

Classification of finitely generated modules over PIDs

Abstract

Support notes for the MMAC course “Modules and Representations” of IST in the academic year 2024/2025. As always, all the rings are unital.

Contents

I	Background on rings	2
1	Euclidean domains	2
2	Principal ideal domains	2
II	Modules over PIDs	3
3	General facts	3
4	Smith normal forms	4
5	Classification of finitely generated modules	4
III	Applications	6
6	Abelian groups	6
7	Jordan canonical forms	6
8	Rational canonical forms	7

Part I

Background on rings

1 Euclidean domains

§1. DEFINITION. By an *euclidean domain (ED)* is meant an integral domain R for which there is a function (called an “euclidean norm”)

$$N : R \rightarrow \mathbb{Z}_{\geq 0}$$

such that $N(0) = 0$ and, for all $a, b \in R$ with $b \neq 0$, there are $q, r \in R$ such that

$$a = qb + r$$

and either $N(r) < N(b)$ or $r = 0$. (In other words, R has a *division algorithm*.)

§2. EXAMPLE. \mathbb{Z} is an ED with euclidean norm $N(a) = |a|$ (modulus of a).

§3. EXAMPLE. $F[x]$ is an ED for any field F , with euclidean norm $N(p) = \deg(p)$.

§4. EXAMPLE. $\mathbb{Z}[i] \subset \mathbb{C}$ (the *Gaussian integers*) is an ED with euclidean norm $N(a + ib) = a^2 + b^2$ for all $a, b \in \mathbb{Z}$.

2 Principal ideal domains

§5. DEFINITION. By a *principal ideal domain (PID)* is meant an integral domain R whose ideals are principal (i.e., they are cyclic submodules of R).

§6. PROPOSITION. *Any ED is a PID.*

Proof. Let R be an ED, and let F be an ideal of R . If $F = \{0\}$ then it is generated by 0, hence principal. Otherwise, let $F \neq \{0\}$, let

$$m = \min\{N(a) \mid a \in F \setminus \{0\}\},$$

and let $b \in J \setminus \{0\}$ be such that $N(b) = m$. Now let $a \in J$ be an arbitrary element of J , and let us divide a by b : choose $q, r \in R$ such that

$$a = qb + r$$

with either $N(r) < N(b)$ or $r = 0$. If $r \neq 0$ we must have $N(r) < N(b)$, and thus $r \in J \setminus \{0\}$ with $N(r) < m$, a contradiction. Hence, we must have $r = 0$, and thus $a \in (b)$. So we see that J is the principal ideal (b) . ■

§7. EXAMPLE. Not every PID is an ED. An example of a PID which is not an ED is the ring of quadratic integers

$$\mathbb{Z} \left[\frac{1 + \sqrt{-19}}{2} \right] = \left\{ a + b \frac{1 + \sqrt{-19}}{2} \mid a, b \in \mathbb{Z} \right\}.$$

Part II

Modules over PIDs

3 General facts

Let R be any commutative ring.

§8. LEMMA. *For any finitely generated R -module M there is a surjective homomorphism of R -modules $q : R^n \rightarrow M$ for some $n \in \mathbb{Z}_{\geq 1}$.*

Proof. Exercise. ■

§9. EXERCISE. *Let M_1, \dots, M_k ($k \geq 1$) be R -modules, and for each $i = 1, \dots, k$ let N_i be a submodule of M_i . Prove that $N_1 \times \dots \times N_k$ is a submodule of $M_1 \times \dots \times M_k$, and that*

$$(M_1 \times \dots \times M_k) / (N_1 \times \dots \times N_k) \cong (M_1/N_1) \times \dots \times (M_k/N_k).$$

§10. COROLLARY. *Let J_1, \dots, J_k be ideals of R ($k \geq 1$). Then*

$$R^k / (J_1 \times \dots \times J_k) \cong (R/J_1) \times \dots \times (R/J_k).$$

§11. LEMMA. Let M be a module, $K \subset M$ a submodule, and

$$q : M \rightarrow M/K$$

the quotient homomorphism.

1. If $A \subset K$ generates K and a set $B \subset M$ is such that $q(B)$ generates M/K , then $A \cup B$ generates M .
2. Moreover, if A is a basis of K and $q(B)$ is a basis of M/K and $q|_B$ is injective, then $A \cap B = \emptyset$ and $A \cup B$ is a basis of M .

