6
MODULES OVER DEDEKIND DOMAINS

Now that we have established the basic ring-theoretic properties of Dedekind domains, we turn to the problem of classifying their finitely generated modules. We attack this problem in three steps. In the first step, we obtain a structure theorem for the projective modules over an arbitrary Dedekind domain. Next, we specialize to the case that the Dedekind domain is a valuation ring, that is, it has only one nonzero prime ideal. Given a general Dedekind domain $\mathcal{O}$ and a prime $\mathfrak{p}$ of $\mathcal{O}$, there is a canonical valuation ring $\mathcal{O}_{\mathfrak{p}}$, the localization of $\mathcal{O}$ at $\mathfrak{p}$, whose prime ideal corresponds to the chosen prime ideal of $\mathcal{O}$. Since a valuation ring is a Euclidean domain, we can apply the results of section 3.3 to describe its modules. Finally, we piece together the structure of a module over a general Dedekind domain from our knowledge of the modules over its various localizations.

In passing, we obtain some results on modules over commutative principal ideal domains that were promised in Chapter 3, but which cannot be conveniently derived from a discussion of noncommutative Euclidean domains.

Two methods of argument in this chapter foreshadow techniques that we consider in greater depth in [BK: CM]. The construction of a localization in section 6.2 is a special case of a more general construction that we consider in section 6.1 of [BK: CM], and the arguments in section 6.3 are a first glimpse of the 'local–global' methods which we discuss in section 7.3 of [BK: CM].

As is customary in this text, we deal with right modules unless the contrary is stated. However, save for some examples, all rings mentioned in this chapter are commutative, and so all modules can be regarded as balanced bimodules (1.2.7). We take advantage of this observation to switch sides on occasion when it seems more natural to work with left scalar multiplication rather than right. This happens mostly when we deal with the ideals of a ring.

6.1 PROJECTIVE MODULES OVER DEDEKIND DOMAINS

Our aim in this section is to classify the finitely generated projective modules over a Dedekind domain $\mathcal{O}$. We show that every ideal of $\mathcal{O}$ is projective and that every projective $\mathcal{O}$-module is a direct sum of ideals. Furthermore, we can write a projective module in the form $P \cong \mathcal{O}^{r-1} \oplus \mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathcal{O}$. The integer r and the ideal class $\{\mathfrak{a}\}$ in $\mathrm{Cl}(\mathcal{O})$ are uniquely determined by the module P (and vice versa), so we can see that there will be non-free projective $\mathcal{O}$-modules provided that the class group $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$ is nontrivial.

We begin with a fact that was first made explicit with the introduction of the techniques of homological algebra, [Cartan & Eilenberg 1956], VII, §§3, 5.

6.1.1 Lemma

Let $\mathfrak{a}$ be a fractional ideal of a Dedekind domain $\mathcal{O}$. Then $\mathfrak{a}$ is a finitely generated projective $\mathcal{O}$-module.

In particular, any integral ideal of $\mathcal{O}$ is a finitely generated projective $\mathcal{O}$-module.

Proof

By (5.1.8), $d\mathfrak{a} \subseteq \mathcal{O}$ for some nonzero element d of $\mathcal{O}$. Evidently, $d\mathfrak{a} \cong \mathfrak{a}$ as an $\mathcal{O}$-module, so we may assume that $\mathfrak{a}$ is integral.

By (5.1.23), $\mathfrak{a}$ is generated by two elements, a_1, a_2, say. Choose any nonzero element x in $\mathfrak{a}$ and define, using invertibility, a fractional ideal $\mathfrak{b}$ by $x\mathcal{O} = \mathfrak{a}\mathfrak{b}$. Then $x = a_1b_1 + a_2b_2$, with b_1, b_2 in $\mathfrak{b}$. There is a surjection $\pi : \mathcal{O}^2 \to \mathfrak{a}$ given by

$$\pi(y_1, y_2) = y_1a_1 + y_2a_2,$$

which is split by the map $z \mapsto (zb_1/x, zb_2/x)$. The assertion now follows by (2.5.8). □

This result leads to a first description of finitely generated projective modules.

6.1.2 Theorem

Let M be a module over a Dedekind domain $\mathcal{O}$. Then the following statements are equivalent.

(i) *$M \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_s$ for a finite set $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_s\}$ of integral ideals of $\mathcal{O}$.*

(ii) *M is finitely generated and projective as an $\mathcal{O}$-module.*

(iii) *There is an injective homomorphism $\sigma : M \to \mathcal{O}^t$ for some integer t.*

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

Proof

(i) $\Rightarrow$ (ii): Immediate from the preceding lemma and (2.5.5).

(ii) $\Rightarrow$ (iii): Since M is finitely generated, there is a surjection from some finitely generated free module $\mathcal{O}^t$ to M; since M is projective, this homomorphism must be split (see (2.5.8)).

(iii) $\Rightarrow$ (i): Argue by induction on t. If $t = 1$ (or 0), M is (isomorphic to) an integral ideal of $\mathcal{O}$, and thus M is projective by the preceding result. For $t > 1$, let $\epsilon : \mathcal{O}^t \to \mathcal{O}$ be given by projection to the t th component. Then $\epsilon\sigma M$ is an ideal of $\mathcal{O}$, so projective, and

$$M \cong (M \cap \operatorname{Ker} \epsilon\sigma) \oplus \epsilon\sigma M$$

with $\sigma(M \cap \operatorname{Ker} \epsilon\sigma) \subseteq \mathcal{O}^{t-1}$. □

A more precise description of projective modules requires two preliminary results on ideals.

6.1.3 Proposition

Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals in a Dedekind domain $\mathcal{O}$. Then there is an integral ideal $\mathfrak{a}'$ in the ideal class of $\mathfrak{a}$ such that $\mathfrak{a}'$ and $\mathfrak{b}$ are coprime.

Proof

Take a nonzero element a of $\mathfrak{a}$ and let $\mathfrak{c} = (a\mathcal{O})\mathfrak{a}^{-1}$. Since $\mathcal{O}/\mathfrak{bc}$ is a principal ideal ring (5.1.22), we have $\mathfrak{c} = \mathfrak{bc} + c\mathcal{O}$ for some c in $\mathfrak{c}$. Hence $\mathfrak{ac} = \mathfrak{abc} + \mathfrak{ac}$ and so $\mathcal{O} = \mathfrak{b} + \mathfrak{a}(ca^{-1})$. □

6.1.4 Lemma

Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals of the Dedekind domain $\mathcal{O}$. Then there is an $\mathcal{O}$-module isomorphism

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathcal{O} \oplus \mathfrak{ab}.$$

Proof

First, suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime. Define a homomorphism $\alpha : \mathfrak{a} \oplus \mathfrak{b} \to \mathcal{O}$ by $\alpha(a, b) = a - b$. Then α is surjective, so split, and $\operatorname{Ker} \alpha = \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ by (5.1.5).

In general, the preceding result together with (5.1.14) shows that there is an ideal $\mathfrak{a}' \cong \mathfrak{a}$ with $\mathfrak{a}'$ and $\mathfrak{b}$ coprime; then $\mathfrak{a}'\mathfrak{b} \cong \mathfrak{ab}$. □

We also need an enhanced version of the process of 'clearing denominators' introduced in (5.1.7).

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.1.5 Lemma

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $\mathcal{K}$ and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ be integral ideals of $\mathcal{O}$. Then

(i) *any element of the vector space $\mathcal{K}^r$ can be written in the form*

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} a_1 d^{-1} \\ \vdots \\ a_r d^{-1} \end{pmatrix}$$

with $d \in \mathcal{O}$ and $a_i \in \mathfrak{a}_i$ for each i,

(ii) $\mathcal{K}^r = (\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r)\mathcal{K}$.

Proof

Using (5.1.8), it is easily seen that for each i we can write $x_i = c_i/d_i$ with c_i in $\mathfrak{a}_i$ and d_i in $\mathcal{O}$. Taking $d = d_1 \cdots d_r$, we obtain (i), and (ii) is immediate. □

We can now present the main result [Steinitz 1912].

6.1.6 Steinitz' Theorem

Let $\mathcal{O}$ be a Dedekind domain and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ and $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$ be integral ideals of $\mathcal{O}$. Then the following assertions are equivalent:

(i) *there is an $\mathcal{O}$-module isomorphism*

$$\phi : \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \longrightarrow \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s;$$

(ii) $$r = s \text{ and } \{\mathfrak{a}_1 \cdots \mathfrak{a}_r\} = \{\mathfrak{b}_1 \cdots \mathfrak{b}_r\} \text{ in } \mathrm{Cl}(\mathcal{O}).$$

Proof

(i) ⇒ (ii): Let $\mathcal{K}$ be the field of fractions of $\mathcal{O}$ and let $\phi : \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \to \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ be the given isomorphism. By the preceding lemma, an element x of the space $\mathcal{K}^r$ can be expressed in the form $x = a/d$ with $a \in \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ and $d \in \mathcal{O}$. Extend ϕ to a map ϕ' from $\mathcal{K}^r$ to $\mathcal{K}^s$ by $\phi'(x) = \phi(a)/d$. It is straightforward to verify that ϕ' is a well-defined $\mathcal{K}$-linear map and an isomorphism of $\mathcal{K}$-spaces. Thus $r = s$, and both ϕ' and ϕ are represented by left multiplication by a matrix $Q = (q_{ij})$ over $\mathcal{K}$. (Recall that we work with right modules and therefore regard the vector space $\mathcal{K}^r$ as a 'column-space'; see (2.2.9) for a discussion of the relation between endomorphisms of a free module and matrices. In particular, note that the matrix Q is determined to within conjugacy, so that its determinant $\det Q$ is uniquely defined.)

