5. Finitely Generated Modules over a PID

We want to give a complete classification of finitely generated modules over a PID. Recall that a finitely generated module is a quotient of R^n, a free module. Let K be the kernel. Then M is isomorphic to R^n/K, by the Isomorphism Theorem.

Now K is a submodule of a Noetherian module; hence K is finitely generated. Pick a finite set of generators of K (it turns out that K is also isomorphic to a free module. Thus K is isomorphic to R^m, for some m, and in fact $m \leq n$).

As there is a map $R^m \longrightarrow K$, by composition we get an R-linear map

$$\phi\colon R^m \longrightarrow R^n.$$

Since K is determined by ϕ, M is determined by ϕ. The crucial piece of information is to determine ϕ.

As this map is R-linear, just as in the case of vector spaces, everything is determined by the action of ϕ on the standard generators $f_1, f_2, \dots, f_m$. Suppose that we expand $\phi(f_i)$ as a linear combination of the standard generators $e_1, e_2, \dots, e_n$ of R^n.

$$\phi(f_i) = \sum_j a_{ij} e_j.$$

In this case we get a matrix

$$A = (a_{ij}) \in M_{n,m}(R).$$

The point is to choose different bases of R^m and R^n so that the representation of ϕ by A is in a better form. Note the following:

Lemma 5.1. *Let $r_1, r_2, \dots, r_n$ be (respectively free) generators of M. Then so are $s_1, s_2, \dots, s_n$, where we apply one of:*

(1) we multiply one of the r_i by a unit,
(2) we switch the position of r_i and r_j,
(3) we replace r_i by $r_i + ar_j$, where a is any scalar.

Proof. Easy. □

At the level of matrices, (5.1) informs us that we are free to perform anyone of the elementary operations on matrices, namely multiplying a row (respectively column) by a unit, switching two rows (respectively columns) and taking a row and adding an arbitrary multiple of another row (respectively column).

Proposition 5.2. *Let A be a matrix with entries in a PID R.*

Then we can find two invertible square matrices B and C in R such that the matrix BAC has the following form:

The only non-zero entries are on the diagonal and each non-zero entry divides the next one in the list.

If R is a Euclidean domain then we can put A into the given form after a sequence of elementary row and column operations.

Proof. This is much easier than it looks. Suppose that the gcd of the entries of A is d. As R is a PID, d is a linear combination of the entries of A.

Suppose that one of the entries of A is d. By permuting the rows and columns, we may assume that d is at the top left hand corner. As d is the gcd, it divides every entry of A. By row and column reduction we reduce to the case that the only non-zero entry in the first column and row is the entry d at the top left hand corner. Let B be the matrix obtained by striking out the first row and column. Then every element of B is divisible by d and we are done by induction on m and n.

So we have to show that we can manipulate A until one of the entries is d. As R is a PID, d is linear combination of the entries of A. By induction on the number of entries, we may assume that

$$A = \begin{pmatrix} a \\ b \end{pmatrix}.$$

If R is a Euclidean domain then we can put A into the given form after a sequence of row operations; just apply Euclid's algorithm.

In the general case, note that we may find x and y such that

$$d = xa + yb.$$

Note that the gcd of x and y must be 1. Therefore we may find u and v such that

$$1 = ux + vy.$$

Let

$$B = \begin{pmatrix} x & y \\ -v & u \end{pmatrix}.$$

Note that the determinant of B is

$$xu + yv = 1.$$

Thus B is invertible, with inverse

$$\begin{pmatrix} u & -y \\ v & x \end{pmatrix}.$$

On the other hand,

$$BA = \begin{pmatrix} d \\ -va + ub \end{pmatrix}. \qquad \square$$

Corollary 5.3. *Let M be a module over a PID R.*

Then M is isomorphic to $F \oplus T$, where $F \simeq R^r$ is a free module and T is isomorphic to either,

(1)

$$R/\langle d_1 \rangle \oplus R/\langle d_2 \rangle \oplus \cdots \oplus R/\langle d_n \rangle.$$

where d_i divides d_{i+1}, or

(2)

$$R/\langle p_1^{m_1} \rangle \oplus R/\langle p_2^{m_2} \rangle \oplus \cdots \oplus R/\langle p_n^{m_n} \rangle.$$

where p_i is a prime.

The integer r and $d_1, d_2, \dots, d_n$ are invariant, up to associates. r is called the ***rank***.

Proof. By the Chinese Remainder Theorem it suffices to prove the first classification result. By assumption M is isomorphic to a quotient of R^n by an image of R^m. By (5.2) we may assume the corresponding matrix has the given simple form. Now note that the last r rows that contain only zero entries, corresponds to the free part, and there is an obvious corrrespondence between the non-zero rows and the direct summands of the torsion part.

Now suppose that

$$F \oplus T \simeq F' \oplus T',$$

where F and F' are free and T and T' are not. Suppose that we tensor this with the field of fractions K of R. Note that we have

$$R/\langle a \rangle \underset{R}{\otimes} K = \begin{cases} K & \text{if } a = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Indeed if $a = 0$ then we have $R \underset{R}{\otimes} K = K$. On the other hand, note that the annihilator of $R/\langle a \rangle$ is $\langle a \rangle$. By extension of scalars, $R/\langle a \rangle \underset{R}{\otimes} K$ is a vector space over K. The only vector space with non-trivial annihilator is the zero vector space.

Since tensor product commutes with direct sum, we get that

$$K^r \simeq K^{r'}.$$

Thus the rank $r = r'$ is nothing more than the dimension of the K-vector space $M \underset{R}{\otimes} K$.