Proof. Exercise. ■

4 Smith normal forms

See section 3.7 of Jacobson's *Basic Algebra*.

5 Classification of finitely generated modules

From now on R is always a PID.

§12. LEMMA. Let $N \subset R^n$ be a submodule. Then N is free with rank at most n .

Proof. The proof is by induction on n . For $n = 1$ the module is R , and its submodules are the ideals, which for a PID are cyclic submodules. Such a submodule is either the zero module, with rank 0, or a nonzero submodule (a) , hence free with rank 1 because the mapping $1 \mapsto a$ defines an isomorphism of modules $R \rightarrow (a)$. This is the induction base.

Now assume $n > 1$, and let $N \subset R^n$ be a submodule. Consider the following exact sequence:

$$0 \longrightarrow R^{n-1} \xrightarrow[\mathbf{x} \mapsto (\mathbf{x}, 0)]{\iota} R^n \xrightarrow{\pi_n} R \longrightarrow 0.$$

Now consider the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R^{n-1} & \xrightarrow{\iota} & R^n & \xrightarrow{\pi_n} & R \longrightarrow 0 \\ \parallel & & \uparrow \alpha & & \uparrow \beta & & \uparrow \gamma \\ 0 & \longrightarrow & N \cap R^{n-1} & \xrightarrow{j} & N & \xrightarrow{q} & \pi_n(N) \longrightarrow 0 \\ & & & & & & \parallel \end{array}$$

By induction hypothesis, both $N \cap R^{n-1}$ and $\pi_n(N \cap R^n)$ are free, with ranks at most $n-1$ and 1 , respectively. The homomorphisms j and q are the restrictions of ι and π_n , respectively, and therefore j is of course injective, and q is surjective by construction. Moreover, $\pi_n \circ \iota = 0$ implies that $q \circ j = 0$, which means that $j(N \cap R^{n-1}) \subset \ker q$. Conversely, if $\mathbf{y} \in \ker q$ then, by construction, $\mathbf{y} \in N$ and $\mathbf{y} \in \iota(N \cap R^{n-1})$, so $\ker q = j(N \cap R^{n-1})$. Hence, the lower sequence is exact (and α , β and γ define a homomorphism of short exact sequences), and there are two possibilities. If $q \neq 0$, the rank of $\pi_n(N \cap R^n)$ equals 1 , and thus, by §11, N is free with rank equal to $\text{rank}(N \cap R^{n-1}) + 1 \leq n$. If $q = 0$ we have $N = N \cap R^{n-1}$, so $N \subset R^{n-1}$, and thus N is free with rank at most $n-1$, hence also at most n . ■

§13. THEOREM. (Classification of the finitely generated modules over PIDs.) *Let R be a PID and let M be a finitely generated R -module. Then there exist $m, k \in \mathbb{Z}_{\geq 0}$ and $a_1, \dots, a_k \in R$ such that*

$$M \cong R^m \oplus R/(a_1) \oplus \cdots \oplus R/(a_k).$$

Proof. Since M is f.g., there exist $n \in \mathbb{Z}_{\geq 1}$ and a surjective homomorphism $q : R^n \rightarrow M$. By the previous lemmas, the kernel of q is a free submodule of R^n with rank $m \leq n$. Hence, $\ker q \cong R^m$, so there is a short exact sequence

$$0 \longrightarrow R^m \xrightarrow{\iota} R^n \xrightarrow{q} M \longrightarrow 0.$$

Moreover, by an appropriate choice of bases, ι can be represented by a Smith normal form

$$\begin{pmatrix} a_1 & 0 & \cdots & \cdots & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & \vdots & & & \vdots \\ \vdots & & \ddots & & \vdots & & & \vdots \\ \vdots & & & \ddots & 0 & & & \vdots \\ 0 & \cdots & \cdots & 0 & a_k & 0 & \cdots & 0 \\ \vdots & & & & 0 & 0 & & \vdots \\ \vdots & & & & \vdots & & \ddots & \vdots \end{pmatrix},$$

so $\iota(r_1, \dots, r_n) = (a_1 r_1, \dots, a_k r_k, 0, \dots, 0)$, and thus

$$\iota(R^m) = (a_1) \times \cdots \times (a_k) \times \{0\} \times \cdots \times \{0\}.$$