Let

$$a = \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} \in \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r.$$

Since $Qa \in \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r$, we have $\sum_j q_{ij}a_j \in \mathfrak{b}_i$ for all i. In particular, taking $a_h = 0$ for $h \neq j$, we find that $q_{ij}a_j \in \mathfrak{b}_i$ for all i, j. So

$$\begin{aligned} \det(Q) \cdot a_1 \cdots a_r &= \det(Q \cdot \operatorname{diag}(a_1, \ldots, a_r)) \\ &= \det \begin{pmatrix} q_{11}a_1 & \cdots & q_{1r}a_r \\ \vdots & \ddots & \vdots \\ q_{r1}a_1 & \cdots & q_{rr}a_r \end{pmatrix} \\ &\in \mathfrak{b}_1 \cdots \mathfrak{b}_r. \end{aligned}$$

Since $\mathfrak{a}_1 \cdots \mathfrak{a}_r$ is generated by all products $a_1 \cdots a_r$, we find that

$$\det(Q)\mathfrak{a}_1 \cdots \mathfrak{a}_r \subseteq \mathfrak{b}_1 \cdots \mathfrak{b}_r.$$

Similarly, $\det(Q^{-1})\mathfrak{b}_1 \cdots \mathfrak{b}_r \subseteq \mathfrak{a}_1 \cdots \mathfrak{a}_r$, which gives

$$\{\mathfrak{a}_1 \cdots \mathfrak{a}_r\} = \{\mathfrak{b}_1 \cdots \mathfrak{b}_r\}.$$

(ii) $\Rightarrow$ (i): By Lemma (6.1.4) and induction,

$$\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \cong \mathcal{O}^{r-1} \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_r$$

and

$$\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r \cong \mathcal{O}^{r-1} \oplus \mathfrak{b}_1 \cdots \mathfrak{b}_r.$$

However, $\{\mathfrak{a}_1 \cdots \mathfrak{a}_r\} = \{\mathfrak{b}_1 \cdots \mathfrak{b}_r\}$ implies that $\mathfrak{a}_1 \cdots \mathfrak{a}_r \cong \mathfrak{b}_1 \cdots \mathfrak{b}_r$ by (5.1.14). □

6.1.7 The standard form

Steinitz' Theorem tells us that the isomorphism type of a finitely generated projective $\mathcal{O}$-module $M \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ is characterized by two invariants, namely, its *rank*, which is the integer r, and its *ideal class* $\{M\} = \{\mathfrak{a}_1 \cdots \mathfrak{a}_r\}$ in $\mathrm{Cl}(\mathcal{O})$.

Note in particular that M is isomorphic to a projective module in *standard form* $\mathcal{O}^{r-1} \oplus \mathfrak{a}$ with $\mathfrak{a}$ an integral ideal, since by (5.1.14) every ideal class has an integral representative.

The next consequence of Steinitz' Theorem should be contrasted with the phenomenon of non-cancellation which we saw in (3.3.10).

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.1.8 Corollary

Cancellation holds for projective modules over a Dedekind domain: if

$$M \oplus \mathcal{O} \cong N \oplus \mathcal{O}$$

with M and N finitely generated projective, then

$$M \cong N. \qquad \square$$

On the other hand, if we allow both components of the direct sum to vary, we obtain the following observation.

6.1.9 Corollary

If $\mathrm{Cl}(\mathcal{O})$ *is nontrivial, with* $\{\mathfrak{a}\} \neq 1$, *then*

$$\mathfrak{a} \oplus \mathfrak{a}^{-1} \cong \mathcal{O}^2,$$

but

$$\mathfrak{a} \ncong \mathcal{O} \text{ and } \mathfrak{a}^{-1} \ncong \mathcal{O}. \qquad \square$$

We also obtain a result which is more often proved without invoking the theory of Dedekind domains.

6.1.10 Corollary

Let $\mathcal{O}$ be a commutative principal ideal domain. Then every finitely generated projective $\mathcal{O}$-module is free. $\square$

6.1.11 The noncommutative case

The definition of a Dedekind domain can be extended to allow the possibility of noncommutative Dedekind rings, which include the noncommutative Euclidean rings that we discussed in Chapter 4. Such rings share many of the properties of commutative Dedekind domains; comprehensive details can be found in Chapter 5 of [McConnell & Robson 1987].

Exercises

6.1.1 A converse to (6.1.1); see also Exercise 5.1.2.

Let $\mathcal{O}$ be a commutative domain with field of fractions $\mathcal{K}$, and let $\mathfrak{a}$ be a (nonzero) integral ideal of $\mathcal{O}$. Suppose that there is an integral ideal $\mathfrak{a}'$ with $\mathfrak{a}\mathfrak{a}' = x\mathcal{O}$ for some nonzero element x in $\mathcal{O}$. Show that $\mathfrak{a}$ is finitely generated and projective.

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.1.2 Let K be a field. Show that the ideal (X, Y) in the polynomial ring $K[X, Y]$ is not projective

(a) by invoking Exercise 5.1.6,

(b) by showing directly that the surjection $\pi : (K[X, Y])^2 \to (X, Y)$, $\pi(f, g) = Xf - Yg$, cannot be split.

More generally, show that the ideal $(X_1, \ldots, X_k)$ of the polynomial ring $K[X_1, \ldots, X_n]$ is not projective for $n \geq k \geq 2$.

6.1.3 **Tiled orders**

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Given a collection $X = \{\mathfrak{a}_{ij} \mid i, j = 1, \ldots, r\}$ of fractional ideals of $\mathcal{O}$, the *set of tiled matrices* associated to X is the set $T(X)$ of matrices $a = (a_{ij}) \in M_r(K)$ such that $a_{ij} \in \mathfrak{a}_{ij}$ for all i, j.

Show that $T(X)$ is a subring of $M_r(K)$ if and only if $\mathfrak{a}_{ii} = \mathcal{O}$ for all i and $\mathfrak{a}_{ij}\mathfrak{a}_{jk} \subseteq \mathfrak{a}_{ik}$ for all i, j, k.

Show also that, if $T(X)$ is a ring, it is an $\mathcal{O}$-order. Such an order is known as a *tiled order*.

Using Exercises 5.1.8 and 2.1.6, show that the endomorphism ring $\mathrm{End}(M_{\mathcal{O}})$ of a projective (right) $\mathcal{O}$-module $M = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ is the tiled order associated to the set

$$\{\mathfrak{a}_i \mathfrak{a}_j^{-1} \mid i, j = 1, \ldots, r\}.$$

Write down this order when M is in standard form $\mathcal{O}^{r-1} \oplus \mathfrak{a}$.

6.1.4 Suppose that $M = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ and $N = \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ are projective (right) $\mathcal{O}$-modules. Generalize the previous exercise by showing that $\mathrm{Hom}(M, N)$ can be described as the set of $s \times r$ tiled matrices associated with the set of ideals

$$\{\mathfrak{b}_i \mathfrak{a}_j^{-1} \mid i = 1, \ldots, s,\ j = 1, \ldots, r\}.$$

Verify that $\mathrm{Hom}(M, N)$ is an $\mathrm{End}(N)$-$\mathrm{End}(M)$-bimodule by checking the matrix multiplications.

6.2 VALUATION RINGS

In this section, we introduce the valuation associated to a nonzero prime ideal $\mathfrak{p}$ of a Dedekind domain $\mathcal{O}$ and the corresponding valuation ring $\mathcal{O}_{\mathfrak{p}}$. Such a ring $\mathcal{O}_{\mathfrak{p}}$ has a very transparent internal structure. It is a Euclidean domain and hence a principal ideal domain; further, it has only one nonzero prime ideal, and any nonzero ideal is a power of this prime. Thus the module theory of $\mathcal{O}_{\mathfrak{p}}$ is known since it is a special case of that given in section 3.3 for

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

Euclidean domains. In the next section we show how to combine the results for each separate prime $\mathfrak{p}$ to complete the determination of the structure of $\mathcal{O}$-modules.

6.2.1 *Valuations*

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $\mathcal{K}$ and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. By (5.1.19), any fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ has a factorization $\mathfrak{a} = \mathfrak{p}^{v(\mathfrak{a})}\mathfrak{a}'$, where $v(\mathfrak{a}) = v(\mathfrak{p}, \mathfrak{a})$ is an integer uniquely determined by $\mathfrak{a}$, and $\mathfrak{a}'$ is a product of prime ideals other than $\mathfrak{p}$. Of course, we may have $\mathfrak{a}' = \mathcal{O}$, and, by definition, $v(\mathfrak{p}, \mathfrak{a}') = 0$. The integer $v(\mathfrak{a})$ is called the $\mathfrak{p}$-*adic valuation* of $\mathfrak{a}$.

If $\mathfrak{p} = p\mathcal{O}$ is a principal ideal, we may speak instead of the *p-adic valuation.*

If x is a nonzero element of $\mathcal{K}$, we define the $\mathfrak{p}$-adic valuation of x to be $v(x) = v(x\mathcal{O})$. For convenience, we put $v(0) = \infty$, with 0 being either the ideal or the element.

Thus we have functions

$$v : \mathrm{Frac}(\mathcal{O}) \cup \{0\} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

and

$$v : \mathcal{K} \longrightarrow \mathbb{Z} \cup \{\infty\};$$

the context should make it clear which is intended. It is helpful to extend the usual ordering on $\mathbb{Z}$ to $\mathbb{Z} \cup \{\infty\}$ by setting $n < \infty$ for any integer n.

