1

Modules, Lattices, and Orders

In this chapter we present essential background. We rapidly review some basic facts in the theory of rings and modules. In particular, we introduce the concept of a lattice over an integral domain and examine some basic properties of lattices. Next, after a quick review of integrality, we focus on the case of Dedekind domains, a notion that encompasses both the ring of algebraic integers of number fields, that is, of field extensions of $\mathbb{Q}$ of finite degree, and certain rings of algebraic functions. We briefly discuss some basic results regarding the ring-theoretic structure of Dedekind domains and their overrings, as well as the structure theory of finitely generated modules over such rings. Then we deal with central simple algebras over a field, crossed products, and cyclic algebras. We introduce the concept of an order in a finite-dimensional separable algebra defined over the quotient field of a Dedekind domain. The chapter concludes with a discussion of notions from non-abelian Galois cohomology that are needed in the theory of algebraic groups as well as in the geometric investigations in Chapters 10 and 11.

Proofs are often omitted, especially when they are readily available in standard texts in algebra, commutative algebra, or the arithmetic theory of orders such as Jantzen and Schwermer (2014), Serre (1968), Atiyah and Macdonald (1969), Deuring (1968), and Reiner (2003). We shall seldom specify the exact location in these references where the proofs can be found. Naturally, there are some special topics that have importance for us but are less well known or perhaps not stated in the literature in the way we need. For these topics, we often give proofs.

This chapter is intended more as a resume of needed background than as a complete introduction to its material. It also serves to fix notation and conventions. It is suggested to start straightaway with Chapter 2 and then refer back to the algebraic foundations in Chapter 1 as is necessary.

1.1 Modules

In this section, let R denote a ring, not necessarily commutative, with unit element 1. All R-modules are left R-modules, unless otherwise specified. Each R-module M is assumed to satisfy the condition $1 \cdot m = m$ for all $m \in M$.

If $(M_i)_{i\in I}$ is any family of R-modules, we have their direct sum $\bigoplus_{i\in I} M_i$; its elements are families $(m_i)_{i\in I}$ with $m_i \in M_i$, $i \in I$, and almost all m_i are 0. Addition of elements and scalar multiplication are given in the obvious way. Note that we obtain the direct product $\prod_{i\in I} M_i$ if we drop the restriction on the number of non-zero m_is. If $(M_i)_{i\in I}$ is a family of submodules of an R-module M, there is an R-linear map $\phi\colon \bigoplus_{i\in I} M_i \longrightarrow M$, defined by $(m_i)_{i\in I} \mapsto \sum_{i\in I} m_i$. Its image is the R-submodule

$$\sum_{i\in I} M_i := \left\{ \sum_{i\in I} m_i \mid m_i \in M_i, m_i = 0 \text{ for almost all } i \right\}$$

in M. If ϕ is injective, we say that the sum of the M_i is direct and write, by abuse of notation, $\sum_{i\in I} M_i = \bigoplus_{i\in I} M_i$. We have $M_1 + M_2 = M_1 \oplus M_2$ if and only if $M_1 \cap M_2 = \{0\}$.

If M is an R-module and I an index set, we can consider the family $(M_i)_{i\in I}$ with $M_i = M$ for all $i \in I$. In such a case we write $M^{(I)} = \bigoplus_{i\in I} M_i$, and $M^I = \prod_{i\in I} M_i$. In the case, $I = \{1, \ldots, r\}$ for some non-negative integer r, we write $M^r = M^{(I)} = M^I$.

Definition 1.1.1 Let M be an R-module, and let I be an arbitrary index set. Given a family $(m_i)_{i\in I}$ of elements in M, there is a linear map

$$\psi\colon R^{(I)} \longrightarrow M, \qquad (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i m_i.$$

We call the family $(m_i)_{i\in I}$ a set of generators for M (over R) if ψ is surjective. We say that $(m_i)_{i\in I}$ is linearly independent (over R) if ψ is injective. Finally, $(m_i)_{i\in I}$ is a basis of M (over R) if ψ is bijective.

