which shows that, over a *PID*, every submodule of a finitely generated free module is free.

Solution. The first point follows from Exercise 3.10.

Define $\pi : R^{\oplus r} \rightarrow M$ which sends e_i to m_i where e_i is an elementary basis vector. Certainly this is surjective as a projection.

There is a short exact sequence

$$0 \longrightarrow \ker \pi \longrightarrow F \xrightarrow{\pi} M \longrightarrow 0$$

and since π has a right-inverse (sending the basis of M to the basis of F), Proposition III.7.5 implies that this sequence is split and $F \cong M \oplus \ker \pi$.

Note that

$$\left(\frac{R}{\mathfrak{m}} \right)^r \cong \frac{M}{\mathfrak{m}M} \oplus \frac{\ker \pi}{\mathfrak{m} \ker \pi}$$

as vector spaces over R/\mathfrak{m} . Since the dimension of $M/\mathfrak{m}M$ is r , we must have $\ker \pi / \mathfrak{m} \ker \pi = 0$. Then, by Nakayama's lemma, $\ker \pi = 0$.

Thus, $F \cong M$ and M is a free module. □

Exercise .1.6. Let R be an integral domain, and let $M = \langle m_1, \dots, m_r \rangle$ be a finitely generated module. Prove that $\text{rk } M \leq r$. (Use Exercise 3.12.)

Solution. Assume for the sake of contradiction that $k = \text{rk } M > r$. There are surjections $f : R^r \rightarrow M$ and $g : R^k \rightarrow M$. Let $N \in \mathcal{M}_{r,k}(R)$ such that g maps the columns of N to a maximal linearly independent subset of M . By Exercise 3.12, the columns of N are linearly dependent. In particular, there exist $\{r_1, \dots, r_k\}$ such that $r_1 n_1 + \dots + r_k n_k = 0$ where the $n_i \in R^r$. Then

$$g(r_1 n_1 + \dots + r_k n_k) = r_1 g(n_1) + \dots + r_k g(n_k) = 0,$$

which contradicts the assumption that the image of the columns of N is linearly independent. Thus, $k = \text{rk } M \leq r$. \square

Exercise .1.7. Let R be an integral domain, and let M be a finitely generated module over R . Prove that $\text{rk } M = \text{rk}(M/\text{Tor}(M))$.

Solution. First note that $\text{rk}(M/\text{Tor}(M)) \leq \text{rk } M$ because any linearly independent subset of the former induces a linearly independent subset of the latter. Suppose $\text{rk } M = r$ and let $S = \{m_1, \dots, m_r\}$ be a maximal linearly independent subset of M . Consider $S + \text{Tor}(M) = \{m_1 + \text{Tor}(M), \dots, m_r + \text{Tor}(M)\}$. If this set is linearly dependent, then there exist $r_1, \dots, r_r \in R$ such that $r_1 m_1 + \dots + r_r m_r \in \text{Tor}(M)$. That is, there exists an $s \in R, s \neq 0$ such that

$$s(r_1 m_1 + \dots + r_r m_r) = 0.$$

Since R is an integral domain, this implies $r_1 m_1 + \dots + r_r m_r = 0$ and S is linearly dependent in M , a contradiction. Thus, $S + \text{Tor}(M)$ is also linearly independent and we have $\text{rk } M = \text{rk}(M/\text{Tor}(M))$. \square

Exercise .1.8. Let R be an integral domain, and let M be a finitely generated module over R . Prove that $\text{rk } M = r$ if and only if M has a *free* submodule $N \cong R^r$, such that M/N is torsion.

If R is a PID, then N may be chosen so that $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ splits.

Solution. Suppose $\text{rk } M = r$ and let $S = \{m_1, \dots, m_r\}$ be a linearly independent subset. Consider the free submodule $N = \langle S \rangle \cong R^r$. Indeed, an isomorphism is given by mapping corresponding basis elements $m_i \mapsto e_i$. Now let $x + N \in M/N$. If $x + N$ is not a torsion element then there is no $r \in R$ such that $rx \in N$. That is, x is linearly independent of S , but this contradicts that S is a maximal linearly independent set. Thus, $x + N$ is a torsion element and M/N is torsion.

Now suppose M has a free submodule $N \cong R^r$ such that M/N is torsion. Choose a linearly independent set $S = \{m_1, \dots, m_r\}$ such that S is a basis for N . Let $x + N \in M/N$. Since this module is torsion, there exists an $r \in R$ such that $rx \in N$. That is, x is a linear combination of the elements of S . Since this holds for all elements of M , S is a maximal linearly independent subset of M and $\text{rk } M = r$. \square

Exercise .1.9. Let R be an integral domain, and let

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be an exact sequence of finitely generated R -modules. Prove that $\text{rk } M_2 = \text{rk } M_1 + \text{rk } M_3$.