Hence, by §10,

$$M \cong R/(a_1) \times \cdots \times R/(a_k) \times R^{n-k},$$

which yields the envisaged result with $m = n - k$:

$$M \cong R^m \oplus R/(a_1) \oplus \cdots \oplus R/(a_k). \quad \blacksquare$$

§14. COROLLARY. (Invariant factor decomposition.) *Let R be a PID and let M be a finitely generated R -module. Then there exist unique $m, k \in \mathbb{Z}_{\geq 0}$ and a unique list $a_1, \dots, a_k \in R \setminus (R^\times \cup \{0\})$ (up to multiplication by invertibles) such that $a_i \mid a_{i+1}$ for all $i = 1, \dots, k - 1$ and*

$$M \cong R^m \oplus R/(a_1) \oplus \cdots \oplus R/(a_k).$$

Note: The elements a_1, \dots, a_k are the *invariant factors* of M .

§15. ELEMENTARY DIVISORS. Each invariant factor a is a product $p_1^{n_1} \cdots p_\ell^{n_\ell}$ where $n_i \in \mathbb{Z}_{>0}$ and the p_i are distinct primes (equivalently, irreducibles). By the Chinese Remainder Theorem we obtain

$$R/(a) \cong R/(p_1^{n_1}) \times \cdots \times R/(p_\ell^{n_\ell}).$$

Replacing in this way each factor $R/(a_i)$ in the invariant factor classification, we obtain the *elementary divisor classification* of finitely generated modules over PIDs.

Part III

Applications

6 Abelian groups

§16. EXERCISE. Write the statements of the classification of finitely generated abelian groups both in terms of invariant factors and of elementary divisors.

§17. EXERCISE. How many isomorphism classes are there of abelian groups of order 600? Write the list of invariant factors for each of the isomorphism classes.

7 Jordan canonical forms

Let F be an algebraically closed field, V a finite dimensional vector space over F , and $T : V \rightarrow V$ a linear transformation. Equivalently, let V be an $F[x]$ -module which is finite dimensional as a vector space over F . Recall that the equivalence is given by taking T to be defined by $T(v) = xv$ for each $v \in V$.

Since $F[x]$ is a PID, and F is algebraically closed, and V is finite dimensional (notice that $F[x]$ is not finite dimensional as a vector space over F), the elementary divisor classification gives us

$$V \cong F[x]/((x - \lambda_1)^{n_1}) \times \cdots \times F[x]/((x - \lambda_m)^{n_m}).$$

The linear transformation T , which corresponds to the action of x , is componentwise, so its matrix representation is blockwise diagonal. In order to see what each block looks like, consider a module of the form $M = F[x]/((x - \lambda)^n)$. A basis of M as a vector space over F is given by the following polynomials (why?):

$$1, (x - \lambda), (x - \lambda)^2, \dots, (x - \lambda)^{n-1}$$

Then in M we have:

$$x(x - \lambda)^{n-1} = ((x - \lambda) + \lambda)(x - \lambda)^{n-1} = (x - \lambda)^n + \lambda(x - \lambda)^{n-1} = \lambda(x - \lambda)^{n-1},$$

so $(x - \lambda)^{n-1}$ is an eigenvector of T with associated eigenvalue λ . And, for all $i < n - 1$, we have that $(x - \lambda)^i$ is a generalized eigenvector:

$$x(x - \lambda)^i = ((x - \lambda) + \lambda)(x - \lambda)^i = (x - \lambda)^{i+1} + \lambda(x - \lambda)^i.$$

Hence, using this ordered basis, the matrix representation of the restriction of T to M is a Jordan block:

$$\begin{pmatrix} \lambda & 1 & & \cdots & 0 \\ 0 & \lambda & 1 & & 0 \\ \vdots & & \ddots & \cdots & 1 \\ 0 & & \cdots & & \lambda \end{pmatrix}$$

So $T : V \rightarrow V$ has a matrix representation by a Jordan canonical form.

8 Rational canonical forms

The rational canonical form is obtained from the classification theorem of f.g. modules over PIDs, using the invariant factor classification instead of elementary divisors. See Dummit&Foote, chapter 12.