We call an R-module M a free R-module if M has a basis over R. Whereas two bases of a finite-dimensional vector space over a field contain the same number of elements, this is not necessarily the case for free modules over an arbitrary ring. However, in the case of a commutative ring R, the following holds true.

Proposition 1.1.2 *Let R be a non-zero commutative ring, and let M be an R-module. If $m_1, \ldots, m_r$ and $n_1, \ldots, n_s$ are both a basis of M over R, then $r = s$. We call the cardinality of a basis of the free R-module M the rank of M.*

Proof Since R is a non-zero commutative ring, R possesses at least one maximal ideal I. Then R/I is a field. We denote by IM the R-submodule

$$\left\{ \sum_{i=1}^{m} a_i x_i \mid m \in \mathbb{N}, a_i \in I, x_i \in M \right\}$$

of M. Then M/IM carries an R/I-module structure, defined by $(a+I)(x+IM) = ax + IM$. The elements $m_1 + IM, \ldots, m_r + IM$ as well as the elements $n_1 + IM, \ldots, n_s + IM$ form a basis of the vector space M/IM over the field R/I; thus, $r = s$. □

Definition 1.1.3 An R-module M is said to be finitely generated if it has a finite set of generators, equivalently, there exists a surjective morphism $R^n \longrightarrow M$ for some $n > 0$. We say that M is a finitely presented R-module if there exists an exact sequence $R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$ for some $m, n > 0$.

Definition 1.1.4 An R-module M is said to be Noetherian if every submodule of M is finitely generated over R. Accordingly, we call the ring R left-Noetherian if R, viewed as a left R-module, is Noetherian. Similarly, a ring R is called right-Noetherian if R viewed as a right R-module is Noetherian.

This defining condition is equivalent to either of the following two conditions: first, the submodules of M satisfy the ascending chain condition, that is, every ascending chain of submodules of M becomes stationary, and, second, every non-empty set of submodules of M has a maximal element.

Definition 1.1.5 An R-module M is said to be Artinian if M satisfies the descending chain condition, that is, every descending chain of submodules of M is stationary. A ring R is called left-Artinian if R viewed as a left R-module is Artinian.

Lemma 1.1.6 *Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be a short exact sequence of R-modules. Then M is Noetherian (resp. Artinian) if and only if both M' and M'' are Noetherian (resp. Artinian).*

Proof Straightforward exercise for the reader. □

Proposition 1.1.7 *Every finitely generated R-module over a left Noetherian ring R is Noetherian.*

Proof There is a surjective R-morphism $R^n \longrightarrow M$ for some $n > 0$. By Lemma 1.1.6, combined with induction, R^n is a Noetherian R-module. Then the assertion follows from Lemma 1.1.6. □

Proposition 1.1.8 *Let R be a left Noetherian ring, and let I be a two-sided ideal of R. Then the quotient ring R/I is a Noetherian ring.*

Proof The submodules of R/I, viewed as R/I-modules, coincide with the submodules of R/I, viewed as R-modules. Such a submodule, say N, is finitely generated over R/I if and only if N is finitely generated over R. Since R is left Noetherian, the R-module R/I is Noetherian by Proposition 1.1.7. □

Lemma 1.1.9 *If M and N are R-modules such that $M \oplus N \cong M$, and $N \neq (0)$, then M is not a Noetherian module over R.*

Proof Let $\mathcal{X}$ be the set of all submodules $N' \subset M$ for which there exists an R-submodule $M' \subset M$ such that $M = M' \oplus N'$ and $M' \cong M$. The set $\mathcal{X}$ is non-empty since $N' = (0)$ is an element of $\mathcal{X}$.

