
Perhaps the most elegant and concise classifications that exist in elementary algebra is that of finitely generated abelian groups (in stark contrast to that of finite simple groups!) We have seen that abelian groups are nothing other than $\mathbb{Z}$-modules and a natural question is whether or not we can obtain a nice classification of modules over a slightly broader class of rings than just $\mathbb{Z}$. It turns out that, for our purposes, the most fruitful setting to consider is R-modules when R is a PID.

We will eventually apply this theory to the setting where R is a polynomial ring acting on a vector space V over a field $\mathbb{F}$, where the action is defined in terms of a linear transformation T of V. The idea is that knowledge of the module theory of $\mathbb{F}[x]$ will provide information regarding the properties of T. With this in mind, and in keeping with our established convention, we switch orientation and consider right modules. Until further notice, R is a fixed PID and M_R is a module over R (recall that all modules are finitely generated).

We begin somewhat at the end by giving a general structure theorem for M_R which should remind you of finitely generated abelian groups. In fact, although we state it in its full generality, we will only prove it for abelian groups (i.e. for modules over our favourite PID, $\mathbb{Z}$). This cheat is justified by a desire to capture the flavour of the result without getting lost in technical details. I will, however, be delighted to discuss the general case with interested parties!

(PID1) Theorem ***[The Fundamental Theorem of Modules over a PID]*** *If R is a PID then M_R is the direct sum of cyclic submodules.*

Proof. We proceed by induction on the cardinality of a generating set for M of smallest size. Note that, if M is generated by a single element, then it is cyclic and the theorem is (trivially) true. Suppose then that the smallest generating set for M has cardinality $k > 1$ and that the result holds for all l-generated modules with $l < k$. Among all relations of the form

$$y_1 d_1 + y_2 d_2 + \ldots + y_k d_k = 0, \tag{1}$$

where $M = y_1\mathbb{Z} + \ldots + y_k\mathbb{Z}$, $d_i \in \mathbb{Z}$, and not all $y_i d_i = 0$, find the smallest positive integer c occuring as some d_i. Let $z_1, \ldots, z_k$ denote a generating set for which c occurs in such a relation. Thus, reordering the z_i if necessary, we have

$$z_1 c + z_2 e_2 + \ldots + z_k e_k = 0, \tag{2}$$

for some integers $e_2, \ldots, e_k$.

We first claim that, if $z_1 d_1 + \ldots z_k d_k = 0$, then $c | d_1$. Use the division theorem to write $d_1 = qc + r$ for $0 \leq r < c$. Multiplying (2) by q and subtracting, we get $z_1(d_1 - qc) + z_2(d_2 - qe_2) + \ldots + z_k(d_k - qe_k) = 0$. Since $r = d_1 - qc \geq 0$, by minimality of c, it follows that $r = 0$.

We next claim that $c|e_i$ for $2 \leq i \leq k$. It suffices to show that $c|e_2$. Write $e_2 = qc + r$ for $0 \leq r < c$ and put $z_1' = z_1 + z_2 q$. Then $z_1' c + z_2 r + z_3 e_3 + \ldots + z_k e_k = 0$; observe also that $z_1', z_2 \ldots, z_k$ generates M because the z_i do. Again, the minimality of c forces $r = 0$.

Hence, for $2 \leq i \leq k$, we can write $c_i = cq_i$ for some $q_i \in \mathbb{Z}$. Put $z_1^* = z_1 + z_2 q_2 + \ldots + z_k q_k$ and observe that $z_1^*, z_2, \ldots, z_k$ generates M. Now, by equation (2), we have

$$z_1^* c = z_1 c + z_2 c q_2 + \ldots + z_k c q_k = 0. \tag{3}$$

Suppose that $z = z_1^* d_1 = z_2 d_2 + \ldots + z_k d_k \in z_1^* \mathbb{Z} \cap \{z_2, \ldots, z_k\}\mathbb{Z}$, so that

$$(z_1 + z_2 q_2 + \ldots + z_k q_k) d_1 - z_2 d_2 - \ldots - z_k d_k = z_1 d_1 + z_2(q_2 - d_2) + \ldots + z_k(q_k - d_k) = 0.$$

Then, by the first claim, $c|d_1$ and hence, by equation (3), $z = z_1^* d_1 = 0$. We have shown that $M = z_1^*\mathbb{Z} + z_2\mathbb{Z} + \ldots + z_k\mathbb{Z} = z_1^*\mathbb{Z} \oplus \{z_2, \ldots, z_k\}\mathbb{Z}$. By the inductive hypothesis, the module $\{z_2, \ldots, z_k\}\mathbb{Z}$ decomposes as the direct sum of cyclic submodules, and the result now follows. □

