7

LOCAL-GLOBAL METHODS

Let $\mathcal{O}$ be a Dedekind domain. A difficult but important problem is the determination of the structure of modules over an $\mathcal{O}$-order R; this problem arises in various contexts in algebraic number theory, integral representation theory and algebraic geometry. An initial attempt at the problem is suggested by the observation that the localizations $\mathcal{O}_{\mathfrak{p}}$ of $\mathcal{O}$ at its nonzero prime ideals are all local rings, whose modules have a relatively straightforward structure. The structure of modules over the localizations $R_{\mathfrak{p}}$ might be correspondingly straightforward, and we could then hope to obtain information about an R-module from our knowledge of its localizations. Techniques of this nature are called *local-global* methods.

In this chapter, we show that our attempt works reasonably well for the projective modules over an order. However, we need to work with the completions of a Dedekind domain rather than its localizations, since we can then deploy arguments that are based on convergence. Completions are discussed in the first section of the chapter. We then show that the projective modules over a complete order $\widehat{R}$ can be obtained by lifting the projective modules from an Artinian semisimple ring, namely $\widehat{R}/\operatorname{rad}(\widehat{R})$ where $\operatorname{rad}(\widehat{R})$ is the Jacobson radical of $\widehat{R}$. Thus, if we are given an explicit complete order, we have a good chance of determining its projective modules. (Some computations with tiled orders are indicated in the exercises.) In the final section, we investigate the relationship between the local and global structure of modules over orders; in particular, we show that a module is globally projective if and only if it is always locally projective.

However, the methods used here cannot give full information about the global structure of projective modules, even for the Dedekind domain itself. By Steinitz' Theorem (2.3.20 – D), the structure of projective $\mathcal{O}$-modules is governed by the ideal class group, which cannot be detected locally, since every localization or completion of $\mathcal{O}$ is a principal ideal domain and therefore has

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

trivial ideal class group. The tools for the repair of this failing are provided by algebraic K-theory.

As usual, we concentrate on right modules, it being clear that there is a parallel theory for left modules.

7.1 THE COMPLETION OF A DEDEKIND DOMAIN

The key step in our discussion of local-global methods is the construction of the $\mathfrak{p}$-adic completion $\widehat{\mathcal{O}}_{\mathfrak{p}}$ of a Dedekind domain $\mathcal{O}$ at each of its nonzero prime ideals $\mathfrak{p}$. The ring $\widehat{\mathcal{O}}_{\mathfrak{p}}$ is a local Dedekind domain, so its module theory is known. It is also complete in a sense to be made precise below (7.1.10), a property which is inherited by $\widehat{\mathcal{O}}_{\mathfrak{p}}$-modules and, in particular, by $\widehat{\mathcal{O}}_{\mathfrak{p}}$-orders. This observation is exploited in the remaining sections of this text to describe the projective modules over $\widehat{\mathcal{O}}_{\mathfrak{p}}$-orders and to relate the modules over an $\mathcal{O}$-order to the modules over its associated $\widehat{\mathcal{O}}_{\mathfrak{p}}$-orders.

We start with a preliminary resumé of the properties of valuation rings, and then give the construction of completions, first for a Dedekind domain $\mathcal{O}$, and then for $\mathcal{O}$-modules. We show how all the completions can be considered simultaneously by using the adèle ring $A(\mathcal{O})$ of $\mathcal{O}$ (7.1.25), and we establish some further basic results which relate the structure of an $\mathcal{O}$-module to its completions.

The definitions and arguments that we give here are purely algebraic, although they originate in the theory of metric spaces. They apply to much wider classes of ring than Dedekind domains, but at the expense of considerable technical complications which we sidestep by exploiting the strong structure theory of ideals and modules over a Dedekind domain. (Some further results are indicated in the remark and the exercises at the end of the section.)

7.1.1 Valuations

Given a field $\mathcal{K}$, a *valuation* on $\mathcal{K}$ is any function

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

that satisfies the following conditions.

Let $x, y \in \mathcal{K}$.

V1. $v(x) = \infty$ if and only if $x = 0$.
V2. $v(x + y) \geq \min(v(x), v(y))$.
V3. $v(xy) = v(x) + v(y)$.

V4. $v(p) = 1$ for some $p \in \mathcal{K}$.

The last requirement ensures that we avoid trivialities. Any such element p is called a *uniformizing parameter* (or *uniformizer* or *prime element*) for the valuation v.

Here are the elementary properties of valuations.

7.1.2 Lemma

Let v be a valuation on a field $\mathcal{K}$. Then the following hold.

(i) $v(1) = 0$;
(ii) $v(x^{-1}) = -v(x)$, $x \neq 0$;
(iii) $v(-1) = 0$;
(iv) $v(-x) = v(x)$;
(v) *if* $v(x) > v(y)$, *then* $v(x+y) = v(y)$.

Proof

Only (v) needs a little work. We know from V2 that $v(x+y) \geq v(y)$. By (iv) and V2,

$$v(y) = v(-x + (x+y)) \geq \min(v(x), v(x+y));$$

since $v(y) < v(x)$, this leaves $v(y) \geq v(x+y)$. □

A valuation v on the field $\mathcal{K}$ gives rise to a *valuation ring* $\mathcal{V}$, defined as

$$\mathcal{V} = \{x \in \mathcal{K} \mid v(x) \geq 0\}.$$

It is easily verified that $\mathcal{V}$ is indeed a subring of $\mathcal{K}$. The basic properties of $\mathcal{V}$ are described by the next, straightforward, result.

7.1.3 Lemma

(i) *Let $x, y \in \mathcal{V}$ be nonzero. Then $x \mid y$ in $\mathcal{V}$ if and only if $v(x) \leq v(y)$.*
(ii) *Let $x \in \mathcal{K}$, $x \neq 0$. Then either x or x^{-1} is in $\mathcal{V}$.*
(iii) *The group of units in $\mathcal{V}$ is*

$$U(\mathcal{V}) = \{x \in \mathcal{K} \mid v(x) = 0\}.$$

(iv) *$\mathcal{V}$ is a local ring with maximal ideal*

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

(v) *$\mathfrak{m}$ is principal, generated by any uniformizing parameter p (that is, $v(p) = 1$).*

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

(vi) *The fractional $\mathcal{V}$-ideals in $\mathcal{K}$ are the powers*

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

(vii) *$\mathcal{V}$ is a principal ideal domain.* □

7.1.4 Valuations and Dedekind domains

Our main interest is in the valuations that are associated with the nonzero prime ideals of a Dedekind domain. The definition and properties of such valuations are developed in detail in section 6.2 of [BK: IRM]; here, we make a quick review of the salient facts.

Let $\mathcal{O}$ be a Dedekind domain and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. For each nonzero element x of the field of fractions $\mathcal{K}$ of $\mathcal{O}$, we have ([BK: IRM] (6.2.1))

$$x\mathcal{O} = \mathfrak{p}^{v(x)}\mathfrak{b}$$

where $v(x)$ is an integer uniquely determined by x and $\mathfrak{b}$ is a fractional ideal whose prime factorization does not involve any nonzero power of $\mathfrak{p}$.

The function v is easily seen to be a valuation on $\mathcal{K}$, the $\mathfrak{p}$-*adic valuation.* If we need to indicate the prime, we write $v_{\mathfrak{p}}$. It is also straightforward to verify that the corresponding valuation ring is the localization $\mathcal{O}_{\mathfrak{p}}$ of $\mathcal{O}$ at $\mathfrak{p}$ ([BK: IRM] (6.2.6)).

We can now give a characterization of valuation rings.

7.1.5 Theorem

For a commutative domain $\mathcal{V}$ the following statements are equivalent.

(i) *$\mathcal{V}$ is a valuation ring.*

(ii) *$\mathcal{V}$ is a local principal ideal domain which is not a field.*

(iii) *$\mathcal{V}$ is the localization of a Dedekind domain at a nonzero prime ideal.*

Proof

(i) ⇒ (ii) Combine (iv) and (vii) of the lemma above.

(ii) ⇒ (iii) By the definition (2.3.20), every principal ideal domain is a Dedekind domain, while by (6.1.14) any local ring is its own localization at its maximal ideal.

(iii) ⇒ (i) This was observed above. □

It will be convenient to record here the structure theorem for modules over a valuation ring – see ([BK: IRM] (6.2.12) and (6.2.13)). For compatibility with future references, from now on we use $\mathcal{O}$ rather than $\mathcal{V}$ for the valuation ring.

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

7.1.6 Theorem

Let $\mathcal{O}$ be a valuation ring with unique maximal ideal $\mathfrak{p}$ and let M be a finitely generated (right) $\mathcal{O}$-module.

Then

$$M \cong \mathcal{O}/\mathfrak{p}^{\delta_1} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}^{\delta_\ell} \oplus \mathcal{O}^s$$

where $\delta_1 \leq \cdots \leq \delta_\ell$ are the invariant factors *of M and s is the* rank *of M.*

The collection of integers $\delta_1, \ldots, \delta_\ell$ together with ℓ and s are uniquely determined by M and determine M up to isomorphism. □

7.1.7 Generalizations

(i) A valuation ring $\mathcal{V}$ as defined in this text is more properly called a *discrete rank one valuation ring*, since it arises from a discrete valuation v on the field of fractions $\mathcal{K}$ of $\mathcal{V}$, and takes values in the rank one group $\mathbb{Z}$. In view of (ii) of the preceding theorem, $\mathcal{V}$ is sometimes alternatively named a *principal valuation ring.* A discussion of the rings associated with valuations in general can be found in [Cohn 1991].

(ii) A Dedekind domain $\mathcal{O}$ is the intersection $\mathcal{O} = \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$ of its localizations $\mathcal{O}_{\mathfrak{p}}$ at its nonzero prime ideals ([BK: IRM] (6.2.7)); by (7.1.5), each such localization is a valuation ring. Also, the Unique Factorization Theorem for ideals in a Dedekind domain ([BK: IRM] (5.1.19)) tells us that any nonzero element of $\mathcal{O}$ is contained in only finitely many prime ideals. This description of a Dedekind domain provides a characterization of an important class of ring.

A *Krull domain* is a commutative domain $\mathcal{O}$ with $\mathcal{O} = \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$, each ring of fractions $\mathcal{O}_{\mathfrak{p}}$ being a (discrete rank one) valuation ring arising from a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, and each element of $\mathcal{O}$ being contained in only finitely many prime ideals of $\mathcal{O}$. Thus we have shown that every Dedekind domain is a Krull domain.

Such rings occur frequently in algebraic geometry; the archetype is the polynomial ring $\mathcal{F}[X_1, \ldots, X_n]$ over a field $\mathcal{F}$. Many of the properties of Dedekind domains can be extended to Krull domains; for an algebraic investigation of this topic, see [Fossum 1973].

7.1.8 Cauchy sequences

We now give our algebraic formulation of the notions of convergence and completeness. Since this works in any commutative ring, we temporarily consider the general situation of a commutative ring R with ideal $\mathfrak{a}$.

A sequence (r_i), with $r_i \in R$, $i = 1, 2, \ldots$ is an $\mathfrak{a}$-*adic Cauchy sequence* if the following condition is satisfied.

CS. Given any natural number $n > 0$, there is a natural number $k = k(n)$ such that $r_i - r_j \in \mathfrak{a}^n$ whenever $i, j \geq k$.

When $\mathfrak{a} = p\mathcal{O}$ is principal, we speak of a p-adic Cauchy sequence instead.

For example, let p be a prime number, and define

$$r_i = 1 + p + \cdots + p^i \text{ for } i > 0.$$

Then the sequence (r_i) is a p-adic Cauchy sequence in the ring of integers $\mathbb{Z}$.

We say that the Cauchy sequence (r_i) is *convergent* to an element r in R if, given any $n > 0$, there is a $k = k(n)$ such that

$$r_i - r \in \mathfrak{a}^n \text{ whenever } i \geq k.$$

Naturally, r is called the *limit* of the sequence. It is obvious from our example that a Cauchy sequence need not have a limit.

The following result is easily proved; part (b) uses the fact that $\bigcap_{i=0}^{\infty} \mathfrak{p}^i = 0$ for a prime ideal of a Dedekind domain, which follows from the Unique Factorization Theorem for ideals (2.3.20 - A).

7.1.9 Lemma

Let $\mathfrak{a}$ be an ideal of a commutative ring R. Then the following hold.

(a) *Let (r_i) and (s_i) be $\mathfrak{a}$-adic Cauchy sequences. Then $(r_i + s_i)$ and $(r_i s_i)$ are also Cauchy sequences.*

(b) *Suppose that $\bigcap_{i=0}^{\infty} \mathfrak{a}^i = 0$. Then the limit of an $\mathfrak{a}$-adic Cauchy sequence is unique if it exists.*
In particular, if $\mathfrak{p}$ is a nonzero prime ideal of a Dedekind domain $\mathcal{O}$, any convergent $\mathfrak{p}$-adic Cauchy sequence in $\mathcal{O}$ has a unique limit.

(c) *Suppose that $\mathfrak{a}$-adic Cauchy sequences (r_i) and (s_i) have limits r and s respectively. Then $(r_i + s_i)$ has limit $r + s$ and $(r_i s_i)$ has limit rs.* □

7.1.10 Completeness

We now specialize to the case that the ring is a Dedekind domain $\mathcal{O}$ and the ideal is a nonzero prime ideal $\mathfrak{p}$.

We say that $\mathcal{O}$ is $\mathfrak{p}$-*adically complete* if every $\mathfrak{p}$-adic Cauchy sequence in $\mathcal{O}$ also has a limit in $\mathcal{O}$. Evidently, the ring $\mathbb{Z}$ is not p-adically complete for any prime number p.

The problem then is, given $\mathcal{O}$ and $\mathfrak{p}$, to construct in some canonical way a

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

complete ring $\widehat{\mathcal{O}}$ that contains limits of all $\mathfrak{p}$-adic Cauchy sequences from $\mathcal{O}$. Thus, in the p-adic example above, the p-adic completion of $\mathbb{Z}$ should contain an element representing $\sum_{i=0}^{\infty} p^i$.

Before beginning the construction, we give an elementary result that shows that a complete Dedekind domain is already local.

7.1.11 Lemma

Suppose that a Dedekind domain $\mathcal{O}$ is $\mathfrak{p}$-adically complete for some nonzero prime ideal $\mathfrak{p}$.

Then

(i) $\mathcal{O} = \mathcal{O}_{\mathfrak{p}}$,

(ii) $\mathfrak{p}$ *is the only nonzero prime ideal in* $\mathcal{O}$.

Proof

It is clear that (ii) follows from (i) because nonzero prime ideals are maximal in a Dedekind domain. To establish (i), we need to show that every element of $\mathcal{O} \setminus \mathfrak{p}$ is invertible.

First consider an element $1 - r \in 1 + \mathfrak{p}$. Put

$$s_n = 1 + r + \cdots + r^n \text{ for each } n \geq 1;$$

then (s_n) is a Cauchy sequence, and it is easily seen from the preceding lemma (7.1.9) that its limit s is the inverse of $1 - r$.

Next, suppose that x is not in $\mathfrak{p}$. Since the image of x is invertible in the field $\mathcal{O}/\mathfrak{p}$, there is some t in $\mathcal{O}$ such that $xt \in 1 + \mathfrak{p}$. Thus xt and hence x can be inverted in $\mathcal{O}$. □

7.1.12 Constructing the completion

We now give the construction of the $\mathfrak{p}$-adic completion of the Dedekind domain $\mathcal{O}$. The p-adic completions of the integers were introduced in [Hensel 1908], essentially in a power series form that we reveal in (7.1.19). The theory was then clarified by the use of valuation theory ([Kürschák 1913], [Ostrowski 1917]) and extended to arbitrary Dedekind domains. The language of inverse limits now permits us to make a very smooth definition in terms of successive approximation, which is implicit in Hensel's work.

For each $i \geq 0$, let

$$\pi_i : \mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}^i \text{ and } \rho_i : \mathcal{O}/\mathfrak{p}^{i+1} \longrightarrow \mathcal{O}/\mathfrak{p}^i$$

be the canonical ring homomorphisms, all of which are surjective. Note that $\rho_i \pi_{i+1} = \pi_i$ for all i.

The collection $\{\mathcal{O}/\mathfrak{p}^i, \rho_i \mid i \geq 0\}$ then defines an inverse system of rings, and of (right) $\mathcal{O}$-modules, by taking the homomorphism from $\mathcal{O}/\mathfrak{p}^j$ to $\mathcal{O}/\mathfrak{p}^i$ to be the product $\rho_i \cdots \rho_{j-1}$ when $i < j$ (see (5.3.1), where ρ_i is denoted by ${}_{i,i+1}\psi$).

The $\mathfrak{p}$-*adic completion* $\widehat{\mathcal{O}}$ or $\widehat{\mathcal{O}}_\mathfrak{p}$ of $\mathcal{O}$ is defined to be the inverse limit of this system:

$$\widehat{\mathcal{O}} = \{(x_i) \mid x_i \in \mathcal{O}/\mathfrak{p}^i \text{ and } \rho_i x_{i+1} = x_i \text{ for all } i\}.$$

It is easy to verify that the operations

$$(x_i) + (y_i) = (x_i + y_i) \text{ and } (x_i) \cdot (y_i) = (x_i \cdot y_i)$$

make $\widehat{\mathcal{O}}$ into a commutative ring; $\widehat{\mathcal{O}}$ is also an $\mathcal{O}$-module by the rule

$$(x_i) \cdot r = (x_i \cdot \pi_i r).$$

There is a natural ring homomorphism π from $\mathcal{O}$ to $\widehat{\mathcal{O}}$, given by

$$\pi m = (\pi_i m),$$

which is injective since

$$\operatorname{Ker} \pi = \bigcap_{i=0}^{\infty} \mathfrak{p}^i = 0.$$

Thus we may regard $\mathcal{O}$ as a subring of $\widehat{\mathcal{O}}$. Note also that there are canonical ring homomorphisms

$$\widehat{\pi}_i : \widehat{\mathcal{O}} \longrightarrow \mathcal{O}/\mathfrak{p}^i \text{ for } i \geq 1,$$

given by projecting to the ith term, and that $\widehat{\pi}_i \pi = \pi_i$ for each i.

The sense in which $\widehat{\mathcal{O}}$ is to be regarded as 'complete' will be explained after we have shown that it is a valuation ring.

7.1.13 Extending the valuation

Suppose that $\mathcal{O}$ is a valuation ring with maximal ideal $\mathfrak{p} = p\mathcal{O}$ and quotient field $\mathcal{K}$. Then, since $\mathcal{O}$ is also a Dedekind domain, we can form its p-adic completion $\widehat{\mathcal{O}}$. Regarding $\mathcal{O}$ as a subring of $\widehat{\mathcal{O}}$, we can extend the p-adic valuation v to $\widehat{\mathcal{O}}$ as follows. Given an element $x = (x_i)$ of $\widehat{\mathcal{O}}$, define

$$\widehat{v}(x) = \max\{i \mid x_i = 0\} \text{ if } x \neq 0$$

and

$$\widehat{v}(0) = \infty.$$

Thus $\widehat{v}(x) = 0$ if and only if $x_1 \neq 0$, that is, $\widehat{\pi}_1(x) \neq 0$ in $\mathcal{O}/\mathfrak{p}$. Clearly, $\widehat{v} : \widehat{\mathcal{O}} \to \mathbb{Z} \cup \{\infty\}$ is a function that coincides with v on $\mathcal{O}$.

7.1.14 Theorem

Let $\mathcal{O}$ be a valuation ring with maximal ideal $\mathfrak{p} = p\mathcal{O}$ and field of fractions $\mathcal{K}$, and let $\widehat{\mathcal{O}}$ be the p-adic completion of $\mathcal{O}$.

Then the following assertions hold.