Assume there exists a maximal element N' in $\mathcal{X}$. There exists an R-module $M' \cong M$ with $M = M' \oplus N'$, and, by our assumption, there is an isomorphism $\alpha\colon M \oplus N \xrightarrow{\sim} M'$. It follows that $M' = \alpha(M) \oplus \alpha(N)$; hence

$$M = \alpha(M) \oplus (\alpha(N) \oplus N') = M'' \oplus N'',$$

where $M'' = \alpha(M)$ and $N'' = \alpha(N) \oplus N'$. Since the morphism α is injective, we get $M'' \cong M$ and $\alpha(N) \neq (0)$; thus, $N'' \in \mathcal{X}$ and $N' \subsetneq N''$. Therefore $\mathcal{X}$ has no maximal element. □

Proposition 1.1.10 *Let $R \neq \{0\}$ be a left Noetherian ring. If $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_m\}$ are two bases of an R-module M, then $n = m$, that is, two bases of M have the same cardinality.*

Proof Suppose that $n \geq m$. The assumption implies that there are isomorphisms $M \cong R^n$ and $M \cong R^m$. It follows $R^m \cong R^n \cong R^m \oplus R^{n-m}$. Since R^m is a Noetherian module, Lemma 1.1.9 implies $R^{n-m} = (0)$; thus, $n = m$, because R is a non-zero ring. □

We call a chain $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r = (0)$ of submodules of an R-module a composition series of M if each quotient M_i/M_{i+1}, $0 \leq i < r$ is a simple R-module, that is, has no submodules except (0) and itself. If this is the case, r is the length of this chain.

Let $\ell(M) = \ell_R(M)$ denote the least length of a composition series of an R-module M; put $\ell(M) = +\infty$ if M has no composition series. Note that, given an R-module M, all composition series of M have the same length, and, if there is at least one, every chain of submodules of M can be refined to a composition series of M. By definition, an R-module is of finite length if M has a composition series. This latter property is equivalently characterised by the fact the M is both Artinian and Noetherian.

To conclude this section, we briefly recall the notion of tensor algebra and symmetric algebra attached to a module M over a commutative ring R. By definition, the corresponding tensor algebra of M is the R-algebra

$$T_R(M) := \bigoplus_{p=0}^{\infty} T_R^p(M) \text{ with } T_R^p(M) = \otimes^p M \text{ the } p\text{th-tensorial power of } M,$$

equipped with the usual product $T_R^p(M) \times T_R^q(M) \longrightarrow T_R^{p+q}(M)$, defined by the assignment $(x_1 \otimes \cdots \otimes x_p, x_{p+1} \otimes \cdots \otimes x_{p+q}) \mapsto x_1 \otimes \cdots \otimes x_{p+q}$. This is a graded R-algebra, with $T_R^0(M) = R$ and $T_R^1(M) = M$.

The symmetric algebra of M, to be denoted $\mathrm{Sym}_R(M)$, is the algebra obtained as the quotient of the tensor algebra $T_R(M)$ modulo the two-sided ideal I generated by the tensors $x \otimes y - y \otimes x$ for all $x, y \in M$. It is a commutative R-algebra, endowed with the graduation inherited from the one of $T_R(M)$. Clearly, $\mathrm{Sym}_R^0(M) = R$ and $\mathrm{Sym}_R^1(M) = M$. The algebra $\mathrm{Sym}_R(M)$ has the following universal property: for every commutative R-algebra S, there is a natural bijection

$$\mathrm{Hom}_{R-\mathrm{alg}}(\mathrm{Sym}_R(M), S) \xrightarrow{\sim} \mathrm{Hom}_R(M, S),$$

induced by the inclusion $\iota\colon M \longrightarrow \mathrm{Sym}_R(M)$, via $\alpha \mapsto \alpha \circ \iota$. Given another R-module N, together with an R-module homomorphism $\kappa\colon M \longrightarrow N$, the universal property implies, by taking $S = \mathrm{Sym}_R(N)$, that there is an R-algebra homomorphism $\mathrm{Sym}(\kappa)\colon \mathrm{Sym}_R(M) \longrightarrow \mathrm{Sym}_R(N)$ which is graded. In this manner we obtain a functor, to be denoted Sym_R, from the category of commutative R-modules to the category of graded commutative R-algebras.