Deduce that ‘rank’ defines a homomorphism from the Grothendieck group of the category of finitely generated R -modules to \mathbb{Z} .

Solution. Let $r_i = \text{rk } M_i$. By the isomorphism theorems, $M_3 \cong M_2/M_1$. Let $\{u_1, \dots, u_{r_1}\}$ be linearly independent in M_1 and $\{v_1 + M_1, \dots, v_{r_3} + M_1\}$ be linearly independent in M_3 . If

$$a_1 u_1 + \dots + a_{r_1} u_{r_1} + b_1 v_1 + \dots + b_{r_3} v_{r_3} = 0$$

in M_2 , then reducing the equation modulo M_1 yields

$$b_1(v_1 + M_1) + \dots + b_{r_3}(v_{r_3} + M_1) = 0 + M_1$$

so $b_1 = \dots = b_{r_3} = 0$ by linear independence in M_3 . But then $a_1 = \dots = a_{r_1} = 0$ by linear independence in M_1 so $r_2 \geq r_1 + r_3$.

To show the other inequality, let N be a linearly independent subset of M_2 . Let $X \subset N$ be maximal with respect to the property that $f(X)$ is linearly independent in M_3 (where f is the surjection from $M_2 \rightarrow M_3$). Now let $m \in N \setminus X$. The set $f(\{m\} \cup X)$ is linearly dependent in M_3 so there exist $r_m, s_{m,x} \in R$ such that

$$0 = r_m f(m) + \sum_{x \in X} s_{m,x} f(x) = f \left(r_m m + \sum_{x \in X} s_{m,x} x \right),$$

hence $r_m m + \sum_{x \in X} s_{m,x} x \in M_1$. Note that $r_m \neq 0$ since $f(X)$ is linearly independent. Now let $t_m \in R$ such that

$$\sum_{m \in N \setminus X} t_m (r_m m + \sum_{x \in X} s_{m,x} x) = 0$$

and rearrange to yield

$$0 = \sum_{m \in N \setminus X} t_m r_m m + \sum_{x \in X} \sum_{m \in N \setminus X} t_m s_{m,x} x.$$

The linear independence of N shows that $t_m r_m = 0$, so $t_m = 0$ since $r_m \neq 0$ and R is an integral domain. Thus, the elements $(r_m m + \sum_{x \in X} s_{m,x} x)_{m \in N \setminus X}$ are linearly independent. This shows that N can be split into a disjoint union $N = (N \setminus X) \cup X$ such that the elements of $N \setminus X$ are linearly independent in M_1 and the elements of X are linearly independent in M_3 . That is, $r_2 \leq r_1 + r_3$. Combining this with the above inequality yields $\text{rk } M_2 = \text{rk } M_1 + \text{rk } M_3$. \square

Exercise .1.10. Let R be an integral domain, M an R -module, and assume $M \cong R^r \oplus T$, with T a torsion module. Prove directly (that is, without using Theorem 5.6) that $r = \text{rk } M$ and $T \cong \text{Tor}_R(M)$.

Solution. We have an exact sequence

$$0 \longrightarrow R^r \longrightarrow M \longrightarrow T \longrightarrow 0$$

and by the above exercise, $\text{rk } M = \text{rk } R^r + \text{rk } T$. Since the rank of a torsion module is 0 (every element is linearly dependent), we have $\text{rk } M = r$. We also have an isomorphism $T \cong M/R^r$. Note that $\text{Tor}(M) = \{(s, t) \in M \mid \exists r \in R, (rs, rt) = (0, 0)\}$. Since R^r is a free module, if $rs = 0$ with $s \in R^r$, we must have $r = 0$. Thus, $\text{Tor}(M) = \{(0, t) \mid t \in T\}$, and clearly this is isomorphic to T . \square

Exercise .1.11. Let R be an integral domain, let M, N be R -modules, and let $\varphi : M \rightarrow N$ be a homomorphism. For $m \in M$, show that $\text{Ann}(\langle m \rangle) \subseteq \text{Ann}(\langle \varphi(m) \rangle)$.