(i) *If $x \in \widehat{\mathcal{O}}$ is nonzero and $\widehat{v}(x) = h$, then $x = p^h y$ where $y \in \widehat{\mathcal{O}}$ and $\widehat{v}(y) = 0$.*

(ii) *$\widehat{\mathcal{O}}$ is a commutative domain, (and so its field of fractions, denoted $\widehat{\mathcal{K}}$, exists).*

(iii) *The function $\widehat{v}$ extends to a valuation on $\widehat{\mathcal{K}}$, and $\widehat{\mathcal{O}}$ is then the valuation ring of $\widehat{v}$.*

(iv) *The unique maximal ideal of $\widehat{\mathcal{O}}$ is $\mathfrak{p}\widehat{\mathcal{O}} = p\widehat{\mathcal{O}}$. In particular, a uniformizing parameter for $\mathcal{O}$ is also a uniformizing parameter for $\widehat{\mathcal{O}}$.*

(v) *$\widehat{\mathcal{O}}/(\mathfrak{p}\widehat{\mathcal{O}})^h \cong \mathcal{O}/\mathfrak{p}^h$ for all $h > 0$, both as rings and as $\mathcal{O}$-modules.*

(vi) *$\widehat{\mathcal{K}} = \widehat{\mathcal{O}}\mathcal{K}$; more particularly, any element of $\widehat{\mathcal{K}}$ can be written in the form $p^{-h}w$, where $h \geq 0$ and $w \in \widehat{\mathcal{O}}$.*

(vii) *The fractional ideals of $\widehat{\mathcal{O}}$ have the form $p^h\widehat{\mathcal{O}}$ where $h \in \mathbb{Z}$.*

(viii) *$\mathcal{O} = \widehat{\mathcal{O}} \cap \mathcal{K}$.*

Proof

(i) Let $x = (x_i)$. For each i, write $x_i = \pi_i r_i$ with $r_i \in \mathcal{O}$. By hypothesis, $r_i \in p^h\mathcal{O} \setminus \mathfrak{p}^{h+1}$ whenever $i \geq h$. Since $\mathcal{O}$ is a valuation ring, we can define elements $s_{i-h} = p^{-h}r_i$ in $\mathcal{O}$ and thus an element $y = (\pi_{i-h}s_{i-h})_{i \geq h}$ of $\widehat{\mathcal{O}}$. By construction, $\widehat{v}(y) = 0$, and clearly $x = p^h y$.

(ii) Suppose that $x = (x_i)$ and $y = (y_i)$ in $\widehat{\mathcal{O}}$ are nonzero but $xy = 0$. By (i), we may assume that $\widehat{v}(x) = \widehat{v}(y) = 0$. Then $x_1 y_1 = 0$ in the field $\mathcal{O}/p\mathcal{O}$, a contradiction.

(iii) The preceding remarks show that

$$\widehat{v}(x + y) \geq \max(\widehat{v}(x), \widehat{v}(y))$$

and that

$$\widehat{v}(xy) = \widehat{v}(x) + \widehat{v}(y)$$

for elements x, y in $\widehat{\mathcal{O}}$; further, $\widehat{v}(p) = 1$. Extend $\widehat{v}$ to $\widehat{\mathcal{K}}$ by setting

$$\widehat{v}(x/y) = \widehat{v}(x) - \widehat{v}(y).$$

(iv) This follows since $\widehat{v}(p) = 1$.

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

(v) The canonical surjection $\widehat{\pi}_h : \widehat{\mathcal{O}} \to \mathcal{O}/\mathfrak{p}^h$ can now be seen to induce an isomorphism from $\widehat{\mathcal{O}}/\mathfrak{p}^h\widehat{\mathcal{O}}$ to $\mathcal{O}/\mathfrak{p}^h$.
(vi), (vii) These follow from (i), since, by (iii), the equation $\widehat{v}(y) = 0$ makes y a unit of $\widehat{\mathcal{O}}$.
(viii) Clear. □

Since $\widehat{\mathcal{O}}$ is again a Dedekind domain (part (iii) of the above theorem), we may iterate the completion procedure, with the following consequence.

7.1.15 Corollary

The inclusion homomorphisms

$$\mathcal{O} \longrightarrow \mathcal{O}_\mathfrak{p} \longrightarrow \widehat{\mathcal{O}}_\mathfrak{p}$$

induce isomorphisms of inverse systems of rings

$$\{\mathcal{O}/\mathfrak{p}^i \mid i \geq 1\} \cong \{\mathcal{O}_\mathfrak{p}/\mathfrak{p}^i\mathcal{O}_\mathfrak{p} \mid i \geq 1\} \cong \{\widehat{\mathcal{O}}_\mathfrak{p}/\mathfrak{p}^i\widehat{\mathcal{O}}_\mathfrak{p} \mid i \geq 1\}$$

and hence isomorphisms of the completion rings

$$\widehat{\mathcal{O}}_\mathfrak{p} \xrightarrow{\cong} \widehat{(\mathcal{O}_\mathfrak{p})} \xrightarrow{\cong} \widehat{(\widehat{\mathcal{O}}_\mathfrak{p})}\,.$$

Proof

Clearly, from the construction of $\mathcal{O}_\mathfrak{p}$ as a direct limit, the inclusion of $\mathcal{O}$ in $\mathcal{O}_\mathfrak{p}$ induces an injective homomorphism from $\mathcal{O}/\mathfrak{p}^i$ to $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^i\mathcal{O}_\mathfrak{p}$. To see that this map is also a surjection, consider any element $b \in \mathcal{O} \setminus \mathfrak{p}$. By (2.3.20 – A), each ideal of $\mathcal{O}$ has a unique factorization into prime ideals. Any prime ideal $\mathfrak{q}$ that contains the ideal $b\mathcal{O} + \mathfrak{p}^i$ must contain both b and $\mathfrak{p}^i$ and hence both b and $\mathfrak{p}$, which shows that $b\mathcal{O} + \mathfrak{p}^i$ is $\mathcal{O}$. Thus b has an inverse c modulo $\mathfrak{p}^i$, and hence the residue class $\overline{1/b}$ in $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^i\mathcal{O}_\mathfrak{p}$ is the image of $\overline{c}$.

Since $\mathcal{O}_\mathfrak{p}$ is a valuation ring, the isomorphism $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^i\mathcal{O}_\mathfrak{p} \cong \widehat{\mathcal{O}}_\mathfrak{p}/\mathfrak{p}^i\widehat{\mathcal{O}}_\mathfrak{p}$ is just part (v) of (7.1.14) above. It is clear that these isomorphisms are compatible with the homomorphisms implicit in the inverse systems. Thus we obtain isomorphisms of inverse systems and hence of their inverse limits. □

We can now justify the use of the term 'completion'. This is most easily done by characterizing completion in terms of its universal property.

7.1.16 Theorem

Let $\mathfrak{p}$ be a prime ideal of a Dedekind domain $\mathcal{O}$ and let $\widehat{\mathcal{O}}$ be the $\mathfrak{p}$-adic completion of $\mathcal{O}$. Then $\widehat{\mathcal{O}}$ has the following universal property.

(a) *Every $\mathfrak{p}\widehat{\mathcal{O}}$-adic Cauchy sequence in $\widehat{\mathcal{O}}$ has a unique limit; in other words, $\widehat{\mathcal{O}}$ is $\mathfrak{p}\widehat{\mathcal{O}}$-adically complete.*

(b) *Let R be a commutative ring, let $f : \mathcal{O} \to R$ be a ring homomorphism, and suppose that every $f(\mathfrak{p})R$-adic Cauchy sequence in R has a unique limit in R. Then f extends uniquely to a ring homomorphism $\widehat{f} : \widehat{\mathcal{O}} \to R$.*

Proof

(a) Let $c = (c_i)$ be a $\mathfrak{p}\widehat{\mathcal{O}}$-adic Cauchy sequence in $\widehat{\mathcal{O}}$. Thus, given $n > 0$, there is some k such that $c_i - c_j$ is in $\mathfrak{p}^n\widehat{\mathcal{O}}$ for $i > j \geq k$. By (v) of (7.1.14), we can write $c_i = (c_{ui})$ with

$$c_{ui} \in \widehat{\mathcal{O}}/\mathfrak{p}^u\widehat{\mathcal{O}}, \quad \text{where } \rho_u c_{u+1,i} = c_{ui} \text{ for } u \geq 0.$$

Then we must have $c_{ui} = c_{uj}$ provided $i > j \geq k$ and $u \leq n$, which means that for $i \geq k$ the term $c'_n = c_{ni}$ is independent of i. The element $c' = (c'_n)$ in $\widehat{\mathcal{O}}$ is the limit of the Cauchy sequence.

(b) Let $x \in \widehat{\mathcal{O}}$. By definition (7.1.12), $x = (x_i)$ is given by a coherent system of residues $x_i \in \mathcal{O}/\mathfrak{p}^i$, so we may write $x = (\pi_i r_i)$ for elements $r_i \in \mathcal{O}$ which form a $\mathfrak{p}$-adic Cauchy sequence (r_i) in $\mathcal{O}$. The image (fr_i) is an $f(\mathfrak{p})$-adic Cauchy sequence in R, thus we may define $\widehat{f}(x)$ to be the (unique) limit of this sequence.

We need to show that $\widehat{f}$ is well defined. If $x = (\pi_i r'_i)$ for some alternative choice of elements r'_i in $\mathcal{O}$, then, for each i, $r_i - r'_i \in \mathfrak{p}^i$ and so $f(r_i) - f(r'_i) \in (f(\mathfrak{p}))^i$, which means that the sequences $(f(r_i))$ and $(f(r'_i))$ have the same limit in R, as required.

Since limits respect sums and products (7.1.9), $\widehat{f}$ is a ring homomorphism. Finally, $\widehat{f}$ is unique, since any alternative contender $\widehat{f}'$ must map $x - r_i$ into $f(\mathfrak{p})^i R$, whence that $\widehat{f}'(x)$ and $\widehat{f}(x)$ must both be the unique limit of the sequence $(f(r_i))$. □

In another illustration of the power of universal properties, we immediately derive the converse to (a) above.

7.1.17 Corollary

Let $\mathcal{O}$ be a Dedekind domain with prime ideal $\mathfrak{p}$. If $\mathcal{O}$ is $\mathfrak{p}$-adically complete, then $\mathcal{O} = \widehat{\mathcal{O}}_{\mathfrak{p}}$. □

The above results combine to say that complete Dedekind domains are precisely the completions of Dedekind domains at prime ideals. In analogy with (7.1.5) (valuation rings are the localizations of Dedekind domains at prime ideals), such rings are also known as *complete valuation rings*. (Again, we omit the qualifying phrase 'discrete rank one' as we do not consider more general valuations.)

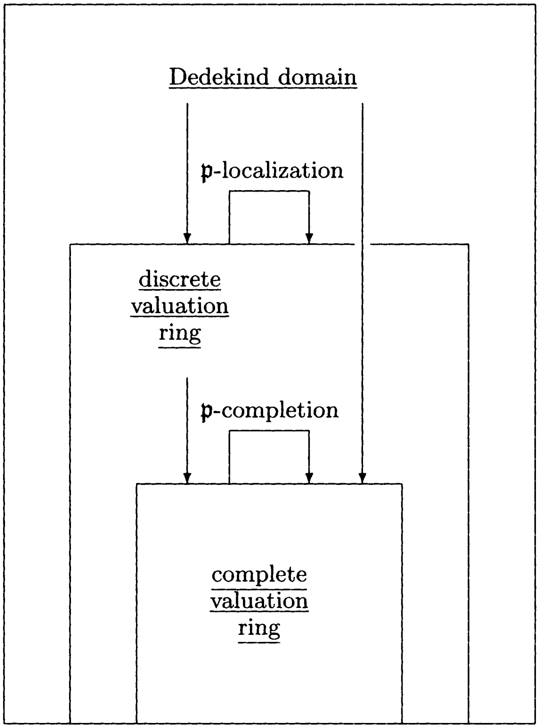

Fig. 7.1. Dedekind domains, localization and completion

Figure 7.1 presents much of the information we have obtained about localization and completion of Dedekind domains. The existence of the intermediate stage in the construction of the completion, namely, the local ring of fractions with respect to a prime ideal, was ignored by the founders of the subject, and was first investigated by [Krull 1938].

Our next result is a key tool for handling the various different completions of a Dedekind domain simultaneously.

7.1.18 The Strong Approximation Theorem

Let $\mathcal{O}$ be a Dedekind domain and let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be a finite set of nonzero prime ideals of $\mathcal{O}$, and, for each i, write

$$\widehat{\mathcal{O}}_i = \widehat{\mathcal{O}}_{\mathfrak{p}_i} \text{ and } \widehat{\mathcal{K}}_i = \widehat{\mathcal{K}}_{\mathfrak{p}_i}.$$

Suppose that we are given elements $x_i \in \widehat{\mathcal{K}}_i$ and integers $m(i)$ for $i = 1, \ldots, r$.

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

(i) *If $x_i \in \widehat{\mathcal{O}}_i$ for each i, then there is an element $x \in \mathcal{O}$ with*

$$x - x_i \in \mathfrak{p}^{m(i)}\widehat{\mathcal{O}}_i \text{ for all } i.$$

(ii) *In general, there is an element $x \in \mathcal{K}$ with*

$$x - x_i \in \mathfrak{p}^{m(i)}\widehat{\mathcal{O}}_i \text{ for all } i$$

and

$$x \in \widehat{\mathcal{O}}_{\mathfrak{q}} \text{ for } \mathfrak{q} \notin S.$$

Proof

It is clearly enough to prove the assertions when each $m(i) \geq 1$.

(i) Each x_i defines a residue class $\overline{x}_i$ in $\widehat{\mathcal{O}}_i/\mathfrak{p}_i^{m(i)}\widehat{\mathcal{O}}_i$, which is isomorphic to $\mathcal{O}/\mathfrak{p}_i^{m(i)}\mathcal{O}$ by (7.1.14). Thus the assertion follows from the Chinese Remainder Theorem ([BK: IRM] (5.1.6)).

(ii) For each i, we can choose an element p_i of $\mathcal{O}$ with $p_i\widehat{\mathcal{O}}_i = \mathfrak{p}_i\widehat{\mathcal{O}}_i$. Thus we can find positive integers $k(1), \ldots, k(r)$ with $p_i^{k(i)}x_i \in \widehat{\mathcal{O}}_i$ for each i.

Put $z = p_1^{k(1)} \cdots p_r^{k(r)}$. By construction, $v_i(z) = k(i)$ for $i = 1, \ldots, r$, where v_i is the valuation corresponding to $\mathfrak{p}_i$. However, there may be other prime ideals $\mathfrak{q}$ with $v_{\mathfrak{q}}(z) > 0$. If so, label these prime ideals $\mathfrak{p}_{r+1}, \ldots, \mathfrak{p}_s$ and write $v_j(z) = h(j)$ for $j = r+1, \ldots, s$ (extending the notation in the obvious way).

By part (i), there is an element y in $\mathcal{O}$ with

$$y - zx_i \in \mathfrak{p}^{m(i)+k(i)}\widehat{\mathcal{O}}_i \text{ for } i = 1, \ldots, r$$

and

$$y \in \mathfrak{p}_j^{h(j)}\widehat{\mathcal{O}}_j \text{ for } j = r+1, \ldots, s.$$

Put $x = y/z$. □

7.1.19 Power series

The elements of the $\mathfrak{p}$-adic completion can also be represented as power series. Choose any element p of $\mathcal{O}$ or of $\widehat{\mathcal{O}}$ with $\mathfrak{p}$-adic valuation 1, so that $p\widehat{\mathcal{O}} = \mathfrak{p}\widehat{\mathcal{O}}$. From (v) of (7.1.14) together with [BK: IRM] (5.1.24), we have isomorphisms of additive groups

$$\mathfrak{p}^h\widehat{\mathcal{O}}/\mathfrak{p}^{h+1}\widehat{\mathcal{O}} \cong \mathfrak{p}^h/\mathfrak{p}^{h+1} \cong \mathcal{O}/\mathfrak{p} \text{ for all } h.$$

Choose some set $\mathcal{S}$ of representatives of $\mathcal{O}/\mathfrak{p}$ in $\mathcal{O}$, and consider a typical element $x = (x_i)$ of $\widehat{\mathcal{O}}$. The element x_i of the residue ring $\mathcal{O}/\mathfrak{p}^i$ can be expressed as the residue of an element r_i in $\mathcal{O}$ of the form

$$r_i = s_0 + s_1 p + \cdots + s_{i-1} p^{i-1} \text{ with each } s_h \in \mathcal{S}.$$

The coherence of the inverse system guarantees that the sequence $s_0, s_1, \ldots \in \mathcal{S}$ is uniquely determined by x. In the limit, we can write

$$x = \sum_{i=0}^{\infty} s_i p^i.$$

A general element of the field of fractions $\widehat{\mathcal{K}}$ of $\widehat{\mathcal{O}}$ will have the form

$$x = \sum_{i=v}^{\infty} s_i p^i$$

where $v = v_{\mathfrak{p}}(x)$ may be negative.

Thus in $\widehat{\mathbb{Z}}_2$ we have the nice expansion

$$-1 = \sum_{i=0}^{\infty} 2^i$$

and, in $\widehat{\mathbb{Q}}_2$,

$$-1/2 = \sum_{i=-1}^{\infty} 2^i.$$

In general, there is no choice of the set $\mathcal{S}$ that facilitates computation with the power series form of elements in $\widehat{\mathcal{O}}$. However, if $\mathcal{O} = \mathcal{F}[T]$ is the polynomial ring over a field $\mathcal{F}$ and $\mathfrak{p} = T\mathcal{F}[T]$, then we always choose $\mathcal{S} = \mathcal{F}$. The T-adic completion of $\mathcal{F}[T]$ is the *ring of formal power series* $\mathcal{F}[[T]]$ over $\mathcal{F}$.

When p is a prime number in the ring of integers $\mathbb{Z}$, we make the obvious choice $\mathcal{S} = \{0, \ldots, p-1\}$; the p-adic completion of $\mathbb{Z}$ is the *ring of p-adic integers* $\widehat{\mathbb{Z}}_p$, with field of fractions $\widehat{\mathbb{Q}}_p$, the *field of p-adic rationals.*

7.1.20 Modules over complete rings

Let M be a finitely generated module over a Dedekind domain $\mathcal{O}$, with $\mathfrak{p}$ a prime ideal of $\mathcal{O}$. We now define a $\mathfrak{p}$-adic Cauchy sequence in M, and we show that M is complete if $\mathcal{O}$ is complete.

A sequence (m_i), with $m_i \in M$, $i = 1, 2, \ldots$, is a $\mathfrak{p}$-*adic Cauchy sequence* in M if the following condition is satisfied.

CSM. Given any natural number $n > 0$, there is a natural number $k = k(n)$ such that $m_i - m_j \in \mathfrak{p}^n M$ whenever $i, j \geq k$.

The Cauchy sequence (m_i) is *convergent* to the limit m in M if, given any $n > 0$, there is a $k = k(n)$ such that

$$m_i - m \in \mathfrak{p}^n M \text{ whenever } i \geq k.$$

The module M is said to be $\mathfrak{p}$-*adically complete* if every Cauchy sequence in M has a limit in M.

7.1.21 Theorem

Suppose that $\mathcal{O}$ is a complete valuation ring, with maximal ideal $\mathfrak{p}$. Then every finitely generated $\mathcal{O}$-module M is $\mathfrak{p}$-adically complete.

Proof

If $M = M_1 \oplus \cdots \oplus M_k$ is a direct sum decomposition of M, then any Cauchy sequence in M decomposes into a direct sum of Cauchy sequences, one in each summand. Thus it is enough to know that each summand is complete.

Since $\mathcal{O}$ is a valuation ring, M is a direct sum of modules of the form $\mathcal{O}$ or $\mathcal{O}/\mathfrak{p}^i$ for $i > 0$ by (7.1.6). But $\mathcal{O}$ is complete by hypothesis, and $\mathcal{O}/\mathfrak{p}^i$ is trivially complete, as any Cauchy sequence must become stationary. □

7.1.22 Completion of modules

Let $\mathcal{O}$ be an arbitrary Dedekind domain and let $\widehat{\mathcal{O}}_\mathfrak{p}$ be the completion of $\mathcal{O}$ at a nonzero prime ideal $\mathfrak{p}$. Following [Serre 1956], we define the $\mathfrak{p}$-*adic completion* of an $\mathcal{O}$-module M to be

$$\widehat{M_\mathfrak{p}} = M \otimes_\mathcal{O} \widehat{\mathcal{O}}_\mathfrak{p}.$$

First, we look at the effect of this construction on the field of fractions of $\mathcal{O}$. By combining (vi) of (7.1.14) with (6.2.10), we can identify the tensor product $\widehat{\mathcal{O}}_\mathfrak{p} \otimes_\mathcal{O} \mathcal{K}$ with the field of fractions $\widehat{\mathcal{K}}_\mathfrak{p} = \widehat{\mathcal{O}}_\mathfrak{p}\mathcal{K}$ of $\widehat{\mathcal{O}}_\mathfrak{p}$. We leave the reader the task of showing that $\widehat{\mathcal{K}}_\mathfrak{p}$ is complete under a suitable extension of the notion of a Cauchy sequence, in which the 'subsets' $\mathfrak{p}^i\widehat{\mathcal{K}}_\mathfrak{p}$ are replaced by the $\widehat{\mathcal{O}}_\mathfrak{p}$-submodules

$$\{x \in \widehat{\mathcal{K}}_\mathfrak{p} \mid v(x) \geq i\}, \quad i \in \mathbb{Z},$$

of $\widehat{\mathcal{K}}_\mathfrak{p}$.