As another consequence of the universal property, we obtain an isomorphism of S-algebras

$$\mathrm{Sym}_R(M) \otimes_R S \xrightarrow{\sim} \mathrm{Sym}_S(M \otimes_R S),$$

which is functorial in M and compatible with the grading. Similarly, given two R-modules M, M', there is an isomorphism of graded R-algebras

$$\mathrm{Sym}_R(M) \otimes \mathrm{Sym}_R(M') \xrightarrow{\sim} \mathrm{Sym}_R(M \oplus M'),$$

which is functorial in M and M'. In the case of a free R-module M, say with basis $\{m_1, \ldots, m_r\}$, the latter isomorphism implies that there is a graded R-algebra isomorphism $R[t_1, \ldots, t_r] \xrightarrow{\sim} \mathrm{Sym}_R(M)$ between the polynomial algebra in the variables $t_1, \ldots, t_r$ and the symmetric algebra.

1.2 Projective R-modules

Now we briefly recall some facts concerning projective R-modules. Given any R-module M, the functor $\mathrm{Hom}_R(M, -)\colon \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_R$ from the category of R-modules to itself is left exact. By definition, an R-module P is projective if and only if the functor $\mathrm{Hom}_R(P, -)$ is exact. We state without proof the following alternative characterisations of a projective R-module.

Proposition 1.2.1 *Let P be any R-module. The following assertions are equivalent:*

(1) *The R-module P is projective.*
(2) *Every short exact sequence $0 \to L \to M \to P \to 0$ of R-modules splits.*
(3) *There exists an R-module P' such that $P \oplus P'$ is a free R-module.*
(4) *Given a surjective homomorphism $\pi\colon M \longrightarrow N$ of R-modules and given a homomorphism $\phi\colon P \to N$ of R-modules there exists a homomorphism $\psi\colon P \longrightarrow M$ such that $\pi \circ \psi = \phi$; that is to say, equivalently, the natural map $\mathrm{Hom}_R(P, M) \longrightarrow \mathrm{Hom}_R(P, N)$ is surjective.*

Let $(P_i)_{i\in I}$ be any family of R-modules. Then the very definition of being projective immediately implies that the direct sum $\bigoplus_{i\in I} P_i$ is projective if and only if each P_i, $i \in I$ is projective.

If R is a commutative ring, an R-module M, by convention a left R-module, may also be viewed naturally as a right R-module. Thus, given two R-modules M, N their tensor product $M \otimes_R N$ is defined as an R-module. If M, N are both projective, then $M \otimes_R N$ is also projective.

The following result generalises a well-known fact valid for submodules of free modules over a principal ideal domain. We call a ring R a left hereditary ring if every left ideal of R is a projective R-module. We have the following structure result for submodules of free modules over a left hereditary ring.

Proposition 1.2.2 *Let R be a left hereditary ring. Then any submodule N of a free (left) R-module M isomorphic to R^s is isomorphic to a direct sum of submodules isomorphic to left ideals of R, and therefore N is projective.*

Proof Let $m_1, \ldots, m_s$ be a free basis of M over R. We proceed by induction over s. For $s = 1$, the result is clear since the submodules of R are left ideals. Now assume that $s > 1$. Let M' be the submodule of M given as $M' = Rm_1 + \cdots + Rm_{s-1}$. Every element $n \in N$ can be written in the form $n = \sum_{i=1}^{s} \nu_i m_i$ with uniquely determined coefficients ν_i, $i = 1, \ldots s$. We consider the R-homomorphism $\phi\colon N \longrightarrow R$, given by $\phi(n) = \nu_s, n \in N$. The image is a left ideal I in R, and $\ker \phi$ equals the submodule $N \cap M'$ of M'. There is an exact sequence

$$0 \longrightarrow N \cap M' \longrightarrow N \longrightarrow I \longrightarrow 0.$$

Since, by assumption on R, the left ideal I is a projective R-module, this sequence splits; hence, $N \cong I \oplus (N \cap M')$. By induction hypothesis, $N \cap M'$ is isomorphic to a direct sum of left ideals of R. Hence N is also isomorphic to a direct sum of left ideals of R. Since each of them is projective, N is a projective R-module. □

We turn our attention to finitely generated projective R-modules M, where R is assumed to be a commutative ring. Properties of these modules play a decisive

role, for example, in the discussion of orders in finite-dimensional central simple algebras.