Note that the annihilator of T is the intersection of the ideals

$$\bigcap_{i=1}^{n} \langle d_i \rangle = \langle d_n \rangle.$$

By assumption we may find R-linear maps

$$f\colon F\oplus T \longrightarrow F'\oplus T' \qquad \text{and} \qquad g\colon F'\oplus T' \longrightarrow F\oplus T,$$

which are inverse to each other. Consider the composition of the natural inclusion $T \longrightarrow F\oplus T$, f and the projection onto F'. Since the annihilator of T is non-trivial, the image has non-trivial annihilator. But then the image is zero. It follows that f and g induce isomorphisms $T \simeq T'$.

Since the annihilator of T is $\langle d_n\rangle$ it follows that

$$\langle d_n\rangle = \langle d'_{n'}\rangle.$$

Thus d_n and $d'_{n'}$ are associates.

We may write $T = T_0 \oplus T_1$ and $T' = T'_0 \oplus T'_1$, where T_1 is the direct sum of all cyclic factors with annihilator $\langle d_n\rangle$, and T_0 is the direct sum of the other cyclic factors. Note that the annihilator of T_0 is bigger than the annihilator $\langle d_n\rangle$ of T_1 and that the annihilators of T_1 and T'_1 are equal. Note that

$$T_1 \simeq \left(\frac{R}{\langle d_n\rangle}\right)^a,$$

for some integer a.

Let $0 \leq m \leq n$ be the largest integer such that d_m and d_n are not associates. Pick a prime factor p of d_n/d_m. Let $d = d_n/p$ and let

$$M_0 \subset M$$

be the submodule of all elements of M with annihilator $\langle d\rangle$. Note that

$$M = T_0 + pT_1 = T'_0 + pT'_1.$$

Since

$$\frac{R}{\langle d_n\rangle}\Big/\frac{\langle p\rangle}{\langle d_n\rangle} \simeq \frac{R}{\langle p\rangle}$$

we have

$$\frac{M}{M_0} \simeq \left(\frac{R}{\langle p\rangle}\right)^a.$$

As the LHS is naturally a vector space over the field $K = \frac{R}{\langle p\rangle}$, we have

$$a = \dim_K \frac{M}{M_0}.$$

Thus $a = a'$.

On the other hand, by Noetherian induction, $T_0 + pT_1$ and $T'_0 + pT'_1$ have the same cyclic factors. Thus T_0 and T_1 have the same cyclic factors. □

One special case deserves attention:

Corollary 5.4. *Let G be a finitely generated abelian group. Then G is isomorphic to $\mathbb{Z}^r \times T$, where T is isomorphic to*

(1)
$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_n},$$
where $d_1, d_2, \dots, d_n$ are positive integers and d_i divides d_{i+1}, or

(2)
$$\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_n^{m_n}}.$$
where $p_1, p_2, \dots, p_n$ are primes.

Really the best way to illustrate the proof of these results, which are not hard, is to illustrate the methods by an example. Suppose we are given

$$\begin{pmatrix} -58 & 4 & 65 & 1 \\ 4 & 2 & 1 & -1 \\ -32 & 2 & 34 & 2 \\ -26 & 2 & 31 & -1 \\ -1 & 1 & 2 & 1 \end{pmatrix}.$$

This represents a $\mathbb{Z}$-linear map
$$\mathbb{Z}^4 \longrightarrow \mathbb{Z}^5,$$
in the standard way. The gcd is 1. Thus we first switch the first and fourth columns.

$$\begin{pmatrix} 1 & 4 & 65 & -58 \\ -1 & 2 & 1 & 4 \\ 2 & 2 & 34 & -32 \\ -1 & 2 & 31 & -26 \\ 1 & 1 & 2 & -1 \end{pmatrix}.$$

We could stop swapping here, but in fact it is better to switch the first and last row

$$\begin{pmatrix} 1 & 1 & 2 & -1 \\ -1 & 2 & 1 & 4 \\ 2 & 2 & 34 & -32 \\ -1 & 2 & 31 & -26 \\ 1 & 4 & 65 & -58 \end{pmatrix}.$$

As we now have a 1 in the first row, we can now eliminate 1, 2 and -1 from the first row, a la Gaussian elimination, to get

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 3 & 3 & 3 \\ 2 & 0 & 30 & -30 \\ -1 & 3 & 33 & -27 \\ 1 & 3 & 63 & -57 \end{pmatrix}.$$

Now eliminate the entries in the first column.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 3 & 3 \\ 0 & 0 & 30 & -30 \\ 0 & 3 & 33 & -27 \\ 0 & 3 & 63 & -57 \end{pmatrix}.$$

Now eliminate as before,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 30 & -30 \\ 0 & 3 & 30 & -30 \\ 0 & 3 & 60 & -60 \end{pmatrix},$$

so that we get

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 30 & -30 \\ 0 & 0 & 30 & -30 \\ 0 & 0 & 60 & -60 \end{pmatrix}.$$

Now eliminate again

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 30 & 0 \\ 0 & 0 & 30 & 0 \\ 0 & 0 & 60 & 0 \end{pmatrix},$$

so that we get

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 30 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

It follows then that we have

$(\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z})/(\mathbb{Z}\oplus 3\mathbb{Z}\oplus 30\mathbb{Z}) \simeq \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}_3\oplus\mathbb{Z}_{30} \simeq \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}_3\times\mathbb{Z}_{30}$.

The free part is $\mathbb{Z} \times \mathbb{Z}$ and the torsion part is $\mathbb{Z}_3 \times \mathbb{Z}_{30} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. In this case the rank is 2.