Now assume that M is a finitely generated $\mathcal{O}$-module. Then $\widehat{M_\mathfrak{p}}$ is a finitely generated $\widehat{\mathcal{O}}_\mathfrak{p}$-module, so that $\widehat{M_\mathfrak{p}}$ is complete by (7.1.21) above. It is straightforward to describe what happens to M during completion.

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

By the structure theory for modules over a Dedekind domain (2.3.20), we know that M is a direct sum of $\mathcal{O}$-modules of the form $\mathfrak{a}$, $\mathcal{O}/\mathfrak{p}^i$ or $\mathcal{O}/\mathfrak{q}^j$, where $\mathfrak{a}$ is an ideal of $\mathcal{O}$ and $\mathfrak{q}$ is some prime ideal of $\mathcal{O}$ other than $\mathfrak{p}$. Since a tensor product with a direct sum is isomorphic to the corresponding direct sum of tensor products, $\widehat{M_\mathfrak{p}}$ is a direct sum of completions of modules of these types. Such completions behave as follows.

- The completion of an ideal must be an ideal of the principal ideal domain $\widehat{\mathcal{O}}_\mathfrak{p}$, and hence isomorphic to $\widehat{\mathcal{O}}_\mathfrak{p}$.
- As remarked in the proof of the preceding result, $\mathcal{O}/\mathfrak{p}^i$ is already its own completion.
- For a factor of the form $\mathcal{O}/\mathfrak{q}^j$, first note that there is some element $x \in \mathfrak{q}^j \backslash \mathfrak{p}$ (otherwise $\mathfrak{q}^j \subseteq \mathfrak{p}$, which cannot happen in a Dedekind domain by unique factorization of ideals (2.3.20 – A)). Since x is a unit in $\widehat{\mathcal{O}}_\mathfrak{p}$ by (7.1.11), and $(\mathcal{O}/\mathfrak{q}^j)x = 0$, we have, for any $y \in \mathcal{O}/\mathfrak{q}^j$,
$$y \otimes 1 = yx \otimes x^{-1} = 0$$
in
$$\widehat{\mathcal{O}}/\mathfrak{q}^j \otimes \widehat{\mathcal{O}}_\mathfrak{p} = \widehat{(\mathcal{O}/\mathfrak{q}^j)}_\mathfrak{p},$$
which shows that
$$\widehat{(\mathcal{O}/\mathfrak{q}^j)}_\mathfrak{p} = 0.$$

If we compare the above analysis with that given for localized modules in (7.1.6), we obtain the next result from (7.1.15).

7.1.23 Proposition

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

(i) *the embedding of $\mathcal{O}$ in $\mathcal{O}_\mathfrak{p}$ induces an isomorphism of $\mathfrak{p}$-torsion submodules*
$$T_\mathfrak{p}(N) \cong T_\mathfrak{p}(N_\mathfrak{p}),$$
the latter being the same as $T(N_\mathfrak{p})$;

(ii) *the embedding of $\mathcal{O}_\mathfrak{p}$ in $\widehat{\mathcal{O}}_\mathfrak{p}$ induces an injective $\mathcal{O}_\mathfrak{p}$-homomorphism from $N_\mathfrak{p}$ to $\widehat{N}_\mathfrak{p}$, which in turn restricts to an isomorphism of $T_\mathfrak{p}(N_\mathfrak{p})$ with $T_\mathfrak{p}(\widehat{N}_\mathfrak{p})$, the latter being the same as $T(\widehat{N}_\mathfrak{p})$.*

(iii) *the embedding of $\mathcal{O}$ in $\widehat{\mathcal{O}}_\mathfrak{p}$ induces an $\mathcal{O}$-isomorphism from $T_\mathfrak{p}(N)$ to $T_\mathfrak{p}(\widehat{N}_\mathfrak{p})$; in particular, $T_\mathfrak{p}(N)$ is already complete.* □

We record an important property of completion.

7.1.24 Theorem

Let $\mathfrak{p}$ be a nonzero prime ideal of a Dedekind domain $\mathcal{O}$. Then the functor $- \otimes_{\mathcal{O}} \widehat{\mathcal{O}}_{\mathfrak{p}} : \mathcal{M}\text{OD}_{\mathcal{O}} \to \mathcal{M}\text{OD}_{\widehat{\mathcal{O}}_{\mathfrak{p}}}$ is exact, and $\widehat{\mathcal{O}}_{\mathfrak{p}}$ is flat, both as a left and as a right $\mathcal{O}$-module.

Proof

By (3.2.8) it is enough to show that an injective homomorphism $\alpha : L \to M$ of finitely generated $\mathcal{O}$-modules induces an injective map on their completions.

Appealing again to the structure theorem for modules (2.3.20), we have $L = \bigoplus_{\mathfrak{q}} T_{\mathfrak{q}}(L) \oplus F(L)$, where $T_{\mathfrak{q}}(L)$ is the $\mathfrak{q}$-primary part of L for a nonzero prime ideal $\mathfrak{q}$, $\bigoplus_{\mathfrak{q}} T_{\mathfrak{q}}(L) = T(L)$ is the torsion part of L, and $F(L) \cong L/T(L)$ is a projective $\mathcal{O}$-module.

It is obvious that $T_{\mathfrak{q}}(L)$ is mapped injectively to $T_{\mathfrak{q}}(M)$ for each prime $\mathfrak{q}$; the preceding discussion now shows that $T_{\mathfrak{q}}(L) \otimes_{\mathcal{O}} \widehat{\mathcal{O}}_{\mathfrak{p}}$ maps injectively to $T_{\mathfrak{q}}(M) \otimes_{\mathcal{O}} \widehat{\mathcal{O}}_{\mathfrak{p}}$ since the modules are either both unchanged or both made zero.

Also, α induces an injection from $F(L)$ to $F(M)$, so it is enough to prove that $F(L) \otimes_{\mathcal{O}} \widehat{\mathcal{O}}_{\mathfrak{p}}$ maps injectively to $F(M) \otimes_{\mathcal{O}} \widehat{\mathcal{O}}_{\mathfrak{p}}$. Since a finitely generated projective $\mathcal{O}$-module is a direct sum of ideals of $\mathcal{O}$, we may assume that L is some (nonzero) ideal $\mathfrak{a}$ of $\mathcal{O}$ and that M is projective. In this case, the completion of L is isomorphic to $\widehat{\mathcal{O}}_{\mathfrak{p}}$, the completion of M is isomorphic to $\widehat{\mathcal{O}}_{\mathfrak{p}}^n$ for some integer n, and there is an induced map $\widehat{\alpha} : \widehat{\mathcal{O}}_{\mathfrak{p}} \to \widehat{\mathcal{O}}_{\mathfrak{p}}^n$ which must be either injective or the zero map. To see that $\widehat{\alpha}$ cannot be zero, notice that $\widehat{\alpha}$ induces a homomorphism $\widehat{\beta} : \widehat{\mathcal{K}}_{\mathfrak{p}} \to \widehat{\mathcal{K}}_{\mathfrak{p}}^n$, where $\widehat{\mathcal{K}}_{\mathfrak{p}}$ is the field of fractions of $\widehat{\mathcal{O}}_{\mathfrak{p}}$. However, $\widehat{\beta}$ can also be computed by first taking the tensor product of the embedding $\mathfrak{a} \to M$ with the field of fractions $\mathcal{K}$ of $\mathcal{O}$, which gives a nonzero split injection of $\mathcal{K}$ into $\mathcal{K}^n$, and then completing (see (vi) of (7.1.14)). □

7.1.25 Adèles

It is useful to be able to consider all the completions of a Dedekind domain $\mathcal{O}$ simultaneously. We can do this by following [Chevalley 1936] and [Chevalley 1940] and introducing the *adèle rings* $A(\mathcal{O})$ and $A(\mathcal{K})$, where $\mathcal{K}$ is the field of fractions of $\mathcal{O}$. We set $A(\mathcal{O}) = \prod_{\mathfrak{p}} \widehat{\mathcal{O}}_{\mathfrak{p}}$, the direct product of all the completions of $\mathcal{O}$, which we make into a ring by the obvious componentwise definitions of addition and multiplication. We identify $\mathcal{O}$ as a subring of $A(\mathcal{O})$ by the diagonal embedding, which sends an element x of $\mathcal{O}$ to the 'constant' sequence $(x)_{\mathfrak{p}}$ in $A(\mathcal{O})$.

The ring $A(\mathcal{K})$ is defined to be the *restricted direct product* $\prod'_{\mathfrak{p}} \widehat{\mathcal{K}}_{\mathfrak{p}}$ of the completions $\widehat{\mathcal{K}}_{\mathfrak{p}}$ with respect to their subrings $\widehat{\mathcal{O}}_{\mathfrak{p}}$, that is, an element x of

$\mathcal{A}(\mathcal{K})$ is a member $x = (x_\mathfrak{p})_\mathfrak{p}$ of the direct product $\prod_\mathfrak{p} \widehat{\mathcal{K}}_\mathfrak{p}$, but with $x_\mathfrak{p} \in \widehat{\mathcal{O}}_\mathfrak{p}$ for almost all $\mathfrak{p}$. Again, we obtain the ring structure through the expected componentwise definitions.

Evidently, $A(\mathcal{O})$ is a subring of $A(\mathcal{K})$, and we can view $\mathcal{K}$ as a subring of $A(\mathcal{K})$ through the diagonal embedding $x \mapsto (x)_\mathfrak{p}$, since an element x of $\mathcal{K}$ can have $\mathfrak{p}$-adic valuation $v_\mathfrak{p}(x) < 0$ for only a finite set of primes $\mathfrak{p}$. Then $\mathcal{O} = A(\mathcal{O}) \cap \mathcal{K}$, since $\mathcal{O} = \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p}$ ([BK: IRM] (6.2.7)). In effect, $\mathcal{O}$ is the pull-back of the rings $\mathcal{K}$ and $A(\mathcal{O})$ over $A(\mathcal{K})$ in the category of rings – see Exercise 1.4.11.

We extend the $\mathfrak{p}$-adic valuations of $\mathcal{K}$ to $A(\mathcal{K})$ by setting $v_\mathfrak{p}(x) = v_\mathfrak{p}(x_\mathfrak{p})$ for $x = (x_\mathfrak{p})_\mathfrak{p} \in A(\mathcal{K})$. By the definition of $\mathcal{A}(\mathcal{K})$, we have $v_\mathfrak{p}(x) < 0$ for only a finite set of primes. The Strong Approximation Theorem (7.1.18) tells us that there is an element $z \in \mathcal{O}$ with $v_\mathfrak{p}(z) = -v_\mathfrak{p}(x)$ at each of these primes, so that $zx \in A(\mathcal{O})$, and hence

$$\mathcal{K}A(\mathcal{O}) = A(\mathcal{K}).$$

We also note that, since $\mathcal{K}$ is a flat $\mathcal{O}$-module, we can identify $A(\mathcal{K})$ as $\mathcal{K} \otimes_\mathcal{O} A(\mathcal{O})$, using (3.3.9).

Let $\mathcal{T}_{A(\mathcal{O}),\mathcal{O}}$ be the category of finitely generated $A(\mathcal{O})$-modules which are torsion as $\mathcal{O}$-modules, and let $\mathcal{T}_{A(\mathcal{O}),\mathfrak{p}}$ be its subcategory of $\mathfrak{p}$-torsion modules.

7.1.26 Proposition

Let $\mathcal{O}$ be a Dedekind domain. Then there are equivalences of categories as follows.

(i) *For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$,*

$$\mathcal{T}_{\mathcal{O},\mathfrak{p}} = \mathcal{T}_{\widehat{\mathcal{O}}_\mathfrak{p},\mathfrak{p}} \simeq \mathcal{T}_{A(\mathcal{O}),\mathfrak{p}}.$$

(ii) $\mathcal{T}_{A(\mathcal{O}),\mathcal{O}} \simeq \bigoplus_\mathfrak{p} \mathcal{T}_{A(\mathcal{O}),\mathfrak{p}}$.

(iii) $\mathcal{T}_{A(\mathcal{O}),\mathcal{O}} \simeq \mathcal{T}_\mathcal{O}$.

Proof

A finitely generated $\mathfrak{p}$-torsion $\mathcal{O}$-module is a direct sum of modules of the form $\mathcal{O}/\mathfrak{p}^h = \widehat{\mathcal{O}}_\mathfrak{p}/\mathfrak{p}^h\widehat{\mathcal{O}}_p$; such a module is therefore an $\widehat{\mathcal{O}}_\mathfrak{p}$-module and vice-versa, so we can identify the categories $\mathcal{T}_{\widehat{\mathcal{O}}_\mathfrak{p},\mathfrak{p}}$ and $\mathcal{T}_{\mathcal{O},\mathfrak{p}}$. It is also clear that any $\mathfrak{p}$-torsion $\mathcal{O}$-module can be viewed as an $A(\mathcal{O})$-module, with $\mathcal{A}(\mathcal{O})$ acting through its $\widehat{\mathcal{O}}_\mathfrak{p}$-component, and therefore $\mathcal{T}_{\mathcal{O},\mathfrak{p}}$ can be regarded as a subcategory of $\mathcal{T}_{A(\mathcal{O}),\mathfrak{p}}$.

Recall also that, by (2.3.21), there is an equivalence of categories

$$\mathcal{T}_\mathcal{O} \simeq \bigoplus_\mathfrak{p} \mathcal{T}_{\mathcal{O},\mathfrak{p}},$$

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

which shows that $\mathcal{T}_{\mathcal{O}}$ can be embedded as a subcategory in $\mathcal{T}_{A(\mathcal{O}),\mathcal{O}}$. To prove (iii), from which (ii) now follows, we have to establish that this embedding is surjective, that is, if M is a module in $\mathcal{T}_{A(\mathcal{O}),\mathcal{O}}$, then M is already finitely generated over $\mathcal{O}$.

Let $\{m_1, \ldots, m_k\}$ be a set of generators of M as an $A(\mathcal{O})$-module. Since M is $\mathcal{O}$-torsion, for each $i = 1, \ldots, k$ there is some nonzero a_i in $\mathcal{O}$ with $a_i m_i = 0$. Put $a = a_1 \cdots a_k$, so that $a \neq 0$ and $aM = 0$. Thus M is a finitely generated module over the residue ring $A(\mathcal{O})/aA(\mathcal{O})$. But a is a unit in $\widehat{\mathcal{O}}_{\mathfrak{p}}$ for all except a finite set S of primes, so that

$$A(\mathcal{O})/aA(\mathcal{O}) = \bigoplus\nolimits_{\mathfrak{p}\in S} \widehat{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{p}^{v(\mathfrak{p},a)}\widehat{\mathcal{O}}_{\mathfrak{p}} \cong \bigoplus\nolimits_{\mathfrak{p}\in S} \mathcal{O}/\mathfrak{p}^{v(\mathfrak{p},a)}$$

as $\mathcal{O}$-modules, which confirms that M must be finitely generated as an $\mathcal{O}$-module. □

Since the tensor product commutes with direct sums and the ring $A(\mathcal{O})$ acts on a $\mathfrak{p}$-primary module through its component $\widehat{\mathcal{O}}_{\mathfrak{p}}$, we obtain the following observation.

7.1.27 Corollary

Let M be a finitely generated torsion $\mathcal{O}$-module. Then there is an $A(\mathcal{O})$-module isomorphism $M \otimes_{\mathcal{O}} A(\mathcal{O}) \cong M$. □

We now record some relationships between the local and the global behaviour of modules and homomorphisms.

7.1.28 Proposition

For any $\mathcal{O}$-module M, the natural $\mathcal{O}$-homomorphism θ from M to $\prod_{\mathfrak{p}} \widehat{M_{\mathfrak{p}}}$ is injective. In particular, if $\widehat{M_{\mathfrak{p}}} = 0$ for all $\mathfrak{p}$, then $M = 0$.

Proof

For every finitely generated submodule N of M, the canonical homomorphisms

$$N \longrightarrow \prod\nolimits_{\mathfrak{p}} N_{\mathfrak{p}} \longrightarrow \prod\nolimits_{\mathfrak{p}} \widehat{N}_{\mathfrak{p}} \longrightarrow \prod\nolimits_{\mathfrak{p}} \widehat{M_{\mathfrak{p}}}$$

are all injective, by (6.2.3), (7.1.23) and (7.1.24) respectively. Since any element of $\operatorname{Ker}\theta$ necessarily belongs to a finitely generated submodule of M, the result follows. □

The next result is a straightforward consequence, proved by mimicking the derivation of (6.2.4) from (6.2.3).

7.1.29 Corollary

Let $\alpha : M \to N$ be a right $\mathcal{O}$-module homomorphism, with $\widehat{\alpha}_\mathfrak{p} : \widehat{M}_\mathfrak{p} \to \widehat{N}_\mathfrak{p}$ the induced $\widehat{\mathcal{O}}_\mathfrak{p}$-module homomorphism for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$. Then the following hold.

(a) *For each prime ideal $\mathfrak{p}$ of $\mathcal{O}$,*

(i) $\operatorname{Ker}\widehat{\alpha}_\mathfrak{p} = (\widehat{\operatorname{Ker}\alpha})_\mathfrak{p}$,

(ii) $\operatorname{Im}\widehat{\alpha_\mathfrak{p}} = (\widehat{\operatorname{Im}\alpha})_\mathfrak{p}$,

(iii) $\operatorname{Cok}\widehat{\alpha}_\mathfrak{p} = (\widehat{\operatorname{Cok}\alpha})_\mathfrak{p}$.

(b) *α is injective if and only if $\widehat{\alpha}_\mathfrak{p}$ is injective for every prime ideal $\mathfrak{p}$.*

(c) *As* (b), *with injective replaced throughout by 'surjective', or by 'bijective', or by 'zero'.*

(d) *A sequence*

$$L \xrightarrow{\ \beta\ } M \xrightarrow{\ \alpha\ } N$$

is exact at M if and only if the sequence

$$\widehat{L}_\mathfrak{p} \xrightarrow{\ \widehat{\beta}_\mathfrak{p}\ } \widehat{M}_\mathfrak{p} \xrightarrow{\ \widehat{\alpha}_\mathfrak{p}\ } \widehat{N}_\mathfrak{p}$$

is exact at $\widehat{M}_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$. □

7.1.30 Completions in general

It is not difficult to construct the completion of an arbitrary ring R or of an arbitrary R-module M with respect to a (twosided) ideal $\mathfrak{a}$ of R (see the exercises). However, in general, a completion need not have a good relationship to the original ring or module, and conditions must be imposed on the ring or the ideal to ensure that there is some reasonable connection. The best results require that R is commutative; even in this case, the arguments are fairly technical. For a discussion, see [Atiyah & Macdonald 1969], Chapter 10.

The noncommutative case is considered in [Northcott 1968], Chapter 9, and (from a more categorical point of view) in [Stenström 1975]. All these texts emphasize the topological aspects of the theory.

Exercises

7.1.1 Let $\mathcal{K}$ be a field with a (discrete rank one) valuation v, valuation ring

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

$\mathcal{V}$ and uniformizing parameter p. Show that the groups of units of $\mathcal{K}$ and $\mathcal{V}$ are related by the direct product decomposition

$$U(\mathcal{K}) = \langle p \rangle \times U(\mathcal{V}),$$

where $\langle p \rangle$ is the (multiplicative) cyclic group generated by p.

7.1.2 Let R be any ring and let $\mathfrak{a}$ be a (twosided) ideal in R.

(i) Define an $\mathfrak{a}$-adic Cauchy sequence in R.

(ii) Let ℓ be the limit of some $\mathfrak{a}$-adic Cauchy sequence. Show that ℓ' is also a limit of the same sequence if and only if

$$\ell - \ell' \in \cap_{i=0}^{\infty} \mathfrak{a}^i.$$

(iii) Give an example where a Cauchy sequence has more than one limit.

(iv) Construct an $\mathfrak{a}$-adic completion $\widehat{R}$ of R.

(v) Show that the natural homomorphism π from R to $\widehat{R}$ has kernel $\bigcap_{i=0}^{\infty} \mathfrak{a}^i$.

Hint. What happens when $\mathfrak{a}^2 = \mathfrak{a}$?

7.1.3 Let M be a right R-module. Construct an $\mathfrak{a}$-adic completion $\widehat{M}$ of M as the inverse limit of the system $\{M/M\mathfrak{a}^i\}$. Show that $\widehat{M}$ is a right $\widehat{R}$-module, and that the natural map from M to $\widehat{M}$ has kernel $\bigcap_{i=0}^{\infty} M\mathfrak{a}^i$, and cokernel $\varprojlim^1 \{M\mathfrak{a}^i\}$ (see Exercise 5.3.2), where the inverse system $\{M\mathfrak{a}^i\}$ is given by inclusions

$$\cdots \hookrightarrow M\mathfrak{a}^{i+1} \hookrightarrow M\mathfrak{a}^i \hookrightarrow \cdots \hookrightarrow M\mathfrak{a} \hookrightarrow M.$$

Hence M is $\mathfrak{a}$-adically complete if and only if $\varprojlim^1 \{M\mathfrak{a}^i\} = 0$.