The elementary properties of these functions are easy to check. For example, to check surjectivity, note as in Exercise 5.1.4 that a proper invertible ideal $\mathfrak{p}$ can never have $\mathfrak{p}^k = \mathfrak{p}^{k+1}$. We record the results for ideals and for elements separately.

6.2.2 Lemma

Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of a Dedekind domain $\mathcal{O}$, and let v be the $\mathfrak{p}$-adic valuation for some prime $\mathfrak{p}$ of $\mathcal{O}$. Then

$$v : \mathrm{Frac}(\mathcal{O}) \cup \{0\} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

is a surjective function with the following properties:

(i) $v(\mathfrak{a}) = \infty$ *if and only if* $\mathfrak{a} = 0$;
(ii) $v(\mathfrak{a} + \mathfrak{b}) \geq \min(v(\mathfrak{a}), v(\mathfrak{b}))$, *with equality if* $v(\mathfrak{a}) \neq v(\mathfrak{b})$;
(iii) $v(\mathfrak{ab}) = v(\mathfrak{a}) + v(\mathfrak{b})$;
(iv) $v(\mathfrak{p}) = 1$;
(v) $v(\mathcal{O}) = 0$;

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

(vi) $v(\mathfrak{a}^{-1}) = -v(\mathfrak{a})$. □

6.2.3 Lemma

Let x and y be nonzero elements of the field of fractions $\mathcal{K}$ of a Dedekind domain $\mathcal{O}$, with v as before. Then

$$v : \mathcal{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

and its restriction

$$v : \mathcal{O} \longrightarrow \{0\} \cup \mathbb{N} \cup \{\infty\}$$

are surjective functions with the following properties:

(i) $v(x) = \infty$ *if and only if* $x = 0$;
(ii) $v(x + y) \geq \min(v(x), v(y))$, *with equality if* $v(x) \neq v(y)$;
(iii) $v(xy) = v(x) + v(y)$;
(iv) $v(p) = 1$ *for any element* $p \in \mathfrak{p} \backslash \mathfrak{p}^2$, *and such elements exist;*
(v) $v(1) = 0$;
(vi) $v(x^{-1}) = -v(x)$. □

Observe that in each of the lemmas above, properties (v) and (vi) are of secondary importance, since they can be deduced from (iii).

The function v is more properly described as a *discrete rank one valuation*, since there is a wider theory of valuations which may have values in ordered groups other than $\mathbb{Z}$, for example $\mathbb{R}$ (non-discrete) or $\mathbb{Z}^n$ (rank n). Such matters are discussed in [Cohn 1991]. However, we have no cause to consider these more general valuations, so we dispense with the qualifying adjectives.

6.2.4 Localization

The *valuation ring* or *localization* of $\mathcal{O}$ at $\mathfrak{p}$ is defined to be the subring $\mathcal{O}_\mathfrak{p}$ of $\mathcal{K}$ consisting of all fractions which can be written in the form a/b with $a, b \in \mathcal{O}$ and $b \notin \mathfrak{p}$. It is not hard to verify that $\mathcal{O}_\mathfrak{p}$ is a subring of $\mathcal{K}$, the crucial point being that, if $b_1, b_2 \in \mathcal{O}$ and $b_1, b_2 \notin \mathfrak{p}$, then $b_1 b_2 \notin \mathfrak{p}$ since $\mathfrak{p}$ is a prime ideal.

To identify the localization in terms of the corresponding valuation, we need a useful lemma.

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.2.5 Lemma

Let $\mathfrak{p}$ be a nonzero prime ideal of a Dedekind domain $\mathcal{O}$ and choose any $p \in \mathfrak{p} \backslash \mathfrak{p}^2$. Let $a \in \mathcal{O}$ and put $v = v(a)$. Then there exist

$$a', a'' \in \mathcal{O} \backslash \mathfrak{p}$$

with

$$aa' = p^v a''.$$

Proof

By (6.2.3), $v(ap^{-v}) = 0$, and so (5.1.19) shows that $ap^{-v}\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ for integral ideals $\mathfrak{a}, \mathfrak{b}$, neither of which is divisible by $\mathfrak{p}$. Take any $a' \in \mathfrak{b} \backslash \mathfrak{p}$; then $aa'p^{-v} = a'' \in \mathfrak{a} \backslash \mathfrak{p}$. □

We obtain an alternative characterization of the localization.

6.2.6 Theorem

Let $\mathfrak{p}$ be a nonzero prime ideal of the Dedekind domain $\mathcal{O}$. Then

$$\mathcal{O}_{\mathfrak{p}} = \{x \in \mathcal{K} \mid v(x) \geq 0\}.$$

Proof

It is clear that $\mathcal{O}_{\mathfrak{p}}$ is contained in the right-hand set. For the converse, take x in $\mathcal{K}$ with $v(x) \geq 0$, and write $x = a/b$ with a and b in $\mathcal{O}$. Put $y = v(a)$ and $z = v(b)$, so that $y \geq z$.

Choose some element p in $\mathfrak{p} \backslash \mathfrak{p}^2$. By the lemma, $aa' = p^y a''$ and $bb' = p^z b''$ with $a', a'', b', b'' \in \mathcal{O} \backslash \mathfrak{p}$. Then

$$x = aa'b'/bb'a' = p^{y-z} a''b'/b''a' \in \mathcal{O}_{\mathfrak{p}}.$$ □

Consider an element x of $\mathcal{K}$. Clearly, x belongs to $\mathcal{O}$ precisely when the ideal $x\mathcal{O}$ is integral, which by (5.1.20) is the same as requiring that $v_{\mathfrak{p}}(x) \geq 0$ for all prime ideals $\mathfrak{p}$. This observation gives an important property of Dedekind domains.

6.2.7 Theorem

Let $\mathcal{O}$ be a Dedekind domain. Then $\mathcal{O} = \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$, where the intersection is taken over all the (nonzero) prime ideals of $\mathcal{O}$. □

The following result is a straightforward application of the properties of valuations that are listed in (6.2.2) and (6.2.3). It also relies on our discussion of local rings in (4.3.24).

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.2.8 Proposition

(i) *Let $x, y \in \mathcal{O}_\mathfrak{p}$ be nonzero. Then $x \mid y$ if and only if $v(x) \leq v(y)$.*
(ii) *Let $x \in \mathcal{K}$, $\neq 0$. Then either x or x^{-1} is in $\mathcal{O}_\mathfrak{p}$.*
(iii) *The group of units in $\mathcal{O}_\mathfrak{p}$ is $U(\mathcal{O}_\mathfrak{p}) = \{x \in \mathcal{K} \mid v(x) = 0\}$.*
(iv) *$\mathcal{O}_\mathfrak{p}$ is a local ring with maximal ideal*

$$\mathfrak{p}\mathcal{O}_\mathfrak{p} = \{x \in \mathcal{K} \mid v(x) \geq 1\}.$$

(v) *The ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is principal, generated by any element $p \in \mathcal{K}$ with $v(p) = 1$.*
(vi) *The fractional $\mathcal{O}_\mathfrak{p}$-ideals in $\mathcal{K}$ are the powers*

$$(\mathfrak{p}\mathcal{O}_\mathfrak{p})^i = \{x \in \mathcal{K} \mid v(x) \geq i\},\ i \in \mathbb{Z}.$$

(vii) *$\mathcal{O}_\mathfrak{p}$ is a principal ideal domain.* □

6.2.9 Uniformizing parameters

An element p of $\mathcal{O}_\mathfrak{p}$ with $v(p) = 1$ is sometimes called a *uniformizing parameter*, or *uniformizer* or *prime element*, because of property (v) above. Note that p can always be chosen to be an element of $\mathcal{O}$ itself. In view of (vii), the ring $\mathcal{O}_\mathfrak{p}$ may also be referred to as a *principal valuation ring* (nonprincipal valuation rings appear in geometric contexts that we do not consider in this text).

6.2.10 The localization as a Euclidean domain

We obtain the structure theory for modules over the valuation ring $\mathcal{O}_\mathfrak{p}$ as a special case of that for Euclidean domains. Recall from (3.2.7) that we need to define a function

$$\varphi : \mathcal{O}_\mathfrak{p} \longrightarrow \{0\} \cup \mathbb{N}$$

with the following properties:

(ED1) $\varphi(a) = 0 \Leftrightarrow a = 0$, where a is in $\mathcal{O}_\mathfrak{p}$;
(ED2) $\varphi(ab) \geq \varphi(a)$ for all nonzero a and b in $\mathcal{O}_\mathfrak{p}$;
(ED3) given a and b in $\mathcal{O}_\mathfrak{p}$, we have $a = bq + r$ for some q and r in $\mathcal{O}_\mathfrak{p}$ with $0 \leq \varphi(r) < \varphi(b)$.

The simplest choice is to put $\varphi(0) = 0$ and $\varphi(a) = 1 + v(a)$ otherwise. By definition, (ED1) holds, and (ED2) is immediate from part (ii) of (6.2.3). The division algorithm is rather trivially satisfied, since part (i) of (6.2.8) shows that we can take $r = a$ if $b \nmid a$.

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

Thus the Diagonal Reduction Theorem (3.3.2) holds for $\mathcal{O}_\mathfrak{p}$, from which we obtain, as in section 3.3, the structure of $\mathcal{O}_\mathfrak{p}$-modules. For convenience, we record this special case of (3.3.6) separately.

