14. 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 $f_1, f_2, \ldots, f_m$. Suppose that we expand $\phi(f_i)$ as a linear combination of the standard generators $e_1, e_2, \ldots, e_n$ 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 14.1. *Let $r_1, r_2, \ldots, r_n$ be (respectively free) generators of M. Then so are $s_1, s_2, \ldots, s_n$, where*

(1) we multiply one of the r_i by an invertible element,
(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, (14.1) informs us that we are free to perform any one of the elementary operations on matrices, namely multiplying a row (respectively column) by an invertible element, switching two rows (respectively columns) and taking a row and adding an arbitrary multiple of another row (respectively column).

Definition-Proposition 14.2. *Let A be a matrix with entries in a Euclidean domain R.*

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

Proof. The key point is to reduce to the case where one of the entries of A is the gcd of the entries of A.

To this end, we first reduce to the case that given any two entries in the same row or column, one entry divides the other. By elementary row and column operations we can always make any two entries adjacent and so we reduce to the case that A is a 2×1 matrix,

$$\begin{pmatrix} a \\ b \end{pmatrix}$$

(the case of a 1×2 is the similar, or just take transposes).

Since we are working over a Euclidean domain (and not just a PID) we can calculate the gcd by using Euclid's algorithm. At each stage we may find q and r such that

$$b = qa + r \qquad \text{or} \qquad a = qb + r.$$

By symmetry we may assume we have the former case. Now either $r = 0$ in which case either a is the gcd, and we are done, or by Euclid's algorithm it suffices to find the gcd of a and r. But if we take the first row of a and multiply by q and subtract this from the second row then we get the matrix

$$\begin{pmatrix} a \\ r \end{pmatrix}.$$

Therefore, after finitely many elementary row and column operations we may assume that given any pair of entries of A one entry divides the other. (14.3) implies that one element d of A is the gcd.

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. □

Lemma 14.3. *Let $A = (a_{ij}) \in M_{n,m}(R)$ be an array of elements of a UFD R, with the property that if two entries belong to the same row or the same column then one divides the other.*

Then one entry is the gcd.

Proof. If A has more than one row then we can do induction on the number of rows. We may asume that the matrix B one gets by deleting the first row has one entry b equal to the gcd. If b divides every element in the first row then it is the gcd of A.

Otherwise there is an element a of the first row that divides every element of B. Thus we may assume that A has one row. If A has more than one column then let C be the matrix one gets by deleting the first column. By induction one entry c of C divides every other element. We compare this with the first element a. If the c divides a then c is the gcd. Otherwise a is the gcd. □

Remark 14.4. *One can actually reduce any matrix over a PID into Smith normal form. In this case one needs to pre- and post-multiply by invertible matrices with entries in R.*

As before we are reduced to the case

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

In the general case, as R is a PID, 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,

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

Note that the entries on the main diagonal are determined.

Definition-Lemma 14.5. *Let A be a matrix with entries in a PID.*

*The ith **determinant divisor**, denoted $d_i(A)$, is the greatest common divisor of all $i \times i$ minors of A.*

The entries on the main diagonal of the Smith normal form are the ratios

$$\frac{d_i(A)}{d_{i-1}(A)}$$

($d_0(A) = 1$ by convention).

Proof. The determinant of an invertible matrix is invertible and so pre- and post-multiplication by invertible matrices do not change the ith determinant divisor.

On the other hand the ith determinant divisor of a matrix in Smith normal form is simply the product of the first i entries on the main diagonal. □

Corollary 14.6. *Let M be a finitely generated 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)

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

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.

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 (14.2) we may assume the corresponding matrix is in Smith normal form. Now note that the rows that contain only zeroes, correspond to the free part, and there is an obvious correspondence between the non-zero rows and the direct summands of the torsion part. □

One special case deserves attention:

Corollary 14.7. *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 $d_1, d_2, \ldots, d_n$ 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 $p_1, p_2, \ldots, p_n$ 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

$$\begin{pmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{pmatrix}.$$

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

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

Now we have a matrix in Smith normal form.

This corrresponds to a $\mathbb{Z}$-linear map

$$\phi\colon \mathbb{Z}^4 \longrightarrow \mathbb{Z}^3.$$

It follows then that we have $(\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z})/(\mathbb{Z} \oplus \mathbb{Z} \oplus 4\mathbb{Z}) \simeq \mathbb{Z}_4$. The free part is zero and the torsion part is $\mathbb{Z}_4$.

Suppose instead we have the matrix:

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

This matrix is already in Smith normal form. This represents a $\mathbb{Z}$-linear map

$$\mathbb{Z}^4 \longrightarrow \mathbb{Z}^5,$$

in the standard way. It follows then that we have

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

The free part is $\mathbb{Z} \times \mathbb{Z}$ and the torsion part is

$$\mathbb{Z}_3 \times \mathbb{Z}_{30} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$