7.1.4 For each $h > 0$, let $\widehat{(\mathfrak{a}^h)}$ denote the completion of $\mathfrak{a}^h$, regarded as a right R-module. Show that $\widehat{(\mathfrak{a}^h)}$ is a twosided ideal in $\widehat{R}$ and that

$$\widehat{R}/\widehat{(\mathfrak{a}^h)} \cong R/\mathfrak{a}^h$$

as rings.

7.1.5 *Assume* that $\widehat{(\mathfrak{a}^h)} = (\widehat{\mathfrak{a}})^h$ for all h. Show that $\widehat{R}$ is $\widehat{\mathfrak{a}}$-adically complete.

Warning. This hypothesis is highly nontrivial; it may not be satisfied when R is noncommutative. For a proof that it holds in the commutative case, see [Atiyah & Macdonald 1969], Proposition 10.15.

7.1.6 Let $\mathcal{O}$ be a Dedekind domain. Show:

(i) if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ with $(\mathfrak{b}, \mathfrak{c}) = 1$, then

$$\widehat{\mathcal{O}}_{\mathfrak{a}} \cong \widehat{\mathcal{O}}_{\mathfrak{b}} \times \widehat{\mathcal{O}}_{\mathfrak{c}}$$

as rings;

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

(ii) if $\mathfrak{a} = \mathfrak{p}^h$ for some prime ideal $\mathfrak{p}$, then $\widehat{\mathcal{O}}_{\mathfrak{a}} \cong \widehat{\mathcal{O}}_{\mathfrak{p}}$.

Hence describe $\widehat{\mathcal{O}}_{\mathfrak{a}}$ in general.

7.1.7 **Skew formal power series**

Let $\mathcal{F}$ be a field and α an endomorphism of $\mathcal{F}$.

The T-adic completion of the skew polynomial ring $\mathcal{F}[T, \alpha]$ (6.1.3) is written $\mathcal{F}[[T, \alpha]]$ and called the ring of *skew formal power series.* Justify this terminology.

7.1.8 **A metric interpretation**

Our discussion of completions can be rephrased in terms of completions of metric spaces.

(1) Suppose that $\mathfrak{a}$ is an ideal in a ring R and that $\bigcap_{i=0}^{\infty} \mathfrak{a}^i = 0$. Given a nonzero element r in R, there is then a unique exponent $v(r)$ with $r \in \mathfrak{a}^{v(r)} \setminus \mathfrak{a}^{v(r)+1}$. By convention, $v(0) = \infty$.
Show that the function $v : R \to \mathbb{N}_{\cup}\{\infty\}$ has the properties

(a) $v(x + y) \geq \min(v(x), v(y))$;
(b) $v(rs) \geq v(r) + v(s)$.

(2) Choose some real number $e > 1$, and define $\|r\| = e^{-v(r)}$ and $\|0\| = 0$. The function $\|\cdot\| : R \to \mathbb{R}$ is called the $\mathfrak{a}$-*adic norm* for R. Verify that it is a norm in the standard sense of the term by checking:

(c) $\|r\| = 0$ if and only if $r = 0$;
(d) for $r, s \in R$, $\|r + s\| \leq \max(\|r\|, \|s\|)$;
(e) the Triangle Inequality: for $r, s \in R$, $\|r + s\| \leq \|r\| + \|s\|$.

(3) Define $d(r, s) = \|r - s\|$. Show that d is a *metric* on R by confirming the following.

(f) $d(r, s) = 0$ if and only if $r = s$,
(g) $d(r, s) = d(s, r)$ for all r and s,
(h) $d(r, t) \leq \max(d(r, s), d(s, t))$ for all r, s and t,
(i) $d(r, t) \leq d(r, s) + d(s, t)$.

Remark. The strong forms (d), (h) of the triangle inequality show that we have in fact an *ultranorm* and an *ultrametric.* It follows from (h) that, for any three elements r, s and t of R, the distances $d(r, t)$, $d(r, s)$ and $d(s, t)$ cannot all be distinct – every triangle is isosceles.

(4) Show that an $\mathfrak{a}$-adic Cauchy sequence (r_i) is a Cauchy sequence in the usual sense:

given any $\epsilon > 0$, there is an $N = N(\epsilon)$ such that $d(r_i, r_j) < \epsilon$ whenever $i, j \geq N$.

Confirm also that the notions of limit, convergence and completeness have their usual meaning.

7.2 THE PROJECTIVE MODULE LIFTING PROBLEM

We next look at the relationship between the projective modules over a ring R and those over a residue ring $R/\mathfrak{a}$, where $\mathfrak{a}$ is a twosided ideal of R.

In one direction, there is not much difficulty: since the quotient functor $- \otimes_R R/\mathfrak{a}$ preserves direct sums, any finitely generated projective right R-module P gives rise to a finitely generated projective right $R/\mathfrak{a}$-module $P/P\mathfrak{a}$.

Much more interesting is the problem in the reverse direction, which is called the *lifting problem for projective modules*: given a finitely generated projective right $R/\mathfrak{a}$-module Q, is there a finitely generated projective right R-module P with $P/P\mathfrak{a} \cong Q$? If so, we say that Q can be *lifted* to P over$R$.

A positive solution to the lifting problem is of most use when the residue ring $R/\mathfrak{a}$ is Artinian semisimple, since then the projective modules over $R/\mathfrak{a}$ are already known. We therefore concentrate on the situation when the ideal is the Jacobson radical $\operatorname{rad}(R)$ of R and the residue ring $R/\operatorname{rad}(R)$ is Artinian, giving conditions which permit projective lifting from $R/\operatorname{rad}(R)$ to R. These conditions hold in particular for orders over complete valuation rings, and lead to a full description of the projective modules for these rings.

Our discussion and results draw on the properties of Artinian rings and modules and of the Jacobson radical, which are developed at length in [BK: IRM], Chapter 4.

7.2.1 Some illustrations

Before we get involved in the general discussion, here are some explicit examples.

Suppose that $R = R_1 \times R_2$ is the direct product of rings. Then any projective R_2-module is already projective as an R-module, and so lifts to itself over R.

If the ring R and the ideal $\mathfrak{a}$ are such that every finitely generated projective $R/\mathfrak{a}$-module happens to be free, then again lifting is possible, as seen from the elementary observation that $R/\mathfrak{a}$ lifts to R. Thus, for instance, every finitely generated $\mathbb{Z}/2\mathbb{Z}$-module lifts to $\mathbb{Z}$.

For an example where lifting is not possible, consider $\mathbb{Z}/6\mathbb{Z}$. The direct sum decomposition $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ shows that $\mathbb{Z}/2\mathbb{Z}$ is a projective $\mathbb{Z}/6\mathbb{Z}$-module; since every projective $\mathbb{Z}$-module is free, the $\mathbb{Z}/6\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ cannot be lifted over $\mathbb{Z}$.

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

7.2.2 Idempotents

For the moment, let R be an arbitrary ring and let $\mathfrak{a}$ be any twosided ideal of R. The lifting problem becomes more amenable when it is recast in terms of idempotent matrices.

Let P be a finitely generated projective right R-module. Then there is a surjective R-module homomorphism $\pi : R^n \to P$ for some n, and, by the definition of a projective module (1.1.7), π is split by some R-module homomorphism $\sigma : P \to R^n$, that is, $\pi\sigma = id_P$. Put $\epsilon = \sigma\pi$; then ϵ is an idempotent element of the endomorphism ring $\mathrm{End}(R^n)$. Conversely, if $P \cong \epsilon R^n$ for some n and some idempotent element ϵ in $\mathrm{End}(R^n)$, then P is projective. (More complete details are given in [BK: IRM] §2.5.)

Furthermore, $\mathrm{End}(R^n)$ can be identified with the matrix ring $M_n(R)$ by choosing a convenient basis of R^n, say the standard basis – see (1.3.4) or, for full details, [BK: IRM] (2.2.9). Thus the idempotent ϵ can be regarded as an idempotent matrix.

The canonical ring homomorphism from R to $R/\mathfrak{a}$ gives a ring homomorphism from $M_n(R)$ to $M_n(R/\mathfrak{a})$; with $\overline{\epsilon}$ as the image of ϵ, it is clear that $\overline{\epsilon}$ is again idempotent, and that $P/P\mathfrak{a} \cong (R/\mathfrak{a})^n$.

In the other direction, let Q be a projective $R/\mathfrak{a}$-module, with associated $n \times n$ idempotent matrix η in $M_n(R/\mathfrak{a})$. If there is an idempotent matrix ϵ in $M_n(R)$ such that $\overline{\epsilon} = \eta$, then $P = \epsilon R^n$ solves the lifting problem for Q. Thus we can solve the lifting problem for projectives if we can solve the *idempotent lifting problem*: given any idempotent matrix η in $M_n(R/\mathfrak{a})$, $n \geq 1$, there is an idempotent matrix ϵ in $M_n(R)$ with $\overline{\epsilon} = \eta$.

More generally, for any ring homomorphism $f : R \to R/\mathfrak{a}$ and idempotent η in $R/\mathfrak{a}$, if there is an idempotent ϵ in R with $\eta = f\epsilon$ then we say that η *lifts to* ϵ in R.

On the face of it, the idempotent lifting problem would appear to be harder than the projective lifting problem, since a single projective $R/\mathfrak{a}$-module Q can be obtained from infinitely many idempotent matrices, and we could solve the projective lifting problem by lifting only one of them. However, idempotent lifting can be attacked using the completeness results we established in the previous section. Moreover, the most systematic method of lifting projectives seems to be through lifting idempotents.

7.2.3 Semiperfect rings

We now define a class of ring by requiring that idempotent elements of $R/\operatorname{rad}(R)$ can be lifted into R, where $\operatorname{rad}(R)$ is the Jacobson radical of R. (The theory of the Jacobson radical is developed in [BK: IRM] §4.3.)

We say that the ring R is *semilocal* if $R/\operatorname{rad}(R)$ is semisimple and Artinian. We say that R is *semiperfect* if it is semilocal and every idempotent of $R/\operatorname{rad}(R)$ can be lifted into R.

It is easy to see that a local ring must be semiperfect, since $R/\operatorname{rad}(R)$ is then a division ring, with 0 and 1 as its only idempotents.

The following lemma is a first step in producing semiperfect rings.

7.2.4 Lemma

Let $\mathfrak{n}$ be a nilpotent ideal of the ring R. Then idempotents can be lifted from $R/\mathfrak{n}$ into R.

Proof

Suppose that $\mathfrak{n}^n = 0$, $n > 1$. Let η be an idempotent in $R/\mathfrak{n}$ and choose any r in R that maps to η. Then $(r^2 - r)^n = 0$, hence $r^n = f(r)r^{n+1}$, where $f(r)$ is a polynomial in r with integer coefficients. Thus $f(r)^n r^n$ is an idempotent in R, which lifts η since $f(\eta)\eta = \eta$. □

7.2.5 Corollary

Suppose that the ring R is Artinian. Then R is semiperfect.

Proof

We know $\operatorname{rad}(R)$ to be nilpotent ([BK: IRM] (4.3.20)). □

7.2.6 Orders over complete valuation rings

Let $\widehat{\mathcal{O}}$ be a complete valuation ring, with maximal ideal $\mathfrak{p}$, and let R be an $\widehat{\mathcal{O}}$-order. By definition, $\widehat{\mathcal{O}}$ belongs to the centre of R and R is then a finitely generated torsion free $\widehat{\mathcal{O}}$-module. For example, it follows from (7.1.23) that if S is an $\mathcal{O}$-order, where $\mathcal{O}$ is a Dedekind domain with nonzero prime ideal $\mathfrak{p}$, then $R = \widehat{S}_{\mathfrak{p}} = \widehat{\mathcal{O}}_{\mathfrak{p}} \otimes_{\mathcal{O}} S$ is an $\widehat{\mathcal{O}}_{\mathfrak{p}}$-order.

We show that R is semiperfect. First, note that the discussion in (7.1.21) shows R to be a free $\widehat{\mathcal{O}}$-module which is $\mathfrak{p}R$-adically complete, both as an $\widehat{\mathcal{O}}$-module and also as a ring.

7.2.7 Lemma

(i) $\mathfrak{p}R \subseteq \operatorname{rad}(R)$, *the Jacobson radical of R.*

(ii) $\operatorname{rad}(R/\mathfrak{p}R) = \operatorname{rad}(R)/\mathfrak{p}R$.

(iii) $\operatorname{rad}(R)^h \subseteq \mathfrak{p}R$ *for some h.*

Proof

(i) We call upon an equivalence that is part of Nakayama's Lemma ([BK: IRM] (4.3.10)): given a ring S and a right ideal $\mathfrak{a}$ of S, we have $M\mathfrak{a} \neq M$ for all nonzero finitely generated right S-modules M if and only if $\mathfrak{a} \subseteq \operatorname{rad}(S)$.

Suppose then that M is a finitely generated (right) R-module with $M \cdot \mathfrak{p}R = M$. Then M is a finitely generated $\widehat{\mathcal{O}}$-module with the same property, and so $M = 0$, since $\mathfrak{p} = \operatorname{rad}(\widehat{\mathcal{O}})$ by (iv) of (7.1.14). Thus $\mathfrak{p}R \subseteq \operatorname{rad}(R)$.

(ii) Given (i), this is immediate from the definition of the Jacobson radical as the intersection of the maximal right ideals of a ring ([BK: IRM] (4.3.1)).

(iii) Since R is a free $\widehat{\mathcal{O}}$-module of finite rank, $R/\mathfrak{p}R$ is a finite-dimensional vector space over the field $\widehat{\mathcal{O}}/\mathfrak{p}$ and hence Artinian. Thus $R/\mathfrak{p}R$ has nilpotent radical $\operatorname{rad}(R)/\mathfrak{p}R$, by (ii). □

7.2.8 The Idempotent Lifting Theorem

Let R be an $\widehat{\mathcal{O}}$-order, where $\widehat{\mathcal{O}}$ is a complete valuation ring. Then idempotents can be lifted from $R/\operatorname{rad}(R)$ into R, and hence R is semiperfect.

Proof

Let η be an idempotent in $R/\operatorname{rad}(R)$. By the preceding lemma, $\operatorname{rad}(R/\mathfrak{p}R) = \operatorname{rad}(R)/\mathfrak{p}R$ is a nilpotent ideal of $R/\mathfrak{p}R$. Thus η lifts to an idempotent $\eta^{(1)}$ in $R/\mathfrak{p}R$, by (7.2.4).

Since, for each $h \geq 2$, $(\mathfrak{p}^{h-1}R)/(\mathfrak{p}^hR)$ is a nilpotent ideal in $R/\mathfrak{p}^hR$, we can lift $\eta^{(1)}$ to a sequence of idempotents $\eta^{(h)}$ in $R/\mathfrak{p}^hR$ for $h \geq 2$, such that the image of $\eta^{(h)}$ in $R/\mathfrak{p}^{h-1}R$ is always $\eta^{(h-1)}$. Taking the preimages of these idempotents in R, we obtain a $\mathfrak{p}R$-adic Cauchy sequence in R whose limit is the desired idempotent. □

The Idempotent Lifting Theorem appears to be folklore. Its consequences for the lifting of projective modules are due to Nakayama, Reiner and Swan – see [Curtis & Reiner 1966] §77.

We remind the reader that units can also be lifted ([BK: IRM] (4.3.25)).

7.2.9 Lemma

Let R be an $\widehat{\mathcal{O}}$-order, where $\widehat{\mathcal{O}}$ is a complete valuation ring. Then x is a unit of R if and only if its residue $\overline{x}$ is a unit in $R/\operatorname{rad}(R)$. □

7.2.10 Projective lifting

We next review some properties of irreducible modules that we need to establish the projective lifting property. For any ring R, a *representative set* of irreducible right R-modules is a set $\mathcal{I}(R) = \{I_j \mid j \in J\}$ of irreducible

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

(right) R-modules such that each irreducible (right) R-module is isomorphic to exactly one member of this set.

Let S be an Artinian semisimple ring. The Wedderburn-Artin Theorem ([BK: IRM] (4.2.3)) shows that

$$S = M_{n_1}(\mathcal{D}_1) \times \cdots \times M_{n_k}(\mathcal{D}_k)$$

for some division rings $\mathcal{D}_1, \ldots, \mathcal{D}_k$ and integers $n_1, \ldots, n_k$.

By [BK: IRM] (4.2.7), a representative set of irreducible S-modules is given by

$$\mathcal{I}(S) = \{I_1, \ldots, I_k\}$$

where $I_i = {}^{n_i}\mathcal{D}_i$ for $i = 1, \ldots, k$, and $I_i = \eta_i S$ for some idempotent η_i in S. Furthermore, any finitely generated right S-module is projective and can be expressed as

$$M \cong (I_1)^{h_1} \oplus \cdots \oplus (I_k)^{h_k}$$

for unique natural numbers $h_1, \ldots, h_k$ (some of which may be 0).

Now take R to semilocal, so that $R/\operatorname{rad}(R)$ is an Artinian semisimple ring. An irreducible R-module I has $I \cdot \operatorname{rad}(R) = 0$ (cf. [BK: IRM] (4.3.8)), and so is already an $R/\operatorname{rad}(R)$-module. Thus a representative set of irreducible R-modules is $\mathcal{I}(R) = \mathcal{I}(R/\operatorname{rad}(R))$.

We have the main result.

7.2.11 The Projective Lifting Theorem

Let R be a semiperfect ring and let M be a finitely generated $R/\operatorname{rad}(R)$-module. Then M can be lifted to a finitely generated projective R-module.

Moreover, for an arbitrary ring R, any such lifting, if it exists, is unique up to isomorphism.

Proof

First, any irreducible module I_i can be lifted – we have $I_i = \eta_i(R/\operatorname{rad}(R))$ and the idempotent η_i can be lifted to an idempotent ϵ_i of R, since R is semiperfect. Thus $P_i = \epsilon_i R$ is a projective module that lifts I_i. It is now clear that an arbitrary finitely generated $R/\operatorname{rad}(R)$-module M lifts to the finitely generated projective R-module

$$P = (P_1)^{h_1} \oplus \cdots \oplus (P_k)^{h_k}$$

in which the exponents $h_1, \ldots, h_k$ are those occurring in the decomposition of M into irreducible modules.

Now let R be an arbitrary ring, and suppose that P and Q are both projective liftings of M, that is,

$$P/P \cdot \mathrm{rad}(R) \cong M \cong Q/Q \cdot \mathrm{rad}(R).$$

Let π and ω be the canonical surjections of P to $P/P \cdot \mathrm{rad}(R)$ and Q to $Q/Q \cdot \mathrm{rad}(R)$ respectively, and let $\gamma : P/P \cdot \mathrm{rad}(R) \to Q/Q \cdot \mathrm{rad}(R)$ be the isomorphism implicit above. Since Q is projective, there is an R-module homomorphism θ from Q to P with $\gamma\pi\theta = \omega$ ([BK: IRM] (2.5.4)). It follows that $P = \theta Q + P \cdot \mathrm{rad}(R)$. Since P is finitely generated, Nakayama's Lemma ([BK: IRM] (4.3.10)) gives $P = \theta Q$. Because P is projective, $Q \cong P \oplus K$, where K is $\mathrm{Ker}\,\theta$. Then

$$P/P \cdot \mathrm{rad}(R) \oplus K/K \cdot \mathrm{rad}(R) \cong Q/Q \cdot \mathrm{rad}(R),$$

from which $K/K \cdot \mathrm{rad}(R) = 0$, and so $K = 0$ by Nakayama again. □

This result gives a description of all finitely generated projective modules over R.

7.2.12 Theorem

Let R be a semiperfect ring, let $I_1, \dots, I_k$ be a representative set of irreducible right R-modules, and for each i let P_i be a projective R-module that lifts I_i.

Let P be a finitely generated projective R-module. Then there exist unique non-negative integers $h_1, \dots, h_k$ with

$$P \cong (P_1)^{h_1} \oplus \cdots \oplus (P_k)^{h_k}.$$

Proof

Choose the integers $h_1, \dots, h_k$ to be those occurring in the irreducible decomposition of $P/P \cdot \mathrm{rad}(R)$. Then both sides of the isomorphism above are projective modules that lift $P/P \cdot \mathrm{rad}(R)$. □

7.2.13 Functoriality of lifting

Although we are able to lift projective modules from $R/\mathrm{rad}(R)$ over R, in general we are not able to define a functorial lifting from $\mathcal{P}_{R/\mathrm{rad}(R)}$ to $\mathcal{P}_R$. The problem lies with the lifting of homomorphisms, which cannot be done unless the ring surjection from R to $R/\mathrm{rad}(R)$ is split (as a ring homomorphism).