6.2.11 The Invariant Factor Theorem

Let M be a finitely generated (right) $\mathcal{O}_\mathfrak{p}$-module. Then

$$M \cong \mathcal{O}_\mathfrak{p}/d_1\mathcal{O}_\mathfrak{p} \oplus \cdots \oplus \mathcal{O}_\mathfrak{p}/d_\ell\mathcal{O}_\mathfrak{p} \oplus (\mathcal{O}_\mathfrak{p})^s,$$

where $d_1, \ldots, d_\ell$ are nonunits in $\mathcal{O}_\mathfrak{p}$, $d_1 \mid d_2 \mid \cdots \mid d_\ell$ and $s \geq 0$. □

It is convenient to rephrase the Invariant Factor Theorem in terms of ideals. To do this, put $\delta(i) = v(d_i)$ for $i = 1, \ldots, \ell$.

6.2.12 Corollary

Let M be a finitely generated (right) $\mathcal{O}_\mathfrak{p}$-module. Then

$$M \cong \mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^{\delta(1)} \oplus \cdots \oplus \mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^{\delta(\ell)} \oplus (\mathcal{O}_\mathfrak{p})^s,$$

where $\delta(1) \leq \cdots \leq \delta(\ell)$ are positive integers. □

6.2.13 Rank and invariant factors

As defined in (3.3.7), the elements $d_1, \ldots, d_\ell$ of $\mathcal{O}_\mathfrak{p}$ are the invariant factors of M, and the integer s is the rank of M. We can equally refer to the ideals $(\mathfrak{p}\mathcal{O}_\mathfrak{p})^{\delta(1)}, \ldots, (\mathfrak{p}\mathcal{O}_\mathfrak{p})^{\delta(\ell)}$ as being the invariant factors of M.

In the next section, we show that the invariant factors are uniquely determined by the module M (6.3.12), that is, the elements $d_1, \ldots, d_\ell$ are determined up to multiplication by units of $\mathcal{O}_\mathfrak{p}$. The rank of M is also unique, which we confirm in (6.3.6).

Exercises

6.2.1 Let $\mathcal{O}$ be a Dedekind domain and let $\mathbf{Q}$ be a subset of the set $\mathbf{P}$ of nonzero prime ideals of $\mathcal{O}$. Show that

$$\mathcal{O}_\mathbf{Q} = \bigcap_{\mathfrak{p} \in \mathbf{Q}} \mathcal{O}_\mathfrak{p}$$

is also a Dedekind domain and find its prime ideals.

Show that $\mathcal{O}_\mathbf{Q}$ is not a finitely generated $\mathcal{O}$-module unless $\mathbf{P} = \mathbf{Q}$. (Exercise 5.1.10 helps.)

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.2.2 Let $\mathcal{O} = \mathcal{O}_{\mathfrak{p}}$ be a valuation ring with (unique) maximal ideal $\mathfrak{p}$, and suppose that R is an $\mathcal{O}$-order.

Show that any finitely generated right R-module is also finitely generated as an $\mathcal{O}$-module.

Deduce that

(i) $\mathfrak{p}R \subseteq \mathrm{rad}(R)$, the Jacobson radical of R as a ring,
(ii) R is a semilocal ring,
(iii) $\mathrm{rad}(R) = \pi^{-1}(\mathrm{rad}(R/\mathfrak{p}R))$, the inverse image with respect to the natural homomorphism π from R to $R/\mathfrak{p}R$,
(iv) $(\mathrm{rad}(R))^h \subseteq \mathfrak{p}R$ for some integer h.

Hint. Nakayama's Lemma (4.3.10), together with (4.3.12), may be useful.

6.2.3 Let $\mathcal{O}$ be a valuation ring with maximal ideal $\mathfrak{p}$ and suppose that $\mathcal{O}$ has characteristic 0, so that $\mathbb{Z}$ can be regarded as a subring of $\mathcal{O}$ (1.1.10). Show that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, where the prime p is the characteristic of the field $\mathcal{O}/\mathfrak{p}$.

Let G be a finite group, and let $\mathcal{O}G$ be its group ring over $\mathcal{O}$.

(i) Show that, if p does not divide the order $|G|$ of G, then

$$\mathrm{rad}(\mathcal{O}G) = \mathfrak{p}G.$$

(ii) Suppose that $G = \langle \gamma \rangle$ is cyclic of order p. Show that

$$\mathrm{rad}(\mathcal{O}G) = (1 - \gamma)\mathcal{O}G.$$

[Exercises 4.3.9 and 4.3.11 are relevant.]

6.2.4 Let $\mathcal{O}$ be a valuation ring with maximal ideal $\mathfrak{p}$, and let $R = \begin{pmatrix} \mathcal{O} & \mathfrak{p}^h \\ \mathcal{O} & \mathcal{O} \end{pmatrix}$ be the tiled order consisting of those matrices in $M_2(\mathcal{O})$ with $(1,2)$ th entry belonging to $\mathfrak{p}^h$ where h is an integer, $h \geq 0$.

Show that

$$\mathrm{rad}(R) = \begin{cases} \mathfrak{p}R & h = 0 \\ \begin{pmatrix} \mathfrak{p} & \mathfrak{p}^h \\ \mathcal{O} & \mathfrak{p} \end{pmatrix} & h \geq 1 \end{cases}$$

and that

$$\mathrm{rad}(R)^2 = \begin{cases} \mathfrak{p}R & h = 1 \\ \mathfrak{p}\,\mathrm{rad}(R) & h \neq 1 \end{cases}$$

Let $C(i) = \begin{pmatrix} \mathfrak{p}^i \\ \mathcal{O} \end{pmatrix}$ for $i = 0, \ldots, h$. Prove that each $C(i)$ is a

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

right R-module, and that $C(i) \cong C(j)$ (as an R-module) if and only if $i = j$.

Hint. Any such isomorphism extends to an $M_2(\mathcal{K})$-homomorphism of the irreducible right module $\begin{pmatrix} \mathcal{K} \\ \mathcal{K} \end{pmatrix}$, where $\mathcal{K}$ is the field of fractions of $\mathcal{O}$, and so must be given by left multiplication by an element of $\mathcal{K}$.

In Exercise 7.2.5 of [BK: CM], we show that $C(i)$ is projective as an R-module if and only if $i = 0$ or h, and that any finitely generated projective right R-module is isomorphic to a direct sum of copies of $C(0)$ and $C(h)$. *Assuming* this result, deduce that $\mathrm{rad}(R)$ is projective as a right R-module if and only if $h = 0, 1$.

Remark. For $h = 0, 1$, R is an example of a hereditary order, the theory of which is discussed in detail in [Reiner 1975], Chapter 9; for $h = 0$, the order is maximal.

6.2.5 Repeat the previous exercise with

$$R = \begin{pmatrix} \mathcal{O} & \mathfrak{p}^h & \dots & \mathfrak{p}^h & \mathfrak{p}^h \\ \mathcal{O} & \mathcal{O} & \dots & \mathfrak{p}^h & \mathfrak{p}^h \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{O} & \mathfrak{p}^h \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{O} & \mathcal{O} \end{pmatrix},$$

the $\mathcal{O}$-order consisting of all $n \times n$ matrices with entries above the diagonal belonging to $\mathfrak{p}^h$.

(*Warning.* The same ideas work but are trickier to implement; the generalization of the module $C(i)$ requires multiple indices.)

6.3 TORSION MODULES OVER DEDEKIND DOMAINS

We now combine the results of the preceding two sections to obtain a complete description of the finitely generated modules over an arbitrary Dedekind domain $\mathcal{O}$. We show that an $\mathcal{O}$-module can be decomposed into a direct sum of a torsion-free component and a torsion component. The results of section 6.1 show that the torsion-free component is projective and so its structure is known. The torsion component further decomposes into $\mathfrak{p}$-primary components, one for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$. Almost all of these primary components are zero, and each is a torsion module over the corresponding valuation ring $\mathcal{O}_\mathfrak{p}$, so that its structure is known by the results of the previous section.

As a special case, we obtain a description of the structure of the finitely generated modules over an arbitrary commutative principal ideal domain.

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

The systematic use of the local rings $\mathcal{O}_\mathfrak{p}$ to obtain results on $\mathcal{O}$-modules is comparatively recent, originating with [Krull 1938].

6.3.1 Torsion modules

Let M be a right module over a commutative domain $\mathcal{O}$. An element m in M is said to be a *torsion element* if $mr = 0$ for some $r \neq 0$ in $\mathcal{O}$. The set of all torsion elements in M is denoted by $T(M)$ and called the *torsion submodule* of M. An easy verification reveals that $T(M)$ is indeed a submodule of M.

We say that M is a *torsion module* if $M = T(M)$ and, as in (1.2.23), that M is torsion-free if $T(M) = 0$. (The zero module is therefore both a torsion module and torsion-free; to avoid a proliferation of qualifying phrases, we agree to ignore trivial modifications that result from inserting or deleting zero modules.)

The following is routine.

6.3.2 Lemma

Let M be an $\mathcal{O}$-module, where $\mathcal{O}$ is a commutative domain. Then $T(M)$ is a torsion module and $M/T(M)$ is torsion-free. □

It is clear that the free module $\mathcal{O}^k$ is torsion-free, as are all its submodules. The next result tells us that, in essence, any finitely generated torsion-free module arises as a submodule of a free module.

6.3.3 Lemma

Let M be a finitely generated torsion-free $\mathcal{O}$-module, where $\mathcal{O}$ is a commutative domain. Then there is an injective $\mathcal{O}$-module homomorphism from M to $\mathcal{O}^k$ for some integer k.