Solution. Let $a \in \text{Ann}(\langle m \rangle)$ and consider $r\varphi(m) \in \langle \varphi(m) \rangle$. We have $a \cdot r\varphi(m) = r\varphi(am) = r\varphi(0) = 0$ so $a \in \text{Ann}(\langle \varphi(m) \rangle)$. \square

Exercise .1.12. Complete the proof of uniqueness in Theorem 5.6. (The hint in Exercise IV.6.1 may be helpful.)

Solution. Let R be a PID and suppose M_1, M_2 are isomorphic R -modules. In particular, we have $\text{Tor}(M_1) \cong \text{Tor}(M_2)$ and $\text{rk } M_1 = \text{rk } M_2$. It suffices to show that the decomposition of the torsion submodule is equivalent. We have

$$\text{Tor}(M_1) \cong \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_m)} \cong \frac{R}{(b_1)} \oplus \cdots \oplus \frac{R}{(b_n)} \cong \text{Tor}(M_2).$$

Since R is a PID and in particular a UFD, the decomposition of $\text{Tor}(M_1)$ is unique up to associates so $m = n$. Thus, we can rearrange the factors such that the p_i are associate to the q_i for $i = 1, \dots, n$. The uniqueness for form of elementary divisors follows easily. \square

Exercise .1.13. Let M be a finitely generated module over a Noetherian ring R .

Prove that if R is a PID, then M is torsion-free if and only if it is free. Prove that this property characterizes PIDs. (Cf. Exercise 4.3.)

Solution. If M is torsion-free, then the structure theorem yields $M \cong R^{\text{rk } M}$ so M is free. If M is free, then it has a basis E . Let $m = a_1 e_1 + \cdots + a_n e_n \in M$. Then for $r \neq 0$ in R

$$rm = (ra_1)e_1 + \cdots + (ra_n)e_n \neq 0$$

since $a_i \neq 0 \Rightarrow ra_i \neq 0$. Thus, M is torsion-free.

Now suppose that R is merely a Noetherian domain and every finitely generated module M is torsion-free if and only if it is free. Clearly every ideal $I \subseteq R$ is torsion-free and finitely generated, so I must be free. Assume I is generated by more than one element, say a_1, a_2 . Then $a_2a_1 - a_1a_2 = 0$ is a dependence relation in R so $a_1 = a_2 = 0$, contradicting the fact that they form a basis for I . Thus, I is generated by one element and R is a PID. \square

Exercise .1.14. Give an example of a finitely generated module over an integral domain which is *not* isomorphic to a direct sum of cyclic modules.

Solution. Consider the integral domain $R = \mathbb{Z}[x]$ and the module $M = (2, x)$. Suppose M is a direct sum of cyclic $\mathbb{Z}[x]$ modules. If (N_a) is a family of cyclic submodules of M such that $M = \sum_{a \in A} N_a$ and $N_b \cap \sum_{a \neq b} N_a = 0$ for all $b \in A$, then each N_a is a principal ideal in $\mathbb{Z}[x]$. But clearly if $x_a \in N_a$ and $x_b \in N_b$ then $x_ax_b \in N_a \cap N_b$ so $N_a \cap N_b \neq 0$ and $|A| = 1$, which implies that M is a principal ideal, a contradiction. \square

Exercise .1.15. Prove that the prime ideals appearing in the elementary divisor version of the classification theorem for a torsion module M over a PID are the prime ideals containing the characteristic ideal of M , as defined in Remark 5.8.

Solution. Recall that given a torsion module

$$M \cong \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_m)}$$

with $a_1 \mid \cdots \mid a_m$, we define

$$(a_1 \cdots a_m)$$

to be the characteristic ideal of M . To do. \square

Exercise .1.16. Prove that the prime ideals appearing in the elementary divisor version of the classification theorem for a module M over a PID are the associated primes of M , as defined in Exercise 4.5.

Solution. To do. \square

Exercise .1.17. Let R be a PID. Prove that the Grothendieck group of the category of finitely generated R -modules is isomorphic to \mathbb{Z} .

Solution. Let M be an R -module. By the structure theorem, we have $M \cong R^{\text{rk } M} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$. Next note that we may construct the exact sequence

$$0 \longrightarrow R \xrightarrow{a} R \longrightarrow \frac{R}{(a)} \longrightarrow 0$$

which implies that $[R/(a)] = [0]$ for all $a \in R$. Then we consider the homomorphism $\varphi : K(R\text{-Mod}^{fg}) \rightarrow \mathbb{Z}$ which sends a module M to $\text{rk } M$. It is easy to check that this morphism is well-defined, it is surjective, and the kernel is $[0]$, so it is injective. Thus, φ is an isomorphism. \square