To see this, suppose that there is an additive functor L from $\mathcal{P}_{R/\mathrm{rad}(R)}$ to $\mathcal{P}_R$ such that the composition $(- \otimes_R R/\mathrm{rad}(R)) \circ L$ is (naturally equivalent to)

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

the identity functor on $\mathcal{P}_{R/\operatorname{rad}(R)}$. Such a functor lifts isomorphic $R/\operatorname{rad}(R)$-modules to isomorphic R-modules.

Then $L(R/\operatorname{rad}(R)) = R$. Also, each element x of the ring $R/\operatorname{rad}(R)$ acts as an endomorphism of $R/\operatorname{rad}(R)$ by left multiplication, and so must lift to an element $L(x)$ of $\operatorname{End}(R_R) = R$. Thus L induces a ring homomorphism from $R/\operatorname{rad}(R)$ to R which is necessarily a splitting of the canonical projection.

There are of course circumstances in which there is such a splitting. For example, take R to be the ring of $n \times n$ matrices over the formal power series ring $\mathcal{K}[[T]]$ where $\mathcal{K}$ is a field; the radical of R is evidently TR and R is T-adically complete. Any homomorphism between $M_n(\mathcal{K})$-modules can be represented as a matrix over $\mathcal{K}$, which is its own lifting.

7.2.14 Indecomposable modules

For the moment, take R to be an arbitrary ring. An R-module M is said to be *indecomposable* if it cannot be written as a direct sum $M \cong L \oplus N$ with L and N both nonzero R-modules. A *representative set* of indecomposable finitely generated projective R-modules is a set $\operatorname{Ind}(R) = \{P_\lambda \mid \lambda \in \Lambda\}$, where Λ is some index set, with the following properties.

RSI1: each P_λ is indecomposable, finitely generated and projective;
RSI2: $P_\lambda \ncong P_\mu$ if $\lambda \neq \mu$;
RSI3: if P is any indecomposable finitely generated projective R-module, then $P \cong P_\lambda$ for a unique index λ.

The description of such a set of indecomposable projectives for a particular ring is of great interest. For example, if R is right Artinian and $\operatorname{Ind}(R) = \{R\}$, then we know that every finitely generated projective R-module is free. (In [Bass 1963], it is shown that, under mild conditions on R, infinitely generated projective R-modules are always free. This holds, for example, when R is Noetherian.)

When R is Artinian semisimple, we know from the results quoted above that $\operatorname{Ind}(R)$ is the same as $\mathcal{I}(R)$, the representative set of irreducible R-modules. We have also shown that, for a semiperfect ring R, $\operatorname{Ind}(R) = \{P_1, \ldots, P_k\}$ where P_i lifts the irreducible module I_i. Note that

$$\mathcal{I}(R) = \mathcal{I}(R/\operatorname{rad}(R)) = \{I_1, \ldots, I_k\}.$$

Exercises

7.2.1 Let R be a semiperfect ring. Show that the ring of $n \times n$ matrices over R is also semiperfect.

Hint. Part (iv) of (4.2.7).

7.2.2 Idempotents ϵ, ϵ' of a ring T are said to be *orthogonal* if $\epsilon\epsilon' = \epsilon'\epsilon = 0$.

Show that the following hold for a semiperfect ring R.

(i) If ϵ and ϵ' are orthogonal idempotents of $R/\operatorname{rad}(R)$ and η is some idempotent lifting of ϵ, then ϵ' can be lifted to an idempotent η' orthogonal to η.

(ii) Any finite set $\{\epsilon_1, \ldots, \epsilon_t\}$ of pairwise orthogonal idempotents in $R/\operatorname{rad}(R)$ can be lifted to a set $\{\eta_1, \ldots, \eta_t\}$ of pairwise orthogonal idempotents in R.

(iii) Any set of $n \times n$ matrix units in $R/\operatorname{rad}(R)$ can be lifted into R.

7.2.3 An idempotent is said to be *primitive* if it cannot be expressed non-trivially as a sum of orthogonal idempotents.

Show that η is primitive if and only if $\eta R \eta$ is a local ring.

Deduce that if R is a semiperfect ring with $R/\operatorname{rad}(R) = M_n(\mathcal{D})$, where $\mathcal{D}$ is a division ring, then $R \cong M_n(T)$, where T is a local ring with $T/\operatorname{rad}(T) = \mathcal{D}$.

7.2.4 Let $T = \begin{pmatrix} R & M \\ 0 & S \end{pmatrix}$ be a triangular matrix ring. Show that T is semiperfect if and only if both R and S are semiperfect.

7.2.5 This exercise is a continuation of Exercises 6.2.4 and 6.2.5 of [BK: IRM], and it relates to Exercises 4.1.7 and 4.2.12 in this volume.

Let $\mathcal{O}$ be a complete 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 in $M_2(\mathcal{O})$ consisting of those matrices with 1,2 entry belonging to $\mathfrak{p}^h$, where $h = 0, 1, \ldots$ is a fixed integer.

Verify that

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

and that

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

Show that, up to isomorphism, the only indecomposable finitely generated projective right R-modules are $\begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}$ and $\begin{pmatrix} \mathfrak{p}^h \\ \mathcal{O} \end{pmatrix}$, and that these are not isomorphic for $h \geq 1$. Deduce that $\operatorname{rad}(R)$ is left and right R-projective if and only if $h = 0, 1$.

Generalize the results to the case where

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

consists of the $n \times n$ matrices with entries above the diagonal belonging to $\mathfrak{p}^h$.

Remark. When $h = 0$, R is a maximal order; when $h = 0, 1$, R is a hereditary order (see (7.3.30)).

7.2.6 Let $\mathcal{O}$ be a complete valuation ring with maximal ideal $\mathfrak{p}$, and let R be an $\mathcal{O}$-order. Give a direct proof of (7.2.9): x in R is a unit if and only if the image of x is a unit in $R/\operatorname{rad}(R)$.

7.3 LOCAL-GLOBAL METHODS FOR ORDERS

The results of the previous section provide a good description of the projective modules over a semiperfect ring. The next step in the programme of understanding projective modules in general is to ask whether a given ring R is related to a set of semiperfect rings so as to enable information on projective R-modules to be extracted from information about the projective modules over the associated semiperfect rings.

In general, there seems little chance of finding a useful connection between a given ring and a set of semiperfect rings, but there is one outstanding circumstance in which such a connection can be made, namely, when R is an order over a Dedekind domain $\mathcal{O}$. This is a situation of great interest in number theory and in representation theory.

For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, let $\widehat{\mathcal{O}}_{\mathfrak{p}}$ be the completion of $\mathcal{O}$ at $\mathfrak{p}$, and write $\widehat{R}_{\mathfrak{p}} = \widehat{\mathcal{O}}_{\mathfrak{p}} \otimes_{\mathcal{O}} R$. Then $\widehat{R}_{\mathfrak{p}}$ is an $\widehat{\mathcal{O}}_{\mathfrak{p}}$-order, and so a semiperfect ring (7.2.8). The results of the previous section, in particular (7.2.12), nicely describe the finitely generated projective $\widehat{R}_{\mathfrak{p}}$-modules, whatever the choice of $\mathfrak{p}$. It is therefore natural to ask if this 'local' information can be pieced together to give a solution to the 'global' problem of determining the finitely generated projective R-modules.

7.3.1 Lattices

Throughout this section, $\mathcal{O}$ is a Dedekind domain with field of fractions $\mathcal{K}$, and R is an $\mathcal{O}$-order. Recall that this means that $\mathcal{O}$ is contained in the centre of the ring R, and that R is finitely generated and torsion-free as a (balanced) $\mathcal{O}$-module.

A right *R-lattice* is a finitely generated right R-module which is torsion-free as a (balanced) $\mathcal{O}$-module. A left R-lattice is defined similarly. Unless otherwise stated, we work with right lattices, leaving the left-hand versions of our definitions and results to the reader. However, we sometimes allow $\mathcal{O}$ to act on the left, since we may view any $\mathcal{O}$-module as a balanced module.

Interpreting the definition for $\mathcal{O}$ itself, an $\mathcal{O}$-lattice is the same thing as a finitely generated torsion-free $\mathcal{O}$-module, or alternatively, a finitely generated projective $\mathcal{O}$-module ([BK: IRM] (6.3.4)). Since the field of fractions $\mathcal{K}$ of $\mathcal{O}$ is flat as an $\mathcal{O}$-module, we can regard an R-lattice L as an $\mathcal{O}$-submodule of $\mathcal{K} \otimes_{\mathcal{O}} L$, which, after (3.3.9), we write as $\mathcal{K}L$.

It is customary to refer to $\mathcal{O}$-lattices simply as *lattices* if there is no fear of confusion.

Although an $\mathcal{O}$-lattice is a finitely generated projective module under another name, this does not mean that the theory of lattices is the same as the theory of modules. In lattice theory, we are also concerned with the position of the lattice inside its ambient space $\mathcal{K}L$ and the relationships between several lattices in the same space.

The order R itself is an R-lattice and so an $\mathcal{O}$-lattice, and any (left or right) R-lattice is automatically $\mathcal{O}$-torsion-free and hence $\mathcal{O}$-projective. Conversely, a finitely generated projective $\mathcal{O}$-module which admits an R-module structure must be an R-lattice.

For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the ring of fractions $\mathcal{O}_{\mathfrak{p}}$ is a flat $\mathcal{O}$-module, and so we can identify the localization $L_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} L$ with the product $\mathcal{O}_{\mathfrak{p}}L$, computed inside $\mathcal{K}L$. Note that $\mathcal{K}L$ is a module over the Artinian ring $\mathcal{K}R$, and that $\mathcal{O}_{\mathfrak{p}}L$ is an $R_{\mathfrak{p}}$-lattice, where $R_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}R$ is an $\mathcal{O}_{\mathfrak{p}}$-order.

7.3.2 Full lattices

For the time being, we work only with $\mathcal{O}$-lattices, so we omit the reference to the Dedekind domain $\mathcal{O}$.

Let V be a fixed finite-dimensional vector space over the field of fractions $\mathcal{K}$ of $\mathcal{O}$. A lattice L is said to be a *full lattice in V* if L is an $\mathcal{O}$-submodule of V and L spans V, that is, $\mathcal{K}L = V$.

There are many full lattices in V; for example, take any K-basis $\{e_1, \dots, e_s\}$ of V and put $L = \mathcal{O}e_1 \oplus \cdots \oplus \mathcal{O}e_s$.

It will be convenient to define a *reference lattice* $\mathcal{O}^s$ in V by fixing one such basis $\{e_1, \dots, e_s\}$ of V and writing $\mathcal{O}^s = \mathcal{O}e_1 \oplus \cdots \oplus \mathcal{O}e_s$. Thus in this context, $\mathcal{O}^s$ no longer denotes an 'abstract' free module, but instead a free module with a prescribed basis.

The next result gives a criterion for an $\mathcal{O}$-submodule of V to be a full lattice.

7.3.3 The Comparison Lemma

Let L be a full lattice in the finite-dimensional $\mathcal{K}$-space V and suppose that M is an $\mathcal{O}$-submodule of V.

Then the following statements are equivalent.

(i) *M is a full lattice in V;*

(ii) *there are nonzero elements $a, b \in \mathcal{O}$ with $aL \subseteq M \subseteq b^{-1}L$;*

(iii) *there are nonzero elements $a, b \in \mathcal{K}$ with $aL \subseteq M \subseteq b^{-1}L$.*

Proof

(i) $\Rightarrow$ (ii) Since M spans V, we can find a $\mathcal{K}$-basis $\{e_1, \dots, e_s\}$ of V whose members belong to M. Write the generators of L as $\mathcal{K}$-linear combinations of $\{e_1, \dots, e_s\}$ and put all the elements of $\mathcal{K}$ that occur as coefficients over a (nonzero) common denominator $a \in \mathcal{O}$; then $aL \subseteq M$. Reversing the argument, we get $bM \subseteq L$ for some nonzero $b \in \mathcal{O}$.

(ii) $\Rightarrow$ (iii) Obvious.

(ii) $\Rightarrow$ (i) Since $\mathcal{O}$ is a Noetherian ring, the inclusion $M \subseteq b^{-1}L$ shows that M must be a finitely generated torsion-free $\mathcal{O}$-module. The inclusion $aL \subseteq M$ guarantees that M is full. □

7.3.4 Corollary

Let L and M be full lattices in the same space V. Then $L_\mathfrak{p} = M_\mathfrak{p}$ for almost all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.

Proof

We have $aL \subseteq M \subseteq bL$ for some $a, b \in \mathcal{K}$. The fractional ideals $a\mathcal{O}$ and $b\mathcal{O}$ can have only a finite number of prime ideals $\mathfrak{p}$ as nontrivial factors, and so both a and b are units in almost all localizations $\mathcal{O}_\mathfrak{p}$. □

7.3.5 An anonymous invariant

In order to compare two full lattices in a given space, we introduce an invariant which turns out to be a fractional ideal of $\mathcal{O}$. Given two full lattices L and

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

M in the space V, we define

$$\mathfrak{n}(L, M) = \{k \in \mathcal{K} \mid kL \subseteq M\}.$$

This invariant does not appear to have been given a name in the literature, and we do not propose to introduce one here. The notation has been prompted by the fact that $\mathfrak{n}(L, M)$ is the annihilator of the $\mathcal{O}$-module L/M when M is contained in L.

If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}$, then $L_{\mathfrak{p}}$ and $M_{\mathfrak{p}}$ are full $\mathcal{O}_{\mathfrak{p}}$-lattices in V and we have

$$\mathfrak{n}(L_{\mathfrak{p}}, M_{\mathfrak{p}}) = \{k \in \mathcal{K} \mid kL_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}\}.$$

The basic properties of this invariant are given in the next result.

7.3.6 Theorem

Suppose that V is a vector space over the field of fractions $\mathcal{K}$ of a Dedekind domain $\mathcal{O}$, of finite dimension s. Let L and M be any full lattices in V, and let $\mathcal{O}^s$ be a reference lattice in V.

Then the following assertions hold.

(i) $\mathfrak{n}(a\mathcal{O}^s, b\mathcal{O}^s) = a^{-1}b\mathcal{O}$ *for any nonzero elements a, b in $\mathcal{K}$.*
(ii) $\mathfrak{n}(L, M)$ *is a fractional ideal of $\mathcal{O}$.*
(iii) $\mathfrak{n}(L, L) = \mathcal{O}$.
(iv) $\mathfrak{n}(L, xL) = x\mathcal{O}$ *for any nonzero $x \in \mathcal{K}$.*
(v) $\mathfrak{n}(L_{\mathfrak{p}}, M_{\mathfrak{p}}) = \mathfrak{n}(L, M)_{\mathfrak{p}}$ *for all nonzero primes $\mathfrak{p}$ of $\mathcal{O}$.*
(vi) $\mathfrak{n}(L, M) = \prod_{\mathfrak{p}} \mathfrak{n}(L_{\mathfrak{p}}, M_{\mathfrak{p}})$.

Proof

(i) This follows from the fact that $\mathcal{O}^s = \mathcal{O}e_1 \oplus \cdots \oplus \mathcal{O}e_s$ where $\{e_1, \ldots, e_s\}$ is a $\mathcal{K}$-basis of V.

(ii) It is easy to check that $\mathfrak{n}(L, M)$ is a nonzero $\mathcal{O}$-submodule of $\mathcal{K}$. To see that it is a fractional ideal, take nonzero elements a and b of $\mathcal{K}$ with $a\mathcal{O}^s \subseteq L$ and $M \subseteq b\mathcal{O}^s$; such elements exist by the Comparison Lemma (7.3.3). Then

$$\mathfrak{n}(L, M) \subseteq \mathfrak{n}(a\mathcal{O}^s, b\mathcal{O}^s) = a^{-1}b\mathcal{O},$$

which shows that $\mathfrak{n}$ is a finitely generated module over the Noetherian ring $\mathcal{O}$ and hence that $\mathfrak{n}$ is, by definition (2.3.20), a fractional ideal.

(iii) Evidently, $\mathcal{O} \subseteq \mathfrak{n}(L, L)$. If this is an inequality, then $\mathfrak{p}^{-1} \subseteq \mathfrak{n}(L, L)$ for some nonzero prime ideal $\mathfrak{p}$ ([BK: IRM] (5.1.19)). Thus $L \subseteq \mathfrak{p}L$ and hence $L \subseteq \bigcap_i \mathfrak{p}^i L$. But this is impossible for the reference lattice, as $\bigcap_i \mathfrak{p}^i = 0$ in $\mathcal{O}$, and so it is also impossible for an arbitrary full lattice L, since $a\mathcal{O}^s \subseteq L \subseteq b\mathcal{O}^s$ for some nonzero a, b.

(iv) This is clear from (iii).

(v) Obviously, $\mathfrak{n}(L, M)_{\mathfrak{p}} \subseteq \mathfrak{n}(L_{\mathfrak{p}}, M_{\mathfrak{p}})$. For the reverse inclusion, take $x \in \mathfrak{n}(L_{\mathfrak{p}}, M_{\mathfrak{p}})$ and let $\{\ell_1, \ldots, \ell_t\}$ be a set of generators for L. Then for each i we have $x\ell_i = m_i/a_i$ with m_i in M and $a_i \in \mathcal{O}\backslash\mathfrak{p}$. Taking $a = a_1 \cdots a_t \in \mathcal{O}\backslash\mathfrak{p}$, we get $ax \in \mathfrak{n}(L, M)$ and so $x \in \mathfrak{n}(L, M)_{\mathfrak{p}}$.

(vi) This follows by applying the Unique Factorization Theorem for ideals in $\mathcal{O}$ (2.3.20 – A) to (v), since $\mathfrak{q}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ if $\mathfrak{q}$ is a nonzero maximal ideal different from $\mathfrak{p}$. □

We use the invariant to show that a lattice can be recovered from its localizations.

7.3.7 Proposition

For any lattice L, we have $L = \bigcap_{\mathfrak{p}} L_{\mathfrak{p}}$, the intersection being taken over all nonzero primes $\mathfrak{p}$ of $\mathcal{O}$.

Proof

Let V be the $\mathcal{K}$-space spanned by L. First, consider a reference lattice $\mathcal{O}^s = \mathcal{O}e_1 \oplus \cdots \oplus \mathcal{O}e_s$ for V. At each $\mathfrak{p}$,

$$(\mathcal{O}^s)_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}e_1 \oplus \cdots \oplus \mathcal{O}_{\mathfrak{p}}e_s.$$

By [BK: IRM] (6.2.7), $\mathcal{O} = \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$, from which we see that $\mathcal{O}^s = \bigcap_{\mathfrak{p}}(\mathcal{O}^s)_{\mathfrak{p}}$.

Now choose nonzero $a, b \in \mathcal{K}$ with $a\mathcal{O}^s \subseteq L \subseteq b\mathcal{O}^s$, using the Comparison Lemma (7.3.3). Put $L' = \bigcap_{\mathfrak{p}} L_{\mathfrak{p}}$, which is again an $\mathcal{O}$-module. Since $a(\mathcal{O}^s)_{\mathfrak{p}} \subseteq L_{\mathfrak{p}} \subseteq b(\mathcal{O}^s)_{\mathfrak{p}}$ for all $\mathfrak{p}$, we have $a\mathcal{O}^s \subseteq L' \subseteq b\mathcal{O}^s$ by the previous case. Again appealing to the Comparison Lemma, we see that L' is in fact a lattice.

Now $L \subseteq L'$, and for any prime ideal $\mathfrak{p}$ we have $L' \subseteq L_{\mathfrak{p}}$; thus $L_{\mathfrak{p}} \subseteq L'_{\mathfrak{p}} \subseteq (L_{\mathfrak{p}})_{\mathfrak{p}} = L_{\mathfrak{p}}$, that is, $L_{\mathfrak{p}} = L'_{\mathfrak{p}}$ for all $\mathfrak{p}$. Part (vi) of the preceding result gives $\mathfrak{n}(L', L) = \mathcal{O}$ and hence $L' = L$. □

As we saw in (7.3.4), any two full lattices L and M in the same space V must have identical localizations for all except a finite set of primes. The next result is complementary to this observation, since it tells us that we can vary the localization in any way we wish, provided we make only a finite number of changes.