Proof

By (1.2.23), the $\mathcal{O}$-module M spans a vector space V over the field of fractions $\mathcal{K}$ of $\mathcal{O}$. Since M is finitely generated, V is finite-dimensional. Choose a set of generators $\{m_1, \ldots, m_\ell\}$ of M and a basis $\{e_1, \ldots, e_k\}$ of V, and write

$$m_j = \sum_i e_i x_{ij} \quad \text{with } x_{ij} \in \mathcal{K}.$$

The coefficients can be put over a common denominator d, and then

$$M \cong Md \subseteq e_1\mathcal{O} \oplus \cdots \oplus e_k\mathcal{O}.$$ □

We combine the above result with (6.1.2).

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.3.4 Corollary

Let M be a finitely generated torsion-free module over a Dedekind domain $\mathcal{O}$. Then M is projective. □

Since $M/T(M)$ is torsion-free, the next result is immediate from the definition of a projective module (2.5.1).

6.3.5 Theorem

Let M be a finitely generated module over a Dedekind domain $\mathcal{O}$. Then there is an $\mathcal{O}$-module isomorphism

$$M \cong T(M) \oplus M/T(M).$$ □

6.3.6 The rank

We can also extend the definition of the *rank* to any finitely generated module M over a commutative domain $\mathcal{O}$. If M is torsion-free, we put $\text{rank}(M) = \dim(M\mathcal{K})$, where $M\mathcal{K}$ is the space spanned by M, and, in general, we set $\text{rank}(M) = \text{rank}(M/T(M))$. It is clear that this definition coincides with our previous definition when $\mathcal{O}$ is a Euclidean domain (3.3.7), (6.2.13). It is also obvious that the rank of a module is uniquely defined, and that $\text{rank}(M) = 0$ precisely when M is a torsion module.

6.3.7 Primary modules

Recall that, given an $\mathcal{O}$-module M, the annihilator of M is defined to be the ideal $\text{Ann}(M)$ of $\mathcal{O}$ given by

$$\text{Ann}(M) = \{r \in \mathcal{O} \mid mr = 0 \text{ for all } m \in M\}.$$

It is clear that a finitely generated $\mathcal{O}$-module has a nonzero annihilator if and only if it is a torsion module.

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. An $\mathcal{O}$-module M is called $\mathfrak{p}$-*primary* if $\text{Ann}(M) = \mathfrak{p}^\delta$ for some natural number δ. (The zero module is admitted as a $\mathfrak{p}$-primary module.) If $\mathfrak{p} = p\mathcal{O}$ is a principal ideal, we sometimes prefer to say that a module is p-*primary*. This terminology is more natural if the coefficient ring is a principal ideal domain, such as $\mathbb{Z}$.

Clearly, the factor module $\mathcal{O}/\mathfrak{p}^\delta$ is $\mathfrak{p}$-primary, as is any finite direct sum of such factor modules (with possibly differing exponents). Our aim is to show that any finitely generated $\mathfrak{p}$-primary module can be described in this way, in an essentially unique fashion.

The argument exploits the Invariant Factor Theorem (6.2.11) for the localization $\mathcal{O}_\mathfrak{p}$, the next result providing the connection. Note that any finitely generated torsion $\mathcal{O}_\mathfrak{p}$-module is necessarily $\mathfrak{p}\mathcal{O}_\mathfrak{p}$-primary, since, by (6.2.8), $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is the unique nonzero prime ideal of the principal ideal domain $\mathcal{O}_\mathfrak{p}$.

6.3.8 Proposition

For any $\delta > 0$, $\mathcal{O}/\mathfrak{p}^\delta \cong \mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$ both as rings and as $\mathcal{O}$-modules.

Proof

The natural ring homomorphism from $\mathcal{O}$ to $\mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$ clearly has kernel $\mathfrak{p}^\delta$, so there is an induced injection ι from $\mathcal{O}/\mathfrak{p}^\delta$ to $\mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$.

To see that ι is surjective, take an element $a/b \in \mathcal{O}_\mathfrak{p}$, where $a \in \mathcal{O}$ and $b \in \mathcal{O} \setminus \mathfrak{p}$, and consider the ideal $b\mathcal{O} + \mathfrak{p}^\delta$ of the Dedekind domain $\mathcal{O}$. If this ideal is proper, then, by (5.1.19), it has a unique factorization in terms of prime ideals. Combining (5.1.17) and (5.1.21), we see that the only prime ideal which could possibly occur as a factor of $b\mathcal{O} + \mathfrak{p}^\delta$ is $\mathfrak{p}$ itself. Since $b \notin \mathfrak{p}$, we have $b\mathcal{O} + \mathfrak{p}^\delta = \mathcal{O}$.

Thus $1 = bc + z$ for some c in $\mathcal{O}$ and z in $\mathfrak{p}^\delta$, so $a/b \equiv ac \pmod{(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta}$, that is, $\overline{(a/b)} = \iota(\overline{ac})$, which establishes surjectivity.

Finally, observe that the $\mathcal{O}$-module structure on $\mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta$ arises from this isomorphism – by 'change of rings' (1.2.14). □

We can now give a structure theorem for primary modules (but not yet a uniqueness theorem).

6.3.9 Theorem

Let $\mathfrak{p}$ be a nonzero prime ideal of the Dedekind domain $\mathcal{O}$, and let M be a finitely generated $\mathfrak{p}$-primary $\mathcal{O}$-module.

Then M is also a finitely generated $\mathcal{O}_\mathfrak{p}$-module, and there is a direct decomposition of M, both as an $\mathcal{O}$-module and as an $\mathcal{O}_\mathfrak{p}$-module,

$$M \cong \mathcal{O}/\mathfrak{p}^{\delta(1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(\ell)},$$

where $\delta(1) \leq \cdots \leq \delta(\ell)$ are positive integers.

Proof

By definition, the annihilator of M is $\mathfrak{p}^\delta$ for some $\delta > 0$. Thus M is naturally an $(\mathcal{O}/\mathfrak{p}^\delta)$-module, hence an $(\mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^\delta)$-module, and therefore an $\mathcal{O}_\mathfrak{p}$-module, from the previous result. By (6.2.12), M has a direct decomposition as an $\mathcal{O}_\mathfrak{p}$-module as claimed, and this decomposition is clearly also an $\mathcal{O}$-module decomposition. □

6.3.10 *Elementary divisors*

When the Dedekind domain $\mathcal{O}$ has more than one nonzero prime ideal, the ideals $\mathfrak{p}^{\delta(1)}, \ldots, \mathfrak{p}^{\delta(\ell)}$ occurring in the decomposition of a $\mathfrak{p}$-primary module M are called the *elementary divisors* of M.

If $\mathfrak{p} = p\mathcal{O}$ is principal, in particular, if $\mathcal{O}$ is a principal ideal domain, the corresponding powers $p^{\delta(\mathfrak{p},1)}, \ldots, p^{\delta(\mathfrak{p},\ell(\mathfrak{p}))}$ of the irreducible element p are often called the elementary divisors of M.

This definition anticipates the definition of elementary divisors for an arbitrary torsion module. The elementary divisors of a $\mathfrak{p}$-primary module M as an $\mathcal{O}$-module are, by definition, the same as its invariant factors when M is regarded as an $\mathcal{O}_{\mathfrak{p}}$-module. The extension of the notion of invariant factors to modules over an arbitrary Dedekind domain is outlined in Exercise 6.3.6 below.

We associate with each direct sum decomposition of a $\mathfrak{p}$-primary module into cyclic modules a sequence

$$\mathrm{edt}_{\mathfrak{p}}(M) = (\alpha_1, \alpha_2, \ldots)$$

of natural numbers in which α_i is the number of times that the term $\mathcal{O}/\mathfrak{p}^i$ occurs in the given direct sum. Once uniqueness of the decomposition has been established, as in the next theorem, this sequence may be called the $\mathfrak{p}$-*elementary divisor type* of M.

Note that $\alpha_i = 0$ for all but a finite set of indices; the maximum of the indices for which $\alpha_i \neq 0$ is the *length* of $\mathrm{edt}_{\mathfrak{p}}(M)$. Clearly, the length is the exponent k occurring in the annihilator: $\mathrm{Ann}(M) = \mathfrak{p}^k$.

The zero module corresponds to the zero sequence $(0, 0, \ldots)$, which has length 0, and $\mathcal{O}/\mathfrak{p}^k$ has type $(0, \ldots, 0, 1, 0, \ldots)$ of length k. This notion of length is not the same as the length of a composition series introduced in (4.1.8). Since the terms are used in different contexts, there should be no confusion.

Our main result shows that the elementary divisor type $\mathrm{edt}_{\mathfrak{p}}(M)$ describes a $\mathfrak{p}$-primary module completely.

6.3.11 Theorem

Let M and N be finitely generated $\mathfrak{p}$-primary $\mathcal{O}$-modules. Then $M \cong N$ if and only if $\mathrm{edt}_{\mathfrak{p}}(M) = \mathrm{edt}_{\mathfrak{p}}(N)$.

Proof

It is obvious that if $\mathrm{edt}_{\mathfrak{p}}(M) = \mathrm{edt}_{\mathfrak{p}}(N)$ then $M \cong N$. Suppose conversely

that $M \cong N$, and write

$$\mathrm{edt}_{\mathfrak{p}}(M) = (\alpha_1, \alpha_2, \ldots, \alpha_k, 0, \ldots)$$

and

$$\mathrm{edt}_{\mathfrak{p}}(N) = (\beta_1, \beta_2, \ldots, \beta_\ell, 0, \ldots),$$

where k and ℓ are the lengths of the sequences. We argue by induction on k.

If $k = 1$, then M is in effect a vector space over the field $\mathcal{O}/\mathfrak{p}$ and α_1 is its dimension; since $\mathrm{Ann}(N) = \mathfrak{p}$ also, we must have $\ell = 1$ and $\alpha_1 = \beta_1$.