Armed with this powerful weapon, we proceed now in full generality to nail down completely the structure of M_R. Recall that a finitely generated abelian group is made up of subgroups of two contrasting flavours: the infinite variety (direct products of $\mathbb{Z}$); and the finite variety (direct products of $\mathbb{Z}/n\mathbb{Z}$ for integers n). In the language of modules, the first type are simply free $\mathbb{Z}$-modules. We now define the analogue of the latter type in a general module. We say that $0 \neq x \in M_R$ is <u>torsion</u> if there exists $0 \neq r \in R$ such that $xr = 0$. Set

$$M_t := \{x \in M \mid x \text{ is torsion}\}.$$

We say that M is <u>torsion free</u> if it contains no torsion elements; we say that M is a <u>torsion module</u> if $M = M_t$.

(PID2) Theorem. *M_t is a submodule of M_R and there is a free submodule $M_f \leq M$ such that*

$$M = M_t \oplus M_f.$$

Proof. By **(PID1)**, there exist $x_1, \ldots, x_m \in M$ such that $M = x_1 R \oplus \ldots \oplus x_m R$. For each i, either x_i is torsion or it is not; assume that $x_1, \ldots, x_k$ are the generators which are not torsion and set $M_f := x_1 R \oplus \ldots \oplus x_k R$. It is clear that M_f is free (and, in particular, torsion free) and that $x_{k+1} R \oplus \ldots \oplus x_m R \leq M_t$. Finally, let $x \in M$ and write $x = x_f + x_t$ where $x_f \in M_f$ and $x_t \in x_{k+1} R \oplus \ldots x_m R$. But x is torsion if and only if $x_f = 0$ so that $M_t = x_{k+1} R \oplus \ldots \oplus x_m R$. □

We know that a free R-module is determined up to isomorphism by its rank. Therefore, in view of **(PID2)**, a complete analysis of a finitely generated generated module M_R over a PID R hinges only on a description of its torsion submodule M_t. For $x \in M$ set $\mathcal{A}_x := \{r \in R \mid xr = 0\}$ the <u>ANNIHILATOR</u> of x. Note that $\mathcal{A}_x$ is a (right) ideal of R or, equivalently, a submodule of the regular module R_R. We record a little fact connecting annihilators to cyclic modules (in light of **(PID1)** the precise structure of cyclic modules is now of key interest to us).

(PID3) Lemma. *$M_R = xR$ is cyclic iff $M_R \cong R/\mathcal{A}_x$.*

Proof. Let M_R and let $0 \neq x \in M$. Define $\lambda_x \colon R \to M$ sending $r \mapsto xr$, where R is the regular module R_R. Then M_R is cyclic with generator x iff λ_x is an epimorphism. But in this case, by **(Mod2)**, $\operatorname{im} \lambda_x \cong R/\ker \lambda_x = R/\mathcal{A}_x$. $\square$

Let $\mathcal{P}$ be a complete set of representative of the primes of R. For each M_R and $p \in \mathcal{P}$ set

$$M(p) := \{x \in M \mid \mathcal{A}_x = (p^n) \text{ for some } n \geq 0\}.$$

Then $M(p)$ is a submodule of M (see <u>Exercise 1</u>).

(PID4) Theorem. *If M_R is a torsion module, then*

$$M = \bigoplus_{p \in \mathcal{P}} M(p).$$

Proof. Let $0 \neq x \in M$. Since R is a PID, $\mathcal{A}_x = (a) \neq R$ for some $a = p_1^{e_1} \ldots p_n^{e_n}$ with $p_i \in \mathcal{P}$ and $e_i \in \mathbb{N}$ for $1 \leq i \leq n$. For each i, let $q_i \in R$ such that $q_i p_i^{e_i} = a$. Observe that $xq_i \in M(p_i)$ and that the gcd of $\{q_1, \ldots, q_n\}$ is 1. By the Euclidean Algorithm, there exist $r_i \in R$ with $q_1 r_1 + \ldots + q_n r_n = 1$. But then

$$x = x1 = xq_1 r_1 + \ldots xq_n r_n \in M(p_1) + \ldots + M(p_n),$$

so the submodules $M(p)$ certainly generate M. Next let $p_1, p_2 \in \mathcal{P}$ be distinct and let $y \in M(p_1) \cap M(p_2)$. Then for some $m_1, m_2 \in \mathbb{N}$, we have $\mathcal{A}_y = (p_1^{m_1}) = (p_2^{m_2})$. Hence $m_1 = m_2 = 0$ and $\mathcal{A}_y = R$ so that $y = 0$. The result now follows. $\square$

To complete the description of finitely generated modules over a PID, it suffices now to analyse the structure of the torsion modules $M(p)$ for $p \in R$ a prime.