7.3.8 Proposition

Let L be a full lattice in the finite-dimensional vector space V, and suppose that

(i) *$M(\mathfrak{p})$ is a full $\mathcal{O}_{\mathfrak{p}}$-lattice in V for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, and*

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

(ii) $M(\mathfrak{p}) = L_\mathfrak{p}$ *for almost all* $\mathfrak{p}$.

Then $M = \bigcap_\mathfrak{p} M(\mathfrak{p})$ *is a full* $\mathcal{O}$*-lattice in* V *such that* $M_\mathfrak{p} = M(\mathfrak{p})$ *for all* $\mathfrak{p}$.

Proof

Let $\mathbf{Q}$ be the finite set of primes at which $M(\mathfrak{p})$ and $L_\mathfrak{p}$ differ. At each $\mathfrak{q}$ in $\mathbf{Q}$, we can choose a nonzero element $a(\mathfrak{q})$ of $\mathcal{O}_\mathfrak{q}$ with $a(\mathfrak{q})M(\mathfrak{q}) \subseteq L_\mathfrak{q}$, by using the Comparison Lemma (7.3.3) over the local Dedekind domain $\mathcal{O}_\mathfrak{q}$. We can in fact choose $a(\mathfrak{q})$ to be in $\mathcal{O}$. To see this, write $a(\mathfrak{q}) = x(\mathfrak{q})y(\mathfrak{q})^{-1}$ with $x(\mathfrak{q}) \in \mathcal{O}$ and $y(\mathfrak{q}) \in \mathcal{O}\backslash\mathfrak{q}$. Then $x(\mathfrak{q})M(\mathfrak{q}) \subseteq y(\mathfrak{q})L_\mathfrak{q} = L_\mathfrak{q}$, so we can omit the factor $y(\mathfrak{q})$.

Now put $a = \prod_\mathbf{Q} a(\mathfrak{q})$. Then, for all $\mathfrak{p}$, $aM(\mathfrak{p}) \subseteq L_\mathfrak{p}$, and hence

$$aM = a\left(\bigcap_\mathfrak{p} M(\mathfrak{p})\right) = \bigcap_\mathfrak{p} aM(\mathfrak{p}) \subseteq \bigcap_\mathfrak{p} L_\mathfrak{p} = L.$$

Similarly, we can find some nonzero b in $\mathcal{O}$ with $bL \subseteq M$, which shows M to be a lattice by the Comparison Lemma again.

We have to show that $M_\mathfrak{q} = M(\mathfrak{q})$ for any $\mathfrak{q}$, (regardless of whether or not $\mathfrak{q}$ is in $\mathbf{Q}$). It is immediate from the definition of M that $M_\mathfrak{q} \subseteq M(\mathfrak{q})_\mathfrak{q} = M(\mathfrak{q})$.

To establish the reverse inclusion, choose a set of generators $m_1, \ldots, m_t$ of M as an $\mathcal{O}$-module. Given $x \in M(\mathfrak{q})$, the equality $\mathcal{K}M = V = \mathcal{K}M(\mathfrak{q})$ shows that $x = k_1m_1 + \cdots + k_tm_t$ for some $k_i \in \mathcal{K}$. By the Strong Approximation Theorem (7.1.18), there are elements $\ell_i \in \mathcal{K}$ for $1 \leq i \leq t$ with $\ell_i - k_i \in \mathcal{O}_\mathfrak{q}$ and $\ell_i \in \mathcal{O}_\mathfrak{p}$ for all $\mathfrak{p} \neq \mathfrak{q}$.

Put $x' = \ell_1m_1 + \cdots + \ell_tm_t$. For $\mathfrak{p} \neq \mathfrak{q}$, we have $x' \in M_\mathfrak{p} \subseteq M(\mathfrak{p})$, while

$$x' - x = (\ell_1 - k_1)m_1 + \cdots + (\ell_t - k_t)m_t \in M_\mathfrak{q},$$

and so $x' \in M(\mathfrak{q})$ also.

Thus $x' \in M$, which shows that

$$x = x' + (x - x') \in M_\mathfrak{q}.$$

□

The previous results have an interesting interpretation for $\mathcal{O}$-orders that allows the construction of orders with specified local properties. This exploits the fact that an $\mathcal{O}$-order is a lattice which is also a ring whose centre contains $\mathcal{O}$. The proofs are left to the reader; the only extra information required is that an intersection of subrings of a ring is again a ring.

7.3.9 Theorem

Let R *be an* $\mathcal{O}$*-order which spans the Artinian ring* $\mathcal{K}R$.

(a) *For each nonzero prime ideal* $\mathfrak{p}$ *of* $\mathcal{O}$, $R_\mathfrak{p}$ *is an* $\mathcal{O}_\mathfrak{p}$*-order which spans* $\mathcal{K}R$, *and* $R = \bigcap_\mathfrak{p} R_\mathfrak{p}$.

(b) *Given a collection of $\mathcal{O}_\mathfrak{p}$-orders $S(\mathfrak{p})$ such that*

(i) *$S(\mathfrak{p})$ spans $\mathcal{K}R$ for all $\mathfrak{p}$, and*

(ii) *$S(\mathfrak{p}) = R_\mathfrak{p}$ for almost all $\mathfrak{p}$,*

then $S = \bigcap_\mathfrak{p} S(\mathfrak{p})$ is an $\mathcal{O}$-order which spans $\mathcal{K}R$ and has $S_\mathfrak{p} = S(\mathfrak{p})$ for all $\mathfrak{p}$. □

7.3.10 Completions of lattices

We next consider the relationship between local lattices and complete lattices, that is, between lattices over the ring of fractions $\mathcal{O}_\mathfrak{p}$ and lattices over the completion $\widehat{\mathcal{O}}_\mathfrak{p}$, where $\mathfrak{p}$ is a given nonzero prime ideal of the Dedekind domain $\mathcal{O}$.

By (6.2.8) of [BK: IRM] and (7.1.14) of this book respectively, both $\mathcal{O}_\mathfrak{p}$ and $\widehat{\mathcal{O}}_\mathfrak{p}$ are local principal ideal domains, that is, valuation rings, and we can choose a uniformizing parameter p in $\mathcal{O}_\mathfrak{p}$ which generates the unique maximal ideal of either ring. Further, we can identify the field of fractions $\widehat{\mathcal{K}}_\mathfrak{p}$ of $\widehat{\mathcal{O}}_\mathfrak{p}$ as the product $\widehat{\mathcal{O}}_\mathfrak{p}\mathcal{K} = \widehat{\mathcal{O}}_\mathfrak{p} \otimes_\mathcal{O} \mathcal{K}$ by (7.1.22).

Given a vector space V of finite dimension s over the field of fractions $\mathcal{K}$ of $\mathcal{O}_\mathfrak{p}$, we write $\widehat{V}_\mathfrak{p} = \widehat{\mathcal{O}}_\mathfrak{p} \otimes_\mathcal{O} V$, which is a space over $\widehat{\mathcal{K}}_\mathfrak{p}$ of the same dimension s. Similarly, given a full lattice $L_\mathfrak{p}$ in V, we put $\widehat{L}_\mathfrak{p} = \widehat{\mathcal{O}}_\mathfrak{p} \otimes_\mathcal{O} L_\mathfrak{p}$. We write these expressions in the abbreviated forms $\widehat{V}_\mathfrak{p} = \widehat{\mathcal{O}}_\mathfrak{p}V$ and $\widehat{L}_\mathfrak{p} = \widehat{\mathcal{O}}_\mathfrak{p}L_\mathfrak{p}$, which is permissible by (3.3.9) since $\widehat{\mathcal{O}}_\mathfrak{p}$ is flat as an $\mathcal{O}$-module (7.1.24).

Since a lattice over either $\mathcal{O}_\mathfrak{p}$ or $\widehat{\mathcal{O}}_\mathfrak{p}$ is necessarily a free module ([BK: IRM] (6.3.24)), $\widehat{L}_\mathfrak{p}$ is clearly a full $\widehat{\mathcal{O}}_\mathfrak{p}$-lattice in $\widehat{V}_\mathfrak{p}$. We now show that any full lattice in $\widehat{V}_\mathfrak{p}$ arises in this way.

7.3.11 Proposition

Let M be a full $\widehat{\mathcal{O}}_\mathfrak{p}$-lattice in $\widehat{V}_\mathfrak{p}$. Then

(i) *M has an $\widehat{\mathcal{O}}_\mathfrak{p}$-basis $\{f_1, \dots, f_s\} \subseteq V$;*

(ii) *$M = \widehat{\mathcal{O}}_\mathfrak{p}L_\mathfrak{p}$ where $L_\mathfrak{p} = \mathcal{O}_\mathfrak{p}f_1 \oplus \cdots \oplus \mathcal{O}_\mathfrak{p}f_s$;*

(iii) *$L_\mathfrak{p} = M \cap V$.*

Proof

Take any $\widehat{\mathcal{O}}_\mathfrak{p}$-basis $\{g_1, \dots, g_s\}$ of M and any $\mathcal{K}$-basis $\{h_1, \dots, h_s\}$ of V. Both of these are $\widehat{\mathcal{K}}_\mathfrak{p}$-bases of $\widehat{V}_\mathfrak{p}$, so by the usual change of basis argument (1.3.4), we may write

$$h_j = \sum_i g_i a_{ij}, \quad j = 1, \dots, s, \text{ with all } a_{ij} \in \widehat{\mathcal{K}}_\mathfrak{p}.$$

Let $A = (a_{ij})$, and choose a natural number w such that $p^w A \in M_s(\widehat{\mathcal{O}}_{\mathfrak{p}})$; this is possible by (vi) of (7.1.14).

Next, write $A^{-1} = (b_{ij}) \in M_s(\widehat{\mathcal{K}}_{\mathfrak{p}})$, and for each i, j, use the Strong Approximation Theorem (7.1.18) to choose an element $c_{ij} \in \mathcal{K}$ with

$$c_{ij} - b_{ij} \in p^{2w+1}\widehat{\mathcal{O}}_{\mathfrak{p}}.$$

Put $C = (c_{ij})$.

Then $C - A^{-1} \in p^{2w+1}M_s(\widehat{\mathcal{O}}_{\mathfrak{p}})$ and so $AC - I = X \in p^{w+1}M_s(\widehat{\mathcal{O}}_{\mathfrak{p}})$. Thus $AC = I + X$ is invertible in $M_s(\widehat{\mathcal{O}}_{\mathfrak{p}})$, with inverse given by the binomial expansion of $(I + X)^{-1}$.

Now let $f_k = \sum_j h_j c_{jk} \in V$ for $k = 1, \ldots, s$. Since C is invertible (over $\widehat{\mathcal{K}}_{\mathfrak{p}}$ and hence over $\mathcal{K}$), $\{f_1, \ldots, f_s\}$ is a $\mathcal{K}$-basis of V. But $f_k = \sum_i g_i(\sum_j a_{ij}c_{jk})$, so $\{f_1, \ldots, f_s\}$ must also be an $\widehat{\mathcal{O}}_{\mathfrak{p}}$-basis of M.

Finally, from part (viii) of (7.1.14),

$$M \cap V = \left(\bigoplus_k \widehat{\mathcal{O}}_{\mathfrak{p}} f_k\right) \cap \left(\bigoplus_k \mathcal{K} f_k\right) = \bigoplus_k (\widehat{\mathcal{O}}_{\mathfrak{p}} \cap \mathcal{K}) f_k = \bigoplus_k \mathcal{O}_{\mathfrak{p}} f_k = L_{\mathfrak{p}}.$$

□

The main result is as follows.

7.3.12 Theorem

Let $\mathfrak{p}$ be a nonzero prime ideal of a Dedekind domain $\mathcal{O}$, and let V be a finite-dimensional vector space over the field of fractions $\mathcal{K}$ of $\mathcal{O}$. Then there are mutually inverse, inclusion preserving, bijective correspondences between the set of full $\mathcal{O}_{\mathfrak{p}}$-lattices $L_{\mathfrak{p}}$ in V and the set of full $\widehat{\mathcal{O}}_{\mathfrak{p}}$-lattices M in $\widehat{V}_{\mathfrak{p}}$, given by

$$L_{\mathfrak{p}} \longleftrightarrow \widehat{L}_{\mathfrak{p}} = \widehat{\mathcal{O}}_{\mathfrak{p}} L_{\mathfrak{p}}$$

and

$$M \cap V \longleftrightarrow M.$$

Proof

Choose an $\mathcal{O}_{\mathfrak{p}}$-basis $\{e_1, \ldots, e_s\}$ of $L_{\mathfrak{p}}$. This is also a $\mathcal{K}$-basis of V and an $\widehat{\mathcal{O}}_{\mathfrak{p}}$-basis of $\widehat{L}_{\mathfrak{p}}$; hence

$$\widehat{L}_{\mathfrak{p}} \cap V = (\widehat{\mathcal{O}}_{\mathfrak{p}} \cap \mathcal{K})e_1 + \cdots + (\widehat{\mathcal{O}}_{\mathfrak{p}} \cap \mathcal{K})e_s.$$

But $\widehat{\mathcal{O}}_{\mathfrak{p}} \cap \mathcal{K} = \mathcal{O}_{\mathfrak{p}}$ by (viii) of (7.1.14), so that $\widehat{L}_{\mathfrak{p}} \cap V = L_{\mathfrak{p}}$.

It is clear from the preceding result that $M \cap V$ is a full lattice in V and that $(\widehat{M \cap V})_{\mathfrak{p}} = M$, which proves our assertions. □

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

Before we state the next result, a word on notation. Suppose that V is a given finite-dimensional $\mathcal{K}$-space and that we have a set $\{M(\mathfrak{p})\}$, where each $M(\mathfrak{p})$ is an $\widehat{\mathcal{O}}_\mathfrak{p}$-lattice in $\widehat{V}_\mathfrak{p}$ and $\mathfrak{p}$ varies through all the nonzero prime ideals of $\mathcal{O}$. We would like to work with the intersection $\bigcap_\mathfrak{p} M(\mathfrak{p})$, which we would expect to be an $\mathcal{O}$-lattice in V.

However, we are faced with a technical difficulty in forming the intersection, since, properly speaking, $\widehat{V}_\mathfrak{p} \cap \widehat{V}_\mathfrak{q} = \emptyset$ for any two distinct prime ideals $\mathfrak{p}$ and $\mathfrak{q}$. In fact, the method of construction of the completions $\widehat{\mathcal{O}}_\mathfrak{p}$ of $\widehat{\mathcal{O}}$ shows that $\widehat{\mathcal{O}}_\mathfrak{p} \cap \widehat{\mathcal{O}}_\mathfrak{q} = \emptyset$ already.

We get around the difficulty by using the canonical embedding $\iota_\mathfrak{p}$ of V in $\widehat{V}_\mathfrak{p}$ for each $\mathfrak{p}$. We form the intersection $\iota_\mathfrak{p} V \cap M(\mathfrak{p})$ in $\widehat{V}_\mathfrak{p}$, and define $V \cap M(\mathfrak{p})$ to be the inverse image $\iota_\mathfrak{p}^{-1}(\iota_\mathfrak{p} V \cap M(\mathfrak{p}))$. Then we can interpret the expression $V \cap (\bigcap_\mathfrak{p} M(\mathfrak{p}))$ as $\bigcap_\mathfrak{p}(V \cap M(\mathfrak{p}))$.

We can now extend (7.3.7), (7.3.8) and (7.3.9) to completions. The proofs are routine applications of the previous results.

7.3.13 Theorem

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $\mathcal{K}$, and let L be an $\mathcal{O}$-lattice which spans the finite-dimensional $\mathcal{K}$-space V. Let $\widehat{L}_\mathfrak{p} = \widehat{\mathcal{O}}_\mathfrak{p} \otimes_\mathcal{O} L$ for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$.

Suppose also that, for each $\mathfrak{p}$, $\widehat{M}(\mathfrak{p})$ is a full $\widehat{\mathcal{O}}_\mathfrak{p}$-lattice in $\widehat{V}_\mathfrak{p}$ and that $\widehat{M}(\mathfrak{p}) = \widehat{L}_\mathfrak{p}$ for almost all $\mathfrak{p}$.

Then

(i) $L = V \cap (\bigcap_\mathfrak{p} \widehat{L}_\mathfrak{p})$;

(ii) $M = V \cap (\bigcap_\mathfrak{p} \widehat{M}(\mathfrak{p}))$ *is a full $\mathcal{O}$-lattice in V with $\widehat{M}_\mathfrak{p} = \widehat{M}(\mathfrak{p})$ for all $\mathfrak{p}$.* □

7.3.14 Theorem

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $\mathcal{K}$, and let R be an $\mathcal{O}$-order which spans the Artinian ring $\mathcal{K}R$.

(a) *For each nonzero prime $\mathfrak{p}$ of $\mathcal{O}$, $\widehat{R}_\mathfrak{p} = \widehat{\mathcal{O}}_\mathfrak{p} R$ is an $\widehat{\mathcal{O}}_\mathfrak{p}$-order which spans the Artinian ring $\widehat{\mathcal{K}}_\mathfrak{p} R$, and $R = (\mathcal{K}R) \cap (\bigcap_\mathfrak{p} \widehat{R}_\mathfrak{p})$.*

(b) *Given a collection of $\widehat{\mathcal{O}}_\mathfrak{p}$-orders $\widehat{S}(\mathfrak{p})$ such that*

  (i) *$\widehat{S}(\mathfrak{p})$ spans $\widehat{\mathcal{K}}_\mathfrak{p} R$ for each $\mathfrak{p}$, and*

  (ii) *$\widehat{S}(\mathfrak{p}) = \widehat{R}_\mathfrak{p}$ for almost all $\mathfrak{p}$,*

  then $S = (\mathcal{K}R) \cap \bigcap_\mathfrak{p} \widehat{S}(\mathfrak{p})$ is an $\mathcal{O}$-order which spans $\mathcal{K}R$ and has $\widehat{S}_\mathfrak{p} = \widehat{S}(\mathfrak{p})$ for all $\mathfrak{p}$. □

7.3.15 Adèles for modules

The previous results can be reformulated in terms of adèles. Recall from (7.1.25) that the ring of adèles $A(\mathcal{O})$ of a Dedekind domain $\mathcal{O}$ is $A(\mathcal{O}) = \prod_{\mathfrak{p}} \widehat{\mathcal{O}}_{\mathfrak{p}}$, the direct product of the full set of completions $\widehat{\mathcal{O}}_{\mathfrak{p}}$ of $\mathcal{O}$, where $\mathfrak{p}$ runs through all the nonzero prime ideals of $\mathcal{O}$, and that $A(\mathcal{K}) = \mathcal{K} \otimes_{\mathcal{O}} A(\mathcal{O}) = \mathcal{K}A(\mathcal{O})$. Both $A(\mathcal{O})$ and $A(\mathcal{K})$ are commutative rings.

We extend this notation to $\mathcal{O}$-modules in general by defining

$$A(M) = M \otimes_{\mathcal{O}} A(\mathcal{O})$$

for any (right) $\mathcal{O}$-module M. There is a canonical homomorphism

$$\alpha_M : A(M) \longrightarrow \prod_{\mathfrak{p}} \widehat{M}_{\mathfrak{p}},$$

given by

$$\alpha_M(m \otimes (x_{\mathfrak{p}})) = (m \otimes x_{\mathfrak{p}}),$$

which is clearly natural for homomorphisms $M \to N$ of $\mathcal{O}$-modules. The properties of the canonical homomorphism depend on whether or not the module is finitely generated. The results which immediately follow deal with the case that the module is finitely generated, and subsequently we consider the situation where the module is a finite-dimensional space over the field of fractions of the Dedekind domain.

7.3.16 Proposition

Let M be a finitely generated $\mathcal{O}$-module. Then the canonical homomorphism $\alpha_M : A(M) \to \prod_{\mathfrak{p}} \widehat{M}_{\mathfrak{p}}$ is an isomorphism, where $\mathfrak{p}$ varies through the set of nonzero prime ideals of $\mathcal{O}$.

Proof

There is an internal direct sum decomposition $M = T(M) \oplus M'$ with $T(M)$ the torsion submodule of M and M' torsion-free (2.3.20). Thus it is enough to check the claim for each component $T(M)$ and M' separately.

By (7.1.27), there is a canonical isomorphism

$$A(\mathcal{O}) \otimes_{\mathcal{O}} T(M) \cong T(M),$$

which proves the assertion for $T(M)$ since any $\mathfrak{p}$-component of a finitely generated torsion module is already its own completion (7.1.23).

We may therefore suppose that M is torsion-free, that is, that M is a lattice. Then M is projective and so has the standard form $\mathcal{O}^{s-1} \oplus \mathfrak{a}$, with $\mathfrak{a}$ a fractional ideal of $\mathcal{O}$. Setting aside the free module case as straightforward, we have reduced to the case of a non-principal fractional ideal $\mathfrak{a}$.