Now suppose $k > 1$. First, we note that the quotient modules $M/\mathfrak{p}M$ and $N/\mathfrak{p}N$ are isomorphic and have types

$$\mathrm{edt}_{\mathfrak{p}}(M/\mathfrak{p}M) = (\alpha_1 + \alpha_2 + \cdots + \alpha_k, 0, \ldots)$$

and

$$\mathrm{edt}_{\mathfrak{p}}(N/\mathfrak{p}N) = (\beta_1 + \beta_2 + \cdots + \beta_\ell, 0, \ldots)$$

respectively, which shows that

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k = \beta_1 + \beta_2 + \cdots + \beta_\ell.$$

Next we note that, since $\mathfrak{p}/\mathfrak{p}^i \cong \mathcal{O}/\mathfrak{p}^{i-1}$ for $i > 1$ by (5.1.24), the isomorphic modules $\mathfrak{p}M$ and $\mathfrak{p}N$ have types

$$\mathrm{edt}_{\mathfrak{p}}(\mathfrak{p}M) = (\alpha_2, \ldots, \alpha_k, 0, \ldots)$$

and

$$\mathrm{edt}_{\mathfrak{p}}(\mathfrak{p}N) = (\beta_2, \ldots, \beta_\ell, 0, \ldots)$$

of lengths $k - 1$ and $\ell - 1$; the result now follows by induction. □

For reference, we state an immediate consequence of the preceding result.

6.3.12 Corollary

Let $\mathfrak{p}$ be a nonzero prime ideal of a Dedekind domain $\mathcal{O}$, and let M be a finitely generated torsion $\mathcal{O}_{\mathfrak{p}}$-module. Then the invariant factors

$$(\mathfrak{p}\mathcal{O}_{\mathfrak{p}})^{\delta(1)}, \ldots, (\mathfrak{p}\mathcal{O}_{\mathfrak{p}})^{\delta(\ell)}, \quad \delta(1) \leq \cdots \leq \delta(\ell),$$

of M are unique. □

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.3.13 *Primary decomposition*

We now consider the decomposition of a finitely generated torsion $\mathcal{O}$-module M into a direct sum of $\mathfrak{p}$-primary submodules as $\mathfrak{p}$ ranges over the set $\mathbf{P} = \mathbf{P}(\mathcal{O})$ of nonzero primes of the Dedekind domain $\mathcal{O}$. This gives a characterization of M in terms of the collection $\{\mathrm{edt}_{\mathfrak{p}}(M) \mid \mathfrak{p} \in \mathbf{P}\}$ of elementary divisor types arising from its summands.

We first show that, for each $\mathfrak{p}$, M has a maximal $\mathfrak{p}$-primary submodule. To see this, note that, if M' and M'' are both $\mathfrak{p}$-primary submodules of M (that is, both have annihilators that are powers of $\mathfrak{p}$), then so also is $M' + M''$. Thus, if there were no maximal $\mathfrak{p}$-primary submodule, we could construct an infinite ascending chain in M, contrary to the fact that M is Noetherian, since it is a finitely generated module over the Noetherian ring $\mathcal{O}$ and so itself Noetherian (3.1.4).

We can therefore define the $\mathfrak{p}$-*component* $T_{\mathfrak{p}}(M)$ of M to be the maximal $\mathfrak{p}$-primary submodule of M, that is, the maximal submodule with the property that $\mathrm{Ann}(T_{\mathfrak{p}}(M)) = \mathfrak{p}^k$ for some natural number k. Alternative terms for $T_{\mathfrak{p}}(M)$ are the $\mathfrak{p}$-*torsion part* and the $\mathfrak{p}$-*primary part* of M. Since M is Noetherian, $T_{\mathfrak{p}}(M)$ is finitely generated.

The next result is the key to the existence of the primary decomposition.

6.3.14 Lemma

Let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals of $\mathcal{O}$, and let M be an $\mathcal{O}$-module such that $\mathrm{Ann}(M) = \mathfrak{ab}$.

Then $M = \mathfrak{a}M \oplus \mathfrak{b}M$, and $\mathrm{Ann}(\mathfrak{a}M) = \mathfrak{b}$ *and* $\mathrm{Ann}(\mathfrak{b}M) = \mathfrak{a}$.

Proof

Since $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, $\mathcal{O} = \mathfrak{a} + \mathfrak{b}$. Thus $1 = a + b$ for some elements a, b of $\mathfrak{a}, \mathfrak{b}$ respectively, and so $M = \mathfrak{a}M + \mathfrak{b}M$.

Suppose that $m \in \mathfrak{a}M \cap \mathfrak{b}M$. Then $am = bm = 0$ because $\mathfrak{ab}M = 0$, hence $m = (a + b)m = 0$, which gives the direct sum decomposition.

Clearly $\mathfrak{b} \subseteq \mathrm{Ann}(\mathfrak{a}M)$. Let x be in $\mathrm{Ann}(\mathfrak{a}M)$. Then $x\mathcal{O} \cdot \mathfrak{a} \subseteq \mathrm{Ann}(M) = \mathfrak{ab}$ and hence $x\mathcal{O} \subseteq \mathfrak{b}$, since $\mathfrak{a}$ is an invertible ideal. □

Given the module M and a nonzero prime ideal $\mathfrak{p}$, we write the factorization of the annihilator in the form

$$\mathrm{Ann}(M) = \mathfrak{p}^k \mathfrak{c}(\mathfrak{p}),$$

where $k \geq 0$ is the $\mathfrak{p}$-adic valuation of $\mathrm{Ann}(M)$ and $\mathfrak{p}$ and $\mathfrak{c}(\mathfrak{p})$ are coprime (see (6.2.1)). Note that $k = 0$ and $\mathfrak{c}(\mathfrak{p}) = \mathrm{Ann}(M)$ except for the finite set of primes that actually occur as factors of $\mathrm{Ann}(M)$.

6.3.15 Proposition

Let M be a finitely generated torsion module over a Dedekind domain $\mathcal{O}$. Then the following hold.

(i) $T_{\mathfrak{p}}(M) = \mathfrak{c}(\mathfrak{p})M$.
(ii) $T_{\mathfrak{p}}(M) = 0$ *for all but finitely many primes* $\mathfrak{p}$.
(iii) $M = \bigoplus_{\mathfrak{p}} T_{\mathfrak{p}}(M)$, *where the sum is taken over the set* $\mathbf{P}$ *of all nonzero primes* $\mathfrak{p}$ *of* $\mathcal{O}$.

Proof

Clearly $\mathfrak{c}(\mathfrak{p})M \subseteq T_{\mathfrak{p}}(M)$. By the lemma, we have $M = \mathfrak{p}^k M \oplus \mathfrak{c}(\mathfrak{p})M$ and $\mathrm{Ann}(\mathfrak{p}^k M) = \mathfrak{c}(\mathfrak{p})$. Thus if $m = x + n$ is in $T_{\mathfrak{p}}(M)$, where x and n belong to the respective summands of M, we find that x is annihilated by both the coprime ideals $\mathfrak{p}^k$ and $\mathfrak{c}(\mathfrak{p})$, so must be 0. Thus (i) holds, and (ii) follows since $\mathfrak{c}(\mathfrak{p}) = \mathrm{Ann}(M)$ for almost all primes.

The last part follows by induction on the number of distinct prime factors of $\mathrm{Ann}(M)$. Note that, if $\mathfrak{p}$ is a factor of $\mathrm{Ann}(M)$, then, by the preceding lemma,

$$M = \mathfrak{c}(\mathfrak{p})M \oplus \mathfrak{p}^k M = T_{\mathfrak{p}}(M) \oplus \mathfrak{p}^k M.$$

Now $\mathrm{Ann}(\mathfrak{p}^k M) = \mathfrak{c}(\mathfrak{p})$ has fewer prime factors than $\mathrm{Ann}(M)$, and $T_{\mathfrak{q}}(\mathfrak{p}^k M) = T_{\mathfrak{q}}(M)$ if $\mathfrak{q}$ is a prime different from $\mathfrak{p}$. □

We note that all possible primary decompositions actually occur.

6.3.16 Proposition

Given any set of finitely generated $\mathfrak{p}$-primary $\mathcal{O}$-modules $M_{\mathfrak{p}}$, $\mathfrak{p} \in \mathbf{P}$, only finitely many of which are nonzero, the external direct sum $M = \bigoplus M_{\mathfrak{p}}$ has $T_{\mathfrak{p}}(M) \cong M_{\mathfrak{p}}$ for all $\mathfrak{p}$. □

6.3.17 Elementary divisors again

Given an arbitrary finitely generated torsion $\mathcal{O}$-module M, the *elementary divisors* of M are the ideals

$$\mathfrak{p}^{\delta(\mathfrak{p},1)}, \ldots, \mathfrak{p}^{\delta(\mathfrak{p},\ell(\mathfrak{p}))}$$

that occur in the nontrivial $\mathfrak{p}$-primary components

$$T_{\mathfrak{p}}(M) \cong \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},\ell(\mathfrak{p}))}$$

of M, where $\mathfrak{p}$ varies through the set $\mathbf{P}$ of nonzero prime ideals of $\mathcal{O}$. So that we can list the elementary divisors unambiguously, we must choose some

convenient ordering of $\mathbf{P}$; then, for a given $\mathfrak{p}$, we take the exponents in non-decreasing order.

