15. 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 15.1. *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*

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, (15.1) informs us that we are free to perform any one 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 15.2. *Let A be a matrix with entries in a PID R.*

Then, after a sequence of elementary row operations and column operations, we may put A into the following form. The only non-zero *entries are on the diagonal and each non-zero entry divides the next one in the list.*

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. Thus by repeated row and column operations, and multiplication by units, we may assume that d is equal to one of the entries of A. Now 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. $\square$

Corollary 15.3. *Let M be a module over a PID R.*

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

(1)
$$R/\langle d_1\rangle \oplus R/\langle d_2\rangle \oplus \dots R/\langle d_n\rangle.$$
where d_i divides d_{i+1}, or

(2)
$$R/\langle p_1^{m_1}\rangle \oplus R/\langle p_2^{m_2}\rangle \oplus \dots R/\langle p_n^{m_n}\rangle.$$
where p_i is a prime.

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 (15.2) we may assume the corresponding matrix has the given simple form. Now note that the rows that contain only zeroes, correspond to the free part, and there is an obvious corrrespondence between the non-zero rows and the direct summands of the torsion part. $\square$

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
$$\begin{pmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{pmatrix}$$
The gcd is 1. Thus we first switch the third and first rows.
$$\begin{pmatrix} 1 & 2 & 2 & 1 \\ 2 & 4 & 6 & 6 \\ 3 & 8 & 7 & 9 \end{pmatrix}.$$

As we now have a 1 in the first row, we can now eliminate 2 and 3 from the first column, a la Gaussian elimination, to get

$$\begin{pmatrix} 1 & 2 & 2 & 1 \\ 0 & 0 & 2 & 4 \\ 0 & 2 & 1 & 6 \end{pmatrix}.$$

Now eliminate the entries in the first row.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 4 \\ 0 & 2 & 1 & 6 \end{pmatrix}$$

Now we switch the second and third columns,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 4 \\ 0 & 1 & 2 & 6 \end{pmatrix}$$

and then the second and third rows,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 6 \\ 0 & 2 & 0 & 4 \end{pmatrix}$$

Now eliminate as before,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -4 & -8 \end{pmatrix}$$

Now multiply the third row by -1 and eliminate the 8, to get

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 4 & 0 \end{pmatrix}$$

It follows then that we have $(\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z})/(\mathbb{Z} \oplus \mathbb{Z} \oplus 4\mathbb{Z}) \simeq \mathbb{Z}_4$.

Theorem 15.4. *(Jordan Normal Form) Let $\phi \colon V \longrightarrow V$ be a linear map between finite dimensional vector spaces, over a field F, which is algebraically closed (every polynomial has a root).*

Then there is a basis $e_1, e_2, \dots, e_n$ of V such that the associated matrix has the following decomposition into blocks, $B_1, B_2, \dots, B_k$. Each block has a single number along the main diagonal, and a string of 1's above the main diagonal.

Proof. The idea is to make V into an $F[x]$-module and apply the classification Theorem.

Now the point is that it makes sense to talk about polynomials in ϕ. Thus to define a scalar multiplication

$$F[x] \times V \longrightarrow V$$

just send $(f(x), v)$ to $f(\phi)v$, the result of applying the linear transformation $f(\phi)$ applied to v. In this way V becomes an $F[x]$-module. As F is field, $F[x]$ is a PID. By the classification Theorem, V is isomorphic to

$$k[x]/\langle p_1^{m_1}(x)\rangle \oplus k[x]/\langle p_2^{m_2}(x)\rangle \oplus \dots k[x]/\langle p_k^{m_k}(x)\rangle.$$

where each $p_i(x)$ is a prime (equivalently irreducible) polynomial. The possibility that $f(x) = 0$ is excluded as V is finite dimensional. Now each direct summand corresponds to a block of our matrix. So we might as well assume that there is only one summand (and then only one block).

Since K is algebraically closed, the only irreducible polynomials are in fact linear polynomials. Thus

$$p(x) = (x - \lambda)$$

for some $\lambda \in F$. It follows then that $(\phi - \lambda I)^m = 0$. On the other hand, the given matrix has exactly this $F[x]$-module structure and the $F[x]$-module structure determines ϕ. It follows easily that ϕ has the given form on the given block. $\square$