We have to show that the homomorphism

$$\alpha_{\mathfrak{a}} : \mathfrak{a} \longrightarrow \prod_{\mathfrak{p}} \mathfrak{a}\widehat{\mathcal{O}}_{\mathfrak{p}}$$

is an isomorphism. It is evidently injective, since the homomorphism $\mathcal{K} \to A(\mathcal{K})$ is itself injective.

To see that $\alpha_{\mathfrak{a}}$ is surjective, for each member of the finite set $\mathbf{Q}$ of primes $\mathfrak{p}$ with $\widehat{\mathfrak{a}}_{\mathfrak{p}} \neq \widehat{\mathcal{O}}_{\mathfrak{p}}$, we use the surjectivity of the valuation

$$v_{\mathfrak{p}} : \mathcal{O} \longrightarrow \{0\} \cup \mathbb{N} \cup \{\infty\} \quad ([\text{BK : IRM}]\ (6.2.3))$$

to choose an element $x(\mathfrak{p}) \in \mathcal{O}$ with $v_{\mathfrak{p}}(x(\mathfrak{p})) = v_{\mathfrak{p}}(\mathfrak{a})$. Now define $x = \prod_{\mathfrak{p} \in \mathbf{Q}} x(\mathfrak{p})$, which is an element of $\mathfrak{a}$. Then $\widehat{\mathfrak{a}}_{\mathfrak{p}} = x(\mathfrak{p})\widehat{\mathcal{O}}_{\mathfrak{p}}$ for all $\mathfrak{p}$, and thus $\alpha_{\mathfrak{a}}(x)$ generates $\prod_{\mathfrak{p}} \widehat{\mathfrak{a}}_{\mathfrak{p}}$, proving $\alpha_{\mathfrak{a}}$ to be surjective. □

7.3.17 Corollary

$A(\mathcal{O})$ is a flat $\mathcal{O}$-module, and if R is any $\mathcal{O}$-order, then $A(R)$ is a flat R-module.

Proof

By (3.2.8), it suffices to show that if $\mu : M \to N$ is an injective $\mathcal{O}$-module homomorphism where M is a finitely generated $\mathcal{O}$-module, then the induced homomorphism $\mu \otimes id : A(M) \to A(N)$ is also injective. But in the commutative diagram

$$\begin{array}{ccc} A(M) & \xrightarrow{\mu \otimes id} & A(N) \\ \alpha_M \downarrow & & \downarrow \alpha_N \\ \prod_{\mathfrak{p}} \widehat{M}_{\mathfrak{p}} & \xrightarrow[\prod_{\mathfrak{p}} \mu \otimes id_{\mathfrak{p}}]{} & \prod_{\mathfrak{p}} \widehat{N}_{\mathfrak{p}} \end{array}$$

α_M is an isomorphism by the preceding result, while $\prod_{\mathfrak{p}}(\mu \otimes id)$ is injective since each ring $\widehat{\mathcal{O}}_{\mathfrak{p}}$ is flat as an $\mathcal{O}$-module (7.1.24).

Finally, since the functor $- \otimes_{\mathcal{O}} A(\mathcal{O}) : \mathcal{M}\text{OD}_{\mathcal{O}} \to \mathcal{M}\text{OD}_{\mathcal{O}}$ is exact, so too is the functor

$$- \otimes_R A(R) = - \otimes_R R \otimes_{\mathcal{O}} A(\mathcal{O}) : \mathcal{M}\text{OD}_R \longrightarrow \mathcal{M}\text{OD}_R. \qquad \square$$

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

7.3.18 Adèles for spaces

Let V be a finite-dimensional $\mathcal{K}$-space of dimension s. In contrast to the situation for $\mathcal{O}$-modules (7.3.16), the canonical homomorphism

$$\alpha_V : A(V) = A(\mathcal{O}) \otimes_{\mathcal{O}} V \longrightarrow \prod_{\mathfrak{p}} \widehat{V}_{\mathfrak{p}}$$

does not allow us to identify $A(V)$ with the direct product, since this identification does not hold for the field of fractions $\mathcal{K}$ itself (unless $\mathcal{O}$ has only a finite set of nonzero prime ideals). As we noted in (7.1.25), $A(\mathcal{K})$ is the restricted direct product of the set $\{\widehat{\mathcal{K}}_{\mathfrak{p}}\}$ with respect to $\{\widehat{\mathcal{O}}_{\mathfrak{p}}\}$; that is, $A(\mathcal{K})$ is the $A(\mathcal{O})$-submodule of $\prod_{\mathfrak{p}} \widehat{\mathcal{K}}_{\mathfrak{p}}$ consisting of those elements $x = (x_{\mathfrak{p}})$ with almost all $x_{\mathfrak{p}}$ in $\widehat{\mathcal{O}}_{\mathfrak{p}}$.

With this information, it is now straightforward to verify that $A(V)$ is isomorphic to the restricted direct product of the set $\{\widehat{V}_{\mathfrak{p}}\}$ with respect to $\{(\widehat{\mathcal{O}}_{\mathfrak{p}})^s\}$. In fact, since any two full lattices in V are locally identical for almost all primes, the set of lattices $\{(\widehat{\mathcal{O}}_{\mathfrak{p}})^s\}$ can be replaced by the set $\{\widehat{L}_{\mathfrak{p}}\}$ for any full lattice L in V.

Given a full lattice L in V, the identifications

$$V = \mathcal{K} \otimes_{\mathcal{O}} L = \mathcal{K}L$$

lead to canonical isomorphisms

$$A(V) \cong A(\mathcal{K}) \otimes_{\mathcal{K}} L \cong \mathcal{K} \otimes_{\mathcal{O}} A(L),$$

by means of the commutativity and associativity of the tensor product ((3.1.5) and (3.2.15)). We also regard these isomorphisms as identifications and write

$$A(V) = A(\mathcal{K})L = \mathcal{K}A(L)$$

if convenient. These equalities are validated by the observations that $A(\mathcal{K})$ is $\mathcal{K}$-flat (5.2.6), $\mathcal{K}$ is $\mathcal{O}$-flat (5.2.4), and hence $A(\mathcal{K})$ is $\mathcal{O}$-flat by (3.3.6). Note that $A(V)$ is a free module over $A(\mathcal{K})$, of rank s.

We can now interpret (i) of (7.3.13) in terms of pull-backs (Exercise 1.4.11).

7.3.19 Theorem

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $\mathcal{K}$ and let L be a full $\mathcal{O}$-lattice in the finite-dimensional $\mathcal{K}$-space V. Then there is a commutative

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

diagram of canonical injective $\mathcal{O}$-homomorphisms

$$\begin{array}{ccc} L & \longrightarrow & A(L) \\ \big\downarrow & & \big\downarrow \\ V & \longrightarrow & A(V) \end{array}$$

Furthermore, this square is a pull-back; that is, there is a canonical $\mathcal{O}$-module isomorphism $L \cong V \times_{A(V)} A(L)$. □

When L is the ring $\mathcal{O}$ itself, we recover the fact that

$$\mathcal{O} = \mathcal{K} \cap \left(\bigcap\nolimits_{\mathfrak{p}} \widehat{\mathcal{O}}_{\mathfrak{p}}\right) \cong \mathcal{K} \times_{A(\mathcal{K})} A(\mathcal{O}),$$

which follows from the equalities $\mathcal{O} = \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$ ([BK: IRM] (6.2.7)) and $\mathcal{O}_{\mathfrak{p}} = \mathcal{K} \cap \widehat{\mathcal{O}}_{\mathfrak{p}}$ ((viii) of (7.1.14)).

7.3.20 Lattices over orders

We return to the consideration of R-lattices over an $\mathcal{O}$-order R.

As we have already noted in (7.3.9) and (7.3.14), for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the localization $R_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} R$ and completion $\widehat{R}_{\mathfrak{p}} = \widehat{\mathcal{O}}_{\mathfrak{p}} \otimes_{\mathcal{O}} R$ are orders, over $\mathcal{O}_{\mathfrak{p}}$ and $\widehat{\mathcal{O}}_{\mathfrak{p}}$ respectively. Both R and $R_{\mathfrak{p}}$ span the $\mathcal{K}$-algebra $\mathcal{K}R$, which is Artinian since it has finite dimension over $\mathcal{K}$. The completion $\widehat{R}_{\mathfrak{p}}$ spans the algebra $\widehat{\mathcal{K}}_{\mathfrak{p}}R$, which is likewise Artinian. It follows that $A(R)$ is a ring with $\mathcal{K} \otimes_{\mathcal{O}} A(R) = A(\mathcal{K}R)$.

Suppose that L is an R-lattice. Then L is necessarily an $\mathcal{O}$-lattice, and for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the localization $L_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} L$ and completion $\widehat{L}_{\mathfrak{p}} = \widehat{\mathcal{O}}_{\mathfrak{p}} \otimes_{\mathcal{O}} L$ are lattices over $R_{\mathfrak{p}}$ and $\widehat{R}_{\mathfrak{p}}$ respectively. Thus $A(L)$ is an $A(R)$-module.

Also, $\mathcal{K}L$ is a finitely generated module over the Artinian ring $\mathcal{K}R$, and $A(\mathcal{K}L)$ is a finitely generated module over $A(\mathcal{K}R)$.

We record the following (amalgamated) extension of (7.3.7), (7.3.8) and (7.3.13) to R-lattices. We do not need to give any additional proof of the various equalities in the statement, since an R-lattice is an $\mathcal{O}$-lattice and we have already proved these results for $\mathcal{O}$-lattices. The only new observation required is that an intersection of a set of $R_{\mathfrak{p}}$-lattices or of $\widehat{R}_{\mathfrak{p}}$-lattices, where $\mathfrak{p}$ varies through the nonzero primes of $\mathcal{O}$, must be an R-module, and hence an R-lattice.

7.3.21 Theorem

Let R be an $\mathcal{O}$-order and let L be an R-lattice which spans the finitely generated $\mathcal{K}R$-module V.

Suppose also that, for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we are given an $R_\mathfrak{p}$-lattice $M(\mathfrak{p})$ and an $\widehat{R}_\mathfrak{p}$-lattice $N(\mathfrak{p})$, and that $M(\mathfrak{p}) = L_\mathfrak{p}$ for almost all $\mathfrak{p}$ and $N(\mathfrak{p}) = \widehat{L}_\mathfrak{p}$ for almost all $\mathfrak{p}$.

Then the following assertions hold.

(i) $L = \bigcap_\mathfrak{p} L_\mathfrak{p} = \bigcap_\mathfrak{p} \widehat{L}_\mathfrak{p}$.

(ii) $M = \bigcap_\mathfrak{p} M(\mathfrak{p})$ *is a full R-lattice in V with $M_\mathfrak{p} = M(\mathfrak{p})$ for all $\mathfrak{p}$.*

(iii) $N = V \cap (\bigcap_\mathfrak{p} N(\mathfrak{p}))$ *is a full R-lattice in V with $\widehat{N}_\mathfrak{p} = N(\mathfrak{p})$ for all $\mathfrak{p}$.* □

7.3.22 Projective modules

Let R be an $\mathcal{O}$-order, where $\mathcal{O}$ is a Dedekind domain, and let L be an R-lattice. Our aim is to show that L is projective over R precisely when each of its completions $\widehat{L}_\mathfrak{p}$ is $\widehat{R}_\mathfrak{p}$-projective.

We first need to know that homomorphisms behave well under localization, which fact is a consequence of a more general result.

7.3.23 Theorem

Let $\mathcal{O}$ be a Dedekind domain and let R be an $\mathcal{O}$-order. Suppose that S is a commutative ring extension of $\mathcal{O}$ and that S is flat as an $\mathcal{O}$-module.

Then, for any pair M, N of (right) R-modules with M finitely generated, there is a natural isomorphism

$$\lambda : S \otimes_\mathcal{O} \operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_{S\otimes_\mathcal{O} R}(S \otimes_\mathcal{O} M, S \otimes_\mathcal{O} N).$$

Proof

Clearly, $S \otimes_\mathcal{O} R$ is a ring and $S \otimes_\mathcal{O} M$ and $S \otimes_\mathcal{O} N$ are right $S \otimes_\mathcal{O} R$-modules, so the right-hand term above does exist.

For $s \in S$ and $\alpha \in \operatorname{Hom}(M, N)$, define

$$\lambda(s \otimes \alpha) : S \otimes_\mathcal{O} M \longrightarrow S \otimes_\mathcal{O} N$$

by

$$\lambda(s \otimes \alpha)(t \otimes m) = st \otimes \alpha(m), \quad \text{where } t \in S, m \in M.$$

It is easily verified that λ is a well-defined $S \otimes_\mathcal{O} R$-homomorphism.

To establish that λ is an isomorphism, we first show that there is an exact sequence of right R-module homomorphisms

$$R^m \xrightarrow{\psi} R^n \xrightarrow{\phi} M \longrightarrow 0$$

for some integers m and n.

Since M is finitely generated, we can find such a surjective homomorphism ϕ. Because R is Noetherian ([BK: IRM] (3.1.12)), $\operatorname{Ker}\phi$ is finitely generated, and so there is a surjection $\theta : R^m \to \operatorname{Ker}\phi$ for some m. Take ψ to be the composition of θ with the canonical inclusion.

By (2.1.4), there is an exact sequence of $\mathcal{O}$-modules

$$0 \longrightarrow \operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(R^n, N) \longrightarrow \operatorname{Hom}_R(R^m, N).$$

Since S is flat, this leads to a commutative diagram with exact rows (and with $\otimes$ denoting $\otimes_{\mathcal{O}}$ and T denoting $S \otimes_{\mathcal{O}} R$)

$$\begin{array}{ccccc} S\otimes \operatorname{Hom}_R(M,N) & \rightarrowtail & S\otimes \operatorname{Hom}_R(R^n,N) & \to & S\otimes \operatorname{Hom}_R(R^m,N) \\ \lambda \downarrow & & \lambda' \downarrow & & \lambda'' \downarrow \\ \operatorname{Hom}_T(S\otimes M, S\otimes N) & \rightarrowtail & \operatorname{Hom}_T(S\otimes R^n, S\otimes N) & \to & \operatorname{Hom}_T(S\otimes R^m, S\otimes N) \end{array}$$

in which the left-hand horizontal maps are inclusions and the vertical homomorphisms λ' and λ'' are defined in the same way as λ.

However, for any ring R and module N, $\operatorname{Hom}_R(R, N)$ is naturally isomorphic to N, since an R-homomorphism $\rho : R \to N$ is determined by $\rho(1)$, which can be any element of N. This gives a natural isomorphism $\operatorname{Hom}_R(R^n, N) \cong N^n$ and similarly a natural isomorphism

$$\operatorname{Hom}_{S\otimes R}((S \otimes R)^n, S \otimes N) \cong (S \otimes N)^n.$$

Therefore

$$S \otimes \operatorname{Hom}_R(R^n, N) \cong (S \otimes N)^n \cong \operatorname{Hom}_{S\otimes R}(S \otimes R^n, S \otimes N),$$

which shows λ' to be an isomorphism. Likewise, λ'' is an isomorphism, and hence λ must also be an isomorphism by the Five Lemma (2.3.23). □

7.3.24 Corollary

Let R be an $\mathcal{O}$-order and let M and N be R-modules with M finitely generated. Then the following hold.

(i) $\widehat{\mathcal{O}}_{\mathfrak{p}} \otimes_{\mathcal{O}} \operatorname{Hom}_R(M, N) \cong \operatorname{Hom}_{\widehat{R}_{\mathfrak{p}}}(\widehat{M}_{\mathfrak{p}}, \widehat{N}_{\mathfrak{p}})$ *for any nonzero prime ideal* $\mathfrak{p}$ *of* $\widehat{\mathcal{O}}$.

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

(ii) $A(\mathrm{Hom}_R(M,N)) \cong \mathrm{Hom}_{A(R)}(A(M), A(N))$.

(iii) *If also N is finitely generated, then*

$$A(\mathrm{Hom}_R(M,N)) \cong \prod_{\mathfrak{p}} \mathrm{Hom}_{\widehat{R}_{\mathfrak{p}}}(\widehat{M_{\mathfrak{p}}}, \widehat{N}_{\mathfrak{p}}),$$

the product being taken over all nonzero prime ideals of $\mathcal{O}$.

Proof

(i) and (ii) are immediate by (7.1.24) and (7.3.17), respectively, and (iii) by (7.3.16). □

7.3.25 Corollary

Let R be an $\mathcal{O}$-order and let

$$\mathbf{E} \qquad 0 \longrightarrow N' \xrightarrow{\ \alpha\ } N \xrightarrow{\ \beta\ } N'' \longrightarrow 0$$

be an exact sequence of R-modules with N'' finitely generated. Then the following are equivalent.

(i) $\mathbf{E}$ *is split.*

(ii) *For each prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the sequence*

$$\mathbf{E}_{\mathfrak{p}} \qquad 0 \longrightarrow N'_{\mathfrak{p}} \xrightarrow{\ \alpha_{\mathfrak{p}}\ } N_{\mathfrak{p}} \xrightarrow{\ \beta_{\mathfrak{p}}\ } N''_{\mathfrak{p}} \longrightarrow 0$$

is split exact.

(iii) *For each prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the sequence*

$$\widehat{\mathbf{E}}_{\mathfrak{p}} \qquad 0 \longrightarrow \widehat{N}'_{\mathfrak{p}} \xrightarrow{\ \widehat{\alpha}_{\mathfrak{p}}\ } \widehat{N}_{\mathfrak{p}} \xrightarrow{\ \widehat{\beta}_{\mathfrak{p}}\ } \widehat{N}''_{\mathfrak{p}} \longrightarrow 0$$

is split exact.

(iv) *The sequence*

$$A(\mathbf{E}) \qquad 0 \longrightarrow A(N') \xrightarrow{\ A(\alpha)\ } A(N) \xrightarrow{\ A(\beta)\ } A(N'') \longrightarrow 0$$

is split exact.

Proof

Recall from (2.1.6) that $\mathbf{E}$ is split precisely when

$$\mathrm{Hom}_R(N'', N) \xrightarrow{\ \beta_*\ } \mathrm{Hom}_R(N'', N'')$$

is surjective, with similar results for localizations, completions and adèles. Therefore (i) is equivalent to (ii) by (6.2.4) and to (iii) by (7.1.29). Clearly, (i)

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

implies (iv) just by functoriality of A. To complete the circle of implications, we show that (iv) implies (iii). Consider the commutative diagram

$$\begin{array}{ccc}
\mathrm{Hom}_{A(R)}(A(N''), A(N)) & \xrightarrow{A(\beta)_*} & \mathrm{Hom}_{A(R)}(A(N''), A(N'')) \\
\downarrow & & \downarrow \cong \\
A(\mathrm{Hom}_R(N'', N)) & \xrightarrow{A(\beta_*)} & A(\mathrm{Hom}_R(N'', N'')) \\
\downarrow & & \downarrow \cong \\
\prod_{\mathfrak{p}} \mathrm{Hom}(\widehat{N}''_{\mathfrak{p}}, \widehat{N}_{\mathfrak{p}}) & \xrightarrow[\prod_{\mathfrak{p}} (\widehat{\beta}_{\mathfrak{p}})_*]{} & \prod_{\mathfrak{p}} \mathrm{Hom}(\widehat{N}''_{\mathfrak{p}}, \widehat{N}''_{\mathfrak{p}})
\end{array}$$

with the Hom groups in the bottom row comprising $\widehat{R}_{\mathfrak{p}}$-homomorphisms for each $\mathfrak{p}$.

By the previous corollary, all the vertical maps are defined, (the upper two being λ^{-1} in the notation of the theorem) and the two right-hand vertical maps are isomorphisms. By hypothesis, $A(\beta)_*$ is surjective, whence $(\widehat{\beta}_{\mathfrak{p}})_*$ is surjective for each $\mathfrak{p}$. $\square$

Our main result relies on a criterion for projectivity given in (2.1.8), which we modify to take advantage of the fact that we are here interested in finitely generated modules.

Given any short exact sequence of right R-modules

$$\mathbf{E} \qquad 0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0$$

and a right R-module M, we know that the sequence

$$0 \longrightarrow \mathrm{Hom}_R(M, N') \xrightarrow{\alpha_*} \mathrm{Hom}_R(M, N) \xrightarrow{\beta_*} \mathrm{Hom}_R(M, N'')$$

must be exact. Define $C(M, \mathbf{E})$ to be the cokernel of β_*. Thus $C(M, \mathbf{E})$ is the abelian group which makes the extended sequence

$$0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'') \to C(M, \mathbf{E}) \to 0$$

exact on the right.