When $\mathcal{O}$ is a principal ideal domain, the powers

$$p^{\delta(\mathfrak{p},1)}, \ldots, p^{\delta(\mathfrak{p},\ell(\mathfrak{p}))}$$

of the irreducible elements p are more often called the elementary divisors of M. Now p will run through a representative set $\mathbf{Pe}$ of irreducible elements of $\mathcal{O}$, that is, each prime ideal $\mathfrak{p} \in \mathbf{P}$ is generated by exactly one member p of $\mathbf{Pe}$. We usually write $T_p(M)$ rather than $T_{p\mathcal{O}}(M)$ and call it the *p-primary submodule* or *p-component* of M.

The *elementary divisor type* of M is defined as follows. For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, put

$$\mathrm{edt}_{\mathfrak{p}}(M) = \mathrm{edt}_{\mathfrak{p}}(T_{\mathfrak{p}}(M))$$

which is a sequence of finite length. Then the elementary divisor type of M is defined to be

$$\mathrm{edt}(M) = (\mathrm{edt}_{\mathfrak{p}}(M) \mid \mathfrak{p} \in \mathbf{P}),$$

a sequence of such sequences, where the set $\mathbf{P}$ of primes is again given some convenient ordering. For all except a finite set of primes, $\mathrm{edt}_{\mathfrak{p}}(M) = (0, 0, \ldots)$.

It is clear that we can construct the elementary divisors of a module from its elementary divisor type, and vice versa. Before we can show that its elementary divisor type gives a complete description of a module, we need to discuss how homomorphisms affect the primary components of modules.

6.3.18 Homomorphisms

Suppose that $\lambda : M \to N$ is a homomorphism between finitely generated torsion $\mathcal{O}$-modules, where $\mathcal{O}$ is a Dedekind domain. It is clear from the description of the $\mathfrak{p}$-components of M and N that λ induces a family of $\mathcal{O}$-module homomorphisms

$$T_{\mathfrak{p}}(\lambda) : T_{\mathfrak{p}}(M) \longrightarrow T_{\mathfrak{p}}(N).$$

For all except a finite set of $\mathfrak{p}$, $T_{\mathfrak{p}}(\lambda)$ is the zero map between zero modules.

Conversely, given a family $\{\lambda(\mathfrak{p}) : T_{\mathfrak{p}}(M) \to T_{\mathfrak{p}}(N)\}$ of $\mathcal{O}$-module homomorphisms, the direct sum $\lambda = \bigoplus_{\mathfrak{p}} \lambda(\mathfrak{p})$ is a homomorphism from M to N with $T_{\mathfrak{p}}(\lambda) = \lambda(\mathfrak{p})$ for all $\mathfrak{p}$.

Our discussion should have made the following result obvious.

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.3.19 Proposition

Let M and N be finitely generated torsion $\mathcal{O}$-modules, where $\mathcal{O}$ is a Dedekind domain. Then $M \cong N$ if and only if $T_{\mathfrak{p}}(M) \cong T_{\mathfrak{p}}(N)$ for all primes $\mathfrak{p}$ of $\mathcal{O}$. □

Combining the preceding proposition with the description of primary modules in (6.3.9), together with the fact that the elementary divisor type characterizes primary modules (6.3.11), we obtain the classical description of torsion modules over a Dedekind domain.

6.3.20 The Primary Decomposition Theorem

Let M and N be finitely generated torsion modules over the Dedekind domain $\mathcal{O}$. Then

(i)

$$M \cong \bigoplus\nolimits_{\mathfrak{p}} \left(\mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},\ell(\mathfrak{p}))}\right),$$

where $\delta(\mathfrak{p},1) \leq \cdots \leq \delta(\mathfrak{p},\ell(\mathfrak{p}))$ are positive integers and $\ell(\mathfrak{p}) = 0$ for all except a finite set of primes $\mathfrak{p}$,

(ii) *$M \cong N$ if and only if $\operatorname{edt}(M) = \operatorname{edt}(N)$, that is, $\operatorname{edt}_{\mathfrak{p}}(M) = \operatorname{edt}_{\mathfrak{p}}(N)$ for all (nonzero) primes $\mathfrak{p}$ of $\mathcal{O}$,*

(iii) *the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ with $\ell(\mathfrak{p}) \neq 0$ and the positive integers $\delta(\mathfrak{p},1) \leq \cdots \leq \delta(\mathfrak{p},\ell(\mathfrak{p}))$ are uniquely determined by M, and vice versa – informally, M is determined by its elementary divisors.* □

6.3.21 Alternative decompositions

The Primary Decomposition Theorem shows that a finitely generated torsion module M is a direct sum of cyclic modules. In general, there are many ways in which a torsion module can be written as a direct sum of cyclic modules, because, by the Chinese Remainder Theorem (5.1.5), there is an isomorphism $\mathcal{O}/\mathfrak{ab} \cong \mathcal{O}/\mathfrak{a} \oplus \mathcal{O}/\mathfrak{b}$ for any pair of coprime ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$.

Thus, any uniqueness assertion for a direct decomposition of M into cyclic summands requires the imposition of some extra condition. In the Primary Decomposition Theorem, we in effect require that there are as many cyclic summands as possible. At the opposite extreme, if we ask for as few cyclic summands as possible, we are led to the Invariant Factor Theorem, which is sketched in Exercise 6.3.6 below.

In the case that $\mathcal{O}$ has only one nonzero prime ideal, that is, $\mathcal{O}$ is already local, the Invariant Factor Theorem is the same as the Primary Decomposition Theorem.

6.3.22 *Homomorphisms again*

We need some further remarks on homomorphisms as a preliminary to summarizing our results on modules over a Dedekind domain $\mathcal{O}$.

Let M and N be arbitrary finitely generated $\mathcal{O}$-modules and suppose that $\lambda : M \to N$ is a homomorphism between them. It is easy to see that λ induces a homomorphism

$$T(\lambda) : T(M) \longrightarrow T(N)$$

between the torsion submodules of M and N, and hence a homomorphism

$$F(\lambda) : M/T(M) \longrightarrow N/T(N)$$

between their torsion-free quotient modules.

By (6.3.4), $M/T(M)$ and $N/T(N)$ are projective, and so there are internal direct decompositions

$$M = T(M) \oplus M' \text{ and } N = T(N) \oplus N'$$

with

$$M/T(M) \cong M' \text{ and } N/T(N) \cong M',$$

as noted in (6.3.5). It is easy to check that λ is an isomorphism precisely when both $T(\lambda)$ and $F(\lambda)$ are isomorphisms.

Note that there is usually no canonical choice for the submodules M' and N' – see Exercise 6.3.9. In the language of categories, the methods by which $T(M)$ and $M/T(M)$ are constructed from M are both functorial, but the construction of M' is not.

We summarize all our results in one compendium, which completely classifies finitely generated modules for Dedekind domains.

6.3.23 Theorem

Let M be a finitely generated module over a Dedekind domain $\mathcal{O}$. Then the following assertions hold.

(i) $M = P \oplus T$ *where P is a finitely generated projective $\mathcal{O}$-module and $T = T(M)$ is a finitely generated torsion $\mathcal{O}$-module.*

(ii) $P \cong \mathcal{O}^{r-1} \oplus \mathfrak{a}$ *where $\mathfrak{a}$ is an ideal of $\mathcal{O}$.*

(iii) $T \cong \bigoplus_{\mathfrak{p}} T(\mathfrak{p})$, *where $\mathfrak{p}$ runs through the nonzero prime ideals of $\mathcal{O}$, each $T(\mathfrak{p}) = T_{\mathfrak{p}}(M)$ is a finitely generated $\mathfrak{p}$-primary $\mathcal{O}$-module, and $T(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$.*

(iv) *If $T(\mathfrak{p}) \neq 0$, then*

$$T(\mathfrak{p}) \cong \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(\mathfrak{p},\ell(\mathfrak{p}))},$$

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

where $0 < \delta(\mathfrak{p},1) \leq \cdots \leq \delta(\mathfrak{p},\ell(\mathfrak{p}))$ *(and if* $T(\mathfrak{p}) = 0$*, then* $\ell(\mathfrak{p}) = 0$*).*

Furthermore, the module M *determines, and in turn is determined to within isomorphism by, the following information:*

- *the integer* $r = \operatorname{rank}(M)$*,*
- *the integers* $\ell(\mathfrak{p})$ *for all* $\mathfrak{p}$*,*
- *the integers* $\delta(\mathfrak{p},i)$ *for all* $1 \leq i \leq \ell(\mathfrak{p})$ *and all* $\mathfrak{p}$*,*
- *the class* $\{\mathfrak{a}\}$ *of* $\mathfrak{a}$ *in the ideal class group* $\mathrm{Cl}(\mathcal{O})$*.*

(That is, a module N *is isomorphic to* M *if and only if the set of integers and the ideal class attached to* N *are the same as those for* M*.)*

In particular, the torsion part of M *is determined up to isomorphism by its set of elementary divisors*

$$\{\mathfrak{p}^{\delta(\mathfrak{p},1)},\ldots,\mathfrak{p}^{\delta(\mathfrak{p},\ell(\mathfrak{p}))} \mid \mathfrak{p} \in \mathbf{P}\}.$$

Proof

Assertion (i) follows by (6.3.4) and (6.3.5). For (ii), see (6.1.7), and (iii) is in (6.3.15), noting that here $T(\mathfrak{p}) = T_{\mathfrak{p}}(T)$. Statement (iv) is given in (6.3.20).