(PID5) Lemma. *There exist natural numbers* $n_1 \geq n_2 \geq \ldots \geq n_k \geq 1$ *such that*

$$M(p) \cong R/(p^{n_1}) \oplus \ldots \oplus R/(p^{n_k}).$$

Proof. By **(PID1)**, there exist $x_1, \ldots x_k \in M(p)$ such that $M(p) = x_1 R \oplus \ldots \oplus x_k R$. For $1 \leq i \leq k$, by Lemma 2, $x_i R \cong R/\mathcal{A}_{x_i} = R/(p^{n_i})$ for some natural number n_i. The result now follows by reordering the x_i so that $n_1 \geq n_2 \geq \ldots \geq n_k \geq 1$. □

Combining **(PID2)**, **(PID4)** and **(PID5)**, we have now proved the first of two big decomposition theorems.

(PID6) [Elementary Divisor Theorem] *Let* M_R *be a finitely generated module over the PID* R. *Then there exist: unique primes* $p_1, \ldots, p_m \in \mathcal{P}$; *for each* p_i, *natural numbers* $n_{i1} \geq n_{i2} \geq \ldots \geq n_{ik_i} \geq 1$; *and an integer* $r \geq 0$, *such that*

$$M \cong M_f \oplus \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{k_i} R/(p_i^{n_{ij}}),$$

where M_f *is a free module of rank* r.

Not too surprisingly in view of the name of the preceding theorem, the prime powers $p_i^{n_{ij}}$ which, together with the integer r, characterise the module M_R are called the <u>ELEMENTARY DIVISORS</u> of M. The elementary divisors will be used later to obtain a canonical form for a linear operator. We now reassemble these submodules to obtain another valuable decomposition for M which will give rise to an alternate canonical form. Consider the following array:

$$\boxed{\begin{array}{lcccc} \boldsymbol{p_1}: & n_{11} & \geq & \ldots & \geq & n_{1k_1} \\ \boldsymbol{p_2}: & n_{21} & \geq & \ldots & \geq & n_{2k_2} \\ \vdots & & & & & \\ \boldsymbol{p_m}: & n_{m1} & \geq & \ldots & \geq & n_{mk_m} \end{array}}$$

For each $1 \leq i \leq k := \max\{k_1, \ldots, k_m\}$, put

$$q_i := p_1^{n_{1i}} p_2^{n_{2i}} \ldots p_m^{n_{mi}}.$$

Then we have

$$R/(q_i) \cong R/(p_1^{n_{1i}}) \oplus R/(p_2^{n_{2i}}) \oplus \ldots \oplus R/(p_m^{n_{mi}})$$

(see Exercise 2). Notice that, for $1 \le i < k$, $q_i | q_{i+1}$. The ideals $(q_1), \ldots, (q_k)$ (and also their generators $q_1, \ldots, q_k$) are called the INVARIANT FACTORS of M. Our final result, often called the The Fundamental Theorem of Finitely Generated Modules over a PID, gives an alternate decomposition of M in terms of its invariant factors.

(PID7) [Invariant Factor Theorem] *Let M_R be a finitely generated module over the PID R. Then there is a unique integer $r \geq 0$ and a unique chain of non-trivial ideals*

$$(q_1) \leq (q_2) \leq \ldots \leq (q_k)$$

of R such that

$$M \cong M_f \oplus R/(q_1) \oplus R/(q_2) \oplus \ldots \oplus R/(q_k),$$

where M_f is a free module of rank r.

Exercises.

1. Show that $M(p) = \{x \in M \mid \mathcal{A}_x = (p^n) \text{ for some } n \geq 0\}$ is a submodule of M.
2. Show that if $q = p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$ then
$$R/(q) \cong R/(p_1^{n_1}) \oplus R/(p_2^{n_2}) \oplus \ldots \oplus R/(p_m^{n_m})$$
3. For each of the following abelian groups M describe its torsion submodule M_t and, for each prime $p \in \mathbb{N}$, the submodule $M(p)$:
(a) $M = \mathbb{Q}/\mathbb{Z}$; (b) $M = \mathbb{Q}/2\mathbb{Z}$; (c) $M = \mathbb{R}/\mathbb{Z}$; (d) $M = \mathbb{R}/\mathbb{Q}$.
4. Find the elementary divisors and the invariant factors of the $\mathbb{Z}$-module $\mathbb{Z}_{120} \oplus \mathbb{Z}_{72} \oplus \mathbb{Z}_{98}$.