7.3.26 Proposition

Let R be an $\mathcal{O}$-order and let M be a finitely generated R-module. Then M

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

is projective if and only if $C(M, \mathbf{E}) = 0$ *for every sequence* $\mathbf{E}$ *with* N'' *finitely generated.*

Proof

If M is projective, then $C(M, \mathbf{E}) = 0$ by (2.1.8), regardless of whether or not N'' is finitely generated. For the converse, take any short exact sequence of the form

$$\mathbf{E}_M \qquad 0 \longrightarrow N' \xrightarrow{\ \alpha\ } N \xrightarrow{\ \beta\ } M \longrightarrow 0$$

Then $C(M, \mathbf{E}_M) = 0$ and so $\beta_* : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, M)$ is surjective. Thus there is some R-homomorphism $\sigma : M \to N$ with $\beta\sigma = id_N$, in other words, $\mathbf{E}_M$ must be split. This means that M is projective by definition. □

We need two more ancillary results before we can reach our goal.

7.3.27 Lemma

Suppose that M *and* N'' *are both finitely generated as* R*-modules. Then* $C(M, \mathbf{E})$ *is a finitely generated* $\mathcal{O}$*-module for any short exact sequence* $\mathbf{E}$ *that ends at* N''*.*

Proof

Let X be any R-module. Since $\mathcal{O}$ is contained in the centre of R, we can view $\mathrm{Hom}_R(M, X)$ as an $\mathcal{O}$-module under the rule

$$a\alpha(m) = \alpha(am) \ \text{ for } a \in \mathcal{O},\ m \in M,\ \alpha \in \mathrm{Hom}_R(M, X).$$

It is readily verified that the homomorphisms in the Hom sequence are $\mathcal{O}$-module homomorphisms, so that $C(M, \mathbf{E})$ is also an $\mathcal{O}$-module.

Since M is finitely generated, there is a surjection $R^k \to M$ for some integer k and hence an injection

$$\mathrm{Hom}_R(M, N'') \longrightarrow \mathrm{Hom}_R(R^k, N'') \cong (N'')^k$$

of $\mathcal{O}$-modules. Because N'' is finitely generated over the $\mathcal{O}$-order R, N'' is also finitely generated as an $\mathcal{O}$-module. But $\mathcal{O}$ is Noetherian, so $\mathrm{Hom}_R(M, N'')$ is finitely generated, as must be $C(M, \mathbf{E})$. □

7.3.28 Proposition

Let R *be an* $\mathcal{O}$*-order. Suppose that* M *is a finitely generated right* R*-module and that*

$$\mathbf{E} \qquad 0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

is a short exact sequence of right R-modules with N'' finitely generated. Then the following hold.

(i)

$$A(R) \otimes_R \mathbf{E} = A(\mathcal{O}) \otimes_{\mathcal{O}} R \otimes_R \mathbf{E} \cong \mathbf{A}(\mathcal{O}) \otimes_{\mathcal{O}} \mathbf{E},$$

each sequence being exact.

(ii) *There is an isomorphism*

$$\prod_{\mathfrak{p}} \widehat{C(M, \mathbf{E})}_{\mathfrak{p}} \cong C(A(M), A(R) \otimes_R \mathbf{E})$$

which is natural in M.

Proof

Recall that, by definition, $A(X) = A(\mathcal{O}) \otimes_{\mathcal{O}} X$ for any R-module X. Part (i) follows immediately from the facts that $A(\mathcal{O})$ is a flat $\mathcal{O}$-module and $A(R)$ is a flat R-module (7.3.17).

By (7.3.27) together with (7.3.16),

$$\prod_{\mathfrak{p}} \widehat{C(M, \mathbf{E})}_{\mathfrak{p}} \cong A(C(M, \mathbf{E})) = A(\mathcal{O}) \otimes_{\mathcal{O}} C(M, \mathbf{E}).$$

Appealing to (7.3.23), we have, for any R-module N, an isomorphism

$$A(\mathcal{O}) \otimes_{\mathcal{O}} \operatorname{Hom}_R(M, N) \xrightarrow{\cong} \operatorname{Hom}_{A(R)}(A(\mathcal{O}) \otimes_{\mathcal{O}} M, A(\mathcal{O}) \otimes_{\mathcal{O}} N)$$

which is natural in both M and N. Using flatness again, we obtain an isomorphism

$$A(\mathcal{O}) \otimes_{\mathcal{O}} C(M, \mathbf{E}) \xrightarrow{\cong} C(A(M), A(\mathcal{O}) \otimes_{\mathcal{O}} \mathbf{E})$$

which gives the desired result. □

We now obtain our main result.

7.3.29 Theorem

Let L be an R-lattice, where R is an order over the Dedekind domain $\mathcal{O}$. Then the following statements are equivalent.

(i) *L is a projective R-module.*
(ii) *$L_{\mathfrak{p}}$ is a projective $R_{\mathfrak{p}}$-module for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$.*
(iii) *$\widehat{L}_{\mathfrak{p}}$ is a projective $\widehat{R}_{\mathfrak{p}}$-module for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$.*
(iv) *$A(L)$ is a projective $A(R)$-module.*

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press

Proof

(i) ⇒ (ii) We have $L \oplus L' = R^k$ for some R-module L' and integer k; since $L_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \otimes L$, the implication is established.

(ii) ⇒ (iii) ⇒ (iv) Similar.

(iv) ⇒ (i) Let

$$\mathbf{E} \qquad 0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

be any short exact sequence of R-modules, with N'' finitely generated. Tensoring each term with $A(R)$, which is a flat R-module, gives a short exact sequence $A(R) \otimes_R \mathbf{E}$ of $A(R)$-modules. By (7.3.26), $C(A(L), A(R) \otimes_R \mathbf{E}) = 0$. By the preceding proposition, $\prod_{\mathfrak{p}} \widehat{C(L, \mathbf{E})}_{\mathfrak{p}} = 0$, and hence $C(L, \mathbf{E}) = 0$ (7.1.28). The theorem follows, using (7.3.26) again. □

7.3.30 Maximal and hereditary orders

An $\mathcal{O}$-order R is said to be *hereditary* if every R-lattice is projective as an R-module. The hereditary orders form an important class, among which are the maximal orders – as the name suggests, an $\mathcal{O}$-order $\mathcal{M}$ in a finite-dimensional $\mathcal{K}$-algebra A is *maximal* if $\mathcal{K}\mathcal{M} = A$ and $\mathcal{M}$ is a maximal member of the set of $\mathcal{O}$-orders R with $\mathcal{K}R = A$.

It can be shown that any given $\mathcal{O}$-order R is contained in a maximal order, provided that the algebra $\mathcal{K}R$ is *$\mathcal{K}$-separable*, which means that $\mathcal{L} \otimes_{\mathcal{K}} \mathcal{K}R$ is Artinian semisimple for any field extension $\mathcal{L}$ of $\mathcal{K}$. (This condition is a generalization of separability for extensions of fields.)

In this text, the discussion of maximal and hereditary orders has been confined to some special cases which have been introduced in the exercises, particularly Exercises 7.2.5 and 7.3.2. Full details of the general results can be found in [Reiner 1975].

If an $\mathcal{O}$-order R is contained in a maximal $\mathcal{O}$-order $\mathcal{M}$, then any R-lattice L is *almost always locally projective* in the following sense: there is a finite set $\mathbf{Q}$ of nonzero prime ideals $\mathfrak{q}$ of $\mathcal{O}$ with the property that the localization $L_{\mathfrak{p}}$ is a projective $R_{\mathfrak{p}}$-lattice provided $\mathfrak{p} \notin \mathbf{Q}$.

The existence of such a set $\mathbf{Q}$ follows from (7.3.4), which tells us that $R_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}$ for almost all $\mathfrak{p}$, together with a fundamental result from the theory of maximal orders, that any $\mathcal{M}_{\mathfrak{p}}$-lattice is projective.

7.3.31 The conductor

Since the properties of maximal orders are well documented, it is useful to have invariants which measure the 'difference' between a given order and a maximal order that contains it. More precisely, we seek such invariants for any pair of $\mathcal{O}$-orders R and S with $R \subseteq S$ and which are both full $\mathcal{O}$-lattices in the same Artinian $\mathcal{K}$-algebra A.

The ideal $\mathfrak{n}(S, R)$ is one such measure; a more precise variant is given by the *conductor*, $\mathfrak{c}(S, R)$ which is defined as

$$\mathfrak{c}(S, R) = \{x \in A \mid xS \subseteq R\}.$$

Here are some basic properties of the conductor.

It is not hard to see that the conductor is a twosided ideal of R, since $1 \in S$. It is also a full $\mathcal{O}$-lattice in A, which follows by applying the Comparison Lemma (7.3.3) to the pair R and S and then to the pair R and $\mathfrak{c}(S, R)$. Straightforward calculations based on those in (v) of (7.3.6), (7.3.7) and (7.3.9) show that $\mathfrak{c}(S, R)_{\mathfrak{p}} = \mathfrak{c}(S_{\mathfrak{p}}, R_{\mathfrak{p}})$ for all nonzero prime ideals of $\mathcal{O}$ and that

$$\mathfrak{c}(S, R) = \bigcap\nolimits_{\mathfrak{p}} \mathfrak{c}(S_{\mathfrak{p}}, R_{\mathfrak{p}}).$$

Furthermore, (7.3.4) shows that $S_{\mathfrak{p}} = R_{\mathfrak{p}}$ for almost all $\mathfrak{p}$, so that $\mathfrak{c}(S, R)_{\mathfrak{p}} = R_{\mathfrak{p}}$ for almost all $\mathfrak{p}$.

Similar results can be proved for the completions, using (7.3.12).

7.3.32 Concluding remarks

(a) Local-global methods originated in number theory, where the aim is to use Hensel's complete local rings to obtain exact global information. This was accomplished for integer quadratic forms in [Hasse 1923], with the consequence that the method is sometimes referred to as the 'Hasse principle'. Usually, the global result is not entirely determined by local information – a Dedekind domain may have non-principal ideals, but these cannot be detected locally, since the ideals of a localization are always principal.

The discrepancy between the local and the global information is usually measured by a suitable long exact sequence. The key to the construction of such sequences is often provided by K-theory.

Local-global techniques for commutative rings in general are a highly developed branch of commutative algebra, motivated by the demands of algebraic geometry, as can be seen from [Eisenbud 1995].

The extension of these techniques to noncommutative orders appears to be due originally to the students of Hasse. Such orders are natural objects of study for an algebraic number theorist. For example, let $\mathcal{O}$ be the ring of integers of an algebraic number field K and suppose that K is a Galois extension of $\mathbb{Q}$, with finite Galois group G. Then $\mathcal{O}$ is a $\mathbb{Z}$-module and it is also invariant under the action of G; thus $\mathcal{O}$ is a module over the integral group ring $\mathbb{Z}G$, which is of course an order.

The determination of the structure of $\mathcal{O}$ as a $\mathbb{Z}G$-module is the *Galois module problem*, an important topic in recent years ([Fröhlich 1983], [Snaith 1994]).

(b) One of the most celebrated local-global results is *Swan's Theorem* [Swan 1960], which is as follows.

Let $\mathcal{O}$ be a Dedekind domain whose field of fractions $\mathcal{K}$ has characteristic 0, let G be a finite group such that no prime divisor of the order of G is a unit in $\mathcal{O}$, and let L be a projective $\mathcal{O}G$-lattice.

Then L is *locally free*, that is, $L_{\mathfrak{p}}$ is a free $\mathcal{O}_{\mathfrak{p}}G$-lattice and $\widehat{L}_{\mathfrak{p}}$ is a free $\widehat{\mathcal{O}}_{\mathfrak{p}}G$-lattice for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$. The converse, that locally free implies projective, follows readily from (7.3.29).

Swan's Theorem shows that if L and M are projective $\mathcal{O}G$-lattices which span the same $\mathcal{K}$-space, then L and M are locally isomorphic (Exercise 6.2.5), and so they are in the same genus of $\mathcal{O}G$-modules.

(c) Our results depend heavily on the fact that we work over a Dedekind domain. Reasonably good results can also be obtained over a Krull domain $\mathcal{O}$, since $\mathcal{O} = \bigcap_{\mathfrak{p}} \widehat{\mathcal{O}}_{\mathfrak{p}}$ again. See [Reiner 1975] (5.2) and [Bass 1968] Chapter III §8.

(d) The extent to which local-global methods apply for genuinely noncommutative rings, such as skew polynomial rings defined by an automorphism of infinite inner order ([BK: IRM] (3.2.13)), seems to be an open question.

Exercises

7.3.1 Let R be an $\mathcal{O}$-order, where $\mathcal{O}$ is a Dedekind domain. For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, define $J(\mathfrak{p})$ by the requirement that

$$J(\mathfrak{p})_{\mathfrak{p}} = \operatorname{rad}(R_{\mathfrak{p}}) \text{ and } J(\mathfrak{p})_{\mathfrak{q}} = R_{\mathfrak{q}} \text{ for } \mathfrak{q} \neq \mathfrak{p}.$$

Prove that $J(\mathfrak{p})$ can equally be defined by the corresponding conditions on its completions:

$$\widehat{J(\mathfrak{p})}_{\mathfrak{p}} = \operatorname{rad}(\widehat{R}_{\mathfrak{p}}) \text{ and } \widehat{J(\mathfrak{p})}_{\mathfrak{q}} = \widehat{R}_{\mathfrak{q}} \text{ for } \mathfrak{q} \neq \mathfrak{p}.$$

Show that $J(\mathfrak{p})$ is a twosided ideal of R and that there is a ring isomorphism

$$R/J(\mathfrak{p}) \cong R_{\mathfrak{p}}/\operatorname{rad}(R_{\mathfrak{p}}).$$

7.3.2 This problem globalizes Exercise 7.2.5.

Let $\mathfrak{a}$ be a proper ideal of a Dedekind domain $\mathcal{O}$, and let $R =$

$\begin{pmatrix} \mathcal{O} & \mathfrak{a} \\ \mathcal{O} & \mathcal{O} \end{pmatrix}$ be the tiled order in $M_2(\mathcal{O})$ consisting of those matrices with 1,2 entry belonging to $\mathfrak{a}$.

For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, find $J(\mathfrak{p})$ and compute all its powers, verifying that

$$(J(\mathfrak{p}))^2 = \begin{cases} \mathfrak{p}J(\mathfrak{p}) & \text{if } \mathfrak{p}^2 \text{ divides } \mathfrak{a} \text{ or if } \mathfrak{p} \text{ does not divide } \mathfrak{a}, \\ \mathfrak{p}R & \text{if } \mathfrak{p} \text{ divides } \mathfrak{a} \text{ exactly.} \end{cases}$$

(Thus the general answer will depend on the power $\mathfrak{p}^h$ of $\mathfrak{p}$ that divides $\mathfrak{a}$.)

Show that $J(\mathfrak{p})$ is left and right projective if and only if $h = 0, 1$. Deduce that the ideals $J(\mathfrak{p})$ are projective for all $\mathfrak{p}$ if and only if $\mathfrak{a}$ is squarefree.

Generalize the results to the case when

$$R = \begin{pmatrix} \mathcal{O} & \mathfrak{a} & \cdots & \mathfrak{a} & \mathfrak{a} \\ \mathcal{O} & \mathcal{O} & \cdots & \mathfrak{a} & \mathfrak{a} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathcal{O} & \mathcal{O} & \cdots & \mathcal{O} & \mathfrak{a} \\ \mathcal{O} & \mathcal{O} & \cdots & \mathcal{O} & \mathcal{O} \end{pmatrix}$$

consists of all those $n \times n$ matrices with entries above the diagonal belonging to $\mathfrak{a}$.

Remark. When $\mathfrak{a}$ is squarefree, R is a typical example of a hereditary order.

7.3.3 Let R be an $\mathcal{O}$-order and let

$$\mathbf{E} \qquad 0 \longrightarrow N' \xrightarrow{\ \alpha\ } N \xrightarrow{\ \beta\ } N'' \longrightarrow 0$$

be a sequence of finitely generated right R-modules and R-module homomorphisms. Show that $\mathbf{E}$ is exact if and only if

$$\mathrm{A}(\mathbf{E}) \quad 0 \longrightarrow A(N') \xrightarrow{A(\alpha)} A(N) \xrightarrow{A(\beta)} A(N'') \longrightarrow 0$$

is exact.

7.3.4 Let $R \subseteq S$ be $\mathcal{O}$-orders spanning the same $\mathcal{K}$-algebra, with conductor $\mathfrak{c}$. Show that R is isomorphic to the pull-back of the diagram of rings and ring homomorphisms

$$\begin{array}{ccc} & & S \\ & & \downarrow \\ R/\mathfrak{c} & \longrightarrow & S/\mathfrak{c} \end{array}$$

in which the horizontal arrow is injective and the vertical arrow is surjective. Compute $\mathfrak{c}$, $R/\mathfrak{c}$ and $S/\mathfrak{c}$ when R is the tiled order of Exercise 7.3.2 and S is the full matrix ring containing R.

Remark. The description of an order R as a pull-back of a maximal order S and an Artinian ring $R/\mathfrak{c}$ can be an effective tool for the investigation of the properties of R – see [Milnor 1971] §2.

7.3.5 Let I be a twosided fractional ideal of an $\mathcal{O}$-order R, where $\mathcal{O}$ is a Dedekind domain. Show that I is invertible if and only if $I_{\mathfrak{p}}$ is invertible for all $\mathfrak{p}$.

Deduce that there is a surjection

$$\theta : \mathrm{Pic}(R) \longrightarrow \bigoplus_{\mathfrak{p}} \mathrm{Pic}(R_{\mathfrak{p}}).$$

Remark. It can be shown that, when $\mathcal{O}$ is the ring of integers of a number field, we have $\mathrm{Pic}(R_{\mathfrak{p}}) = 1$ for almost all $\mathfrak{p}$. The map θ need not be injective, as can be seen by taking R to be $\mathcal{O}$ itself. A discussion of local-global results for Pic can be found in [Curtis & Reiner 1987] §55.

7.3.6 **Projective dimension**

The bifunctor Ext has the following properties (see Exercise 2.1.7 or [Rotman 1979]).

Given a right R-module L, let

$$0 \longrightarrow S \longrightarrow P \longrightarrow L \longrightarrow 0$$

be a short exact sequence with P projective. Then for any right R module X, $\mathrm{Ext}^1_R(L, X)$ fits into an exact sequence

$$0 \to \mathrm{Hom}_R(L, X) \to \mathrm{Hom}_R(P, X) \to \mathrm{Hom}_R(S, X) \to \mathrm{Ext}^1_R(L, X) \to 0.$$

Furthermore, for $n > 1$, we have

$$\mathrm{Ext}^{n+1}_R(L, X) = \mathrm{Ext}^n_R(S, X).$$

The *projective dimension* $\mathrm{pd}_R(L)$ of L is defined by

$$\mathrm{pd}_R(L) = \inf\{n \mid \mathrm{Ext}^{n+1}_R(L, X) = 0 \text{ for all } X\}.$$

(a) Confirm that $\mathrm{pd}_R L = 0$ if and only if L is projective, and that $\mathrm{pd}_R S = \mathrm{pd}_R L - 1$ otherwise.

(b) Suppose that L is finitely generated. Verify inductively that the projective dimension can be defined by considering the inf over all finitely generated X.

(c) Extend (7.3.23) as follows.

Let $\mathcal{O}$ be a Dedekind domain and let R be an $\mathcal{O}$-order. Suppose that T is a commutative ring extension of $\mathcal{O}$ and that T is a flat $\mathcal{O}$-module.

Then for any pair L, X of finitely generated right R-modules, there is a natural isomorphism

$$\lambda : T \otimes_{\mathcal{O}} \mathrm{Ext}^n_R(L, X) \longrightarrow \mathrm{Ext}^n_{T\otimes_{\mathcal{O}} R}(T \otimes_{\mathcal{O}} L, T \otimes_{\mathcal{O}} X).$$

(d) Show that $\mathrm{Ext}^n_R(L, X)$ is finitely generated if both L and X are finitely generated.

(e) Deduce the following generalization of (7.3.29):

Let L be an R-lattice. Then

$$\mathrm{pd}_R(L) = \sup\{\mathrm{pd}_{R_\mathfrak{p}}(L_\mathfrak{p}) \mid \mathfrak{p} \text{ is a nonzero prime of } \mathcal{O}\}$$

and

$$\mathrm{pd}_{R_\mathfrak{p}}(L_\mathfrak{p}) = \mathrm{pd}_{\widehat{R}_\mathfrak{p}}(\widehat{L}_\mathfrak{p})$$

for all nonzero primes $\mathfrak{p}$.

https://doi.org/10.1017/9780511608667.008 Published online by Cambridge University Press