The claim about isomorphism follows from (6.3.20) again, combined with Steinitz' Theorem (6.1.6), using the discussion of homomorphisms above. □

Finally, it is useful to have a reinterpretation of the above result when $\mathcal{O}$ is a (commutative) principal ideal domain. In this case, any projective module is free, and it is more usual to describe torsion modules in terms of their p-primary components (6.3.17), where p runs through a representative set **Pe** of irreducible elements of $\mathcal{O}$, that is, **Pe** has exactly one member p for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$. We also regard the elementary divisors of a module as powers of irreducible elements rather than ideals.

The next result is an immediate translation of its predecessor into the changed vocabulary.

6.3.24 Theorem

Let M *be a finitely generated module over a commutative principal ideal domain* $\mathcal{O}$*. Then the following assertions hold.*

(i) $M = F \oplus T$ *where* $F \cong \mathcal{O}^r$ *is a finitely generated free* $\mathcal{O}$*-module and* T *is a finitely generated torsion* $\mathcal{O}$*-module.*

(ii) $T \cong \bigoplus_p T(p)$*, where* $p \in \mathbf{Pe}$*, each* $T(p)$ *is a finitely generated* p*-primary* $\mathcal{O}$*-module, and* $T(p) = 0$ *for almost all* p*.*

(iii) *If* $T(p) \neq 0$*, then*

$$T(p) \cong \mathcal{O}/p^{\delta(p,1)}\mathcal{O} \oplus \cdots \oplus \mathcal{O}/p^{\delta(p,\ell(p))}\mathcal{O},$$

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

where $0 < \delta(p,1) \leq \cdots \leq \delta(p,\ell(p))$ *(and if* $T(p) = 0$, $\ell(p) = 0$*).*

Furthermore, the module M *determines, and in turn is determined to within isomorphism by, the following information:*

- *the integer* $r = \operatorname{rank}(M)$,
- *the integers* $\ell(p)$ *for all* p *in* $\mathbf{Pe}$,
- *the integers* $\delta(p,i)$ *for all* i *with* $1 \leq i \leq \ell(p)$ *and all* p *in* $\mathbf{Pe}$.

In particular, the torsion part of M *is determined up to isomorphism by its set of elementary divisors*

$$\{p^{\delta(p,1)}, \ldots, p^{\delta(p,\ell(p))} \mid p \in \mathbf{Pe}\}. \qquad \square$$

Exercises

In these exercises, the ring $\mathcal{O}$ is a Dedekind domain. For a pair of (right) $\mathcal{O}$-modules M and N we abbreviate $\operatorname{Hom}_{\mathcal{O}}(M,N)$ to $\operatorname{Hom}(M,N)$.

6.3.1 Suppose that $\mathcal{O}$ has infinitely many distinct prime ideals, and put $M = \bigoplus_{\mathfrak{p}} (\mathcal{O}/\mathfrak{p})$. Show that M is a torsion module, but $\operatorname{Ann}(M) = 0$.

Let $N = \bigoplus_{i>0} (\mathcal{O}/\mathfrak{p}^i)$ for any fixed $\mathfrak{p}$. Show that $\operatorname{Ann}(N) = 0$ but that any finitely generated submodule of N is $\mathfrak{p}$-primary.

(This shows the significance of restricting our attention to finitely generated modules, particularly in (6.3.7).)

6.3.2 We can extend the definition of $\mathfrak{p}$-primary to $\mathcal{O}$-modules which are not finitely generated by saying that an $\mathcal{O}$-module M is $\mathfrak{p}$-primary provided that all its finitely generated submodules are $\mathfrak{p}$-primary.

Using Zorn's Lemma, show that any $\mathcal{O}$-module has a maximal $\mathfrak{p}$-primary submodule.

Verify that parts (ii) and (iii) of (6.3.15) continue to hold for non-finitely-generated modules.

6.3.3 Find the composition series of $\mathcal{O}/\mathfrak{p}^\delta$. Hence find the composition factors of an arbitrary $\mathfrak{p}$-primary module M, and find a formula for the length of a composition series for M in terms of its elementary divisor type.

Extend the result to arbitrary finitely generated torsion modules.

6.3.4 Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$. Find the primary decomposition of $\mathcal{O}/\mathfrak{a}$.

Suppose that $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are ideals of $\mathcal{O}$ with $\mathfrak{a}_1 | \cdots | \mathfrak{a}_r$, and let $M = \mathcal{O}/\mathfrak{a}_1 \oplus \cdots \oplus \mathcal{O}/\mathfrak{a}_r$ (the external direct sum). Describe the primary decomposition of M and its elementary divisor type.

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press

6.3.5 **Uniqueness of invariant factors**

Let $\mathcal{O}$ be a (commutative) Euclidean domain, in particular, a polynomial ring $K[T]$, and let M be a finitely generated $\mathcal{O}$-module. By (3.3.6),

$$M \cong \mathcal{O}/e_1\mathcal{O} \oplus \cdots \oplus \mathcal{O}/e_\ell\mathcal{O} \oplus \mathcal{O}^s,$$

where $e_1 \mid e_2 \mid \cdots \mid e_\ell$ are the invariant factors of M.

Identify $T(M)$ and $M/T(M)$, and, using Exercise 6.3.4 above, show that the ideals $e_1\mathcal{O}, \ldots, e_\ell\mathcal{O}$ are unique. Deduce that the invariant factors of M are unique up to multiplication by units.

6.3.6 **Invariant Factor Theorem for Dedekind Domains**

Let $\mathcal{O}$ be an arbitrary Dedekind domain, and let M be a finitely generated torsion module over $\mathcal{O}$. Using the primary decomposition of M, show that there are ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell$ of $\mathcal{O}$ with $\mathfrak{a}_1 | \cdots | \mathfrak{a}_\ell$ and $M \cong \mathcal{O}/\mathfrak{a}_1 \oplus \cdots \oplus \mathcal{O}/\mathfrak{a}_\ell$.

Deduce that if K is a submodule of a free $\mathcal{O}$-module $\mathcal{O}^n$, then there is a basis $(f_1, \ldots, f_n)$ of $\mathcal{O}^n$ such that $K = \mathfrak{a}_1 f_1 \oplus \cdots \oplus \mathfrak{a}_\ell f_\ell$.

(For a direct proof, see [Curtis & Reiner 1966], 22.12.)

6.3.7 Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of $\mathcal{O}$. Show that there is an exact sequence

$$0 \longrightarrow \mathrm{Hom}(\mathfrak{a}, \mathfrak{b}) \longrightarrow \mathrm{Hom}(\mathfrak{a}, \mathcal{O}) \longrightarrow \mathrm{Hom}(\mathfrak{a}, \mathcal{O}/\mathfrak{b}) \longrightarrow 0,$$

and deduce that

$$\mathrm{Hom}(\mathfrak{a}, \mathcal{O}/\mathfrak{b}) \cong \mathfrak{a}^{-1}/\mathfrak{a}^{-1}\mathfrak{b} \cong \mathcal{O}/\mathfrak{b}.$$

Hints. (6.1.1), (5.1.24) and Exercise 5.1.8.

6.3.8 Let M and N be (right) $\mathcal{O}$-modules. Show that

(i) $\mathrm{Hom}(M, N) = 0$ if $\mathrm{Ann}(M)$ and $\mathrm{Ann}(N)$ are coprime,

(ii) $\mathrm{Hom}(M, N) = 0$ if M is a torsion module and N is torsion-free.

6.3.9 Let M and N be finitely generated (right) $\mathcal{O}$-modules, and choose internal direct sum decompositions $M = T(M) \oplus M'$ and $N = T(N) \oplus N'$, so that $M' \cong M/T(M)$, etc.

Show that

$$\mathrm{Hom}(M, N) \cong \begin{pmatrix} \mathrm{Hom}(T(M), T(N)) & \mathrm{Hom}(M', T(N)) \\ 0 & \mathrm{Hom}(M', N') \end{pmatrix},$$

where the matrices act as left multipliers on the 'column' M – Exercises 2.1.6 and 2.1.7 are relevant.

Confirm that $\mathrm{End}(M)$ is a triangular ring of matrices.

Compute $\mathrm{Hom}(\mathcal{O}/\mathfrak{p} \oplus \mathcal{O}, \mathcal{O}/\mathfrak{q} \oplus \mathcal{O})$, where $\mathfrak{p}, \mathfrak{q}$ are prime ideals of $\mathcal{O}$, possibly the same.

Remark. The term $\mathrm{Hom}(M', N')$ is known, by Exercise 6.1.4, and $\mathrm{Hom}(M', T(N))$ is computable by Exercise 6.3.7 above. As noted in (6.3.18), an element λ in $\mathrm{Hom}(T(M), T(N))$ can be represented as a sequence $(\lambda_{\mathfrak{p}})$, where each $\lambda_{\mathfrak{p}}$ is in in $\mathrm{Hom}(T_{\mathfrak{p}}(M), T_{\mathfrak{p}}(N))$. The next exercise gives $\lambda_{\mathfrak{p}}$.

6.3.10 Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. Show that

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}^r, \mathcal{O}/\mathfrak{p}^s) = \{x \in \mathcal{O}/\mathfrak{p}^s \mid \mathfrak{p}^r x = 0\} \cong \begin{cases} \mathcal{O}/\mathfrak{p}^s & r \geq s, \\ \mathcal{O}/\mathfrak{p}^r & r < s. \end{cases}$$

Let $M = \mathcal{O}/\mathfrak{p}^{\delta(1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta(k)}$ and $N = \mathcal{O}/\mathfrak{p}^{\epsilon(1)} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\epsilon(\ell)}$ be $\mathfrak{p}$-primary modules. Describe $\mathrm{Hom}(M, N)$ as a set of $\ell \times k$ matrices.

https://doi.org/10.1017/9780511608674.007 Published online by Cambridge University Press