An alternative characterisation of such an R-module M is that M is a direct summand of a finitely generated free R-module. Indeed, since M is finitely generated, there is a surjective morphism $\alpha\colon R^n \longrightarrow M$ for some $n > 0$. This gives rise to a short exact sequence $0 \to \ker\alpha \to R^n \to M \to 0$. Since M is projective the sequence splits, and M is a direct summand of a finitely generated free R-module. Conversely, using Proposition 1.2.1(3), this last property implies that M is finitely generated projective since a direct summand of a projective module is projective.

We record the following result for later use. The proof may be found in Lam (1999, §2B).

Proposition 1.2.3 *Let R be a commutative ring, let M be a finitely generated projective R-module, and let $M^\vee = \mathrm{Hom}_R(M, R)$ be its dual module. Then the canonical morphism $\iota\colon M \longrightarrow \mathrm{Hom}_R(M^\vee, R)$, defined by $m \mapsto \iota(m)$ with $\iota(m)(\alpha) := \alpha(m)$ for all $m \in M, \alpha \in M^\vee$, is an isomorphism. More generally, given any R-module N, the natural homomorphism $M \otimes_R N \longrightarrow \mathrm{Hom}_R(M^\vee, N)$ is an isomorphism of R-modules.*

Suppose that M is a free R-module of rank n, and let $\alpha\colon M \longrightarrow M$ be an R-module endomorphism. Then α can be extended in a unique way to an R-module endomorphism $\hat{\alpha}$ of the exterior power $\bigwedge^*(M)$ of M. The nth exterior power $\bigwedge^n(M)$ of M is a free R-module of rank one, and, on this component, $\hat{\alpha}$ is multiplication by an element of R. By definition, the determinant $\det(\alpha)$ of α is that element.

More generally, if M be a finitely generated projective R-module, then M is a direct summand in a finitely generated R-module, say $M \oplus M' \cong R^n$ for some $n \in \mathbb{N}$. If $\alpha\colon M \longrightarrow M$ is an R-module endomorphism, the determinant $\det(\alpha \oplus \mathrm{Id}_{M'})$ is well defined. Since $\det(\alpha \oplus \mathrm{Id}_{M'})$ is independent of the choice of the R-module M', we can define the determinant of α by $\det(\alpha) := \det(\alpha \oplus \mathrm{Id}_{M'})$. The usual properties of determinants are valid, that is, given R-module endomorphisms $\alpha, \beta\colon M \longrightarrow M$, we have $\det(\alpha \circ \beta) = \det(\alpha) \cdot \det(\beta)$, and $\det(\mathrm{Id}_M) = 1_R$. Moreover, α is invertible if and only if $\det(\alpha) \in R^\times$.

Let S be a commutative R-algebra. Any $\alpha \in \mathrm{End}_R(M)$ gives rise to an endomorphism $\alpha \otimes \mathrm{Id}_S \in \mathrm{End}_S(M \otimes_R S)$. Then $\det(\alpha) = \det(\alpha \otimes_R \mathrm{Id}_S)$ naturally viewed as elements in S.

The notion of a trace of an endomorphism of a finitely generated projective R-module M can be dealt with in an analogous way, by defining $\mathrm{tr}(\alpha) := \mathrm{tr}(\alpha \oplus 0_{M'})$.

Recall that a non-zero ring R is called a local ring if R has a unique maximal left ideal, or, equivalently, if R modulo its radical is a division ring. In the case of such a ring we have (cf. Lam, 2001, Thm. 19.29)

Proposition 1.2.4 *Let R be any local ring. Then any finitely generated projective R-module M is a finitely generated free R-module.*

1.3 Modules of fractions and localisation

Throughout this section, A denotes a commutative ring. A multiplicatively closed subset of A is a subset S of A such that $0 \notin S$, $1 \in S$, and S is closed under multiplication. Define a relation, denoted $\sim$, on the Cartesian product $A \times S$ as follows: $(a, s) \sim (b, t)$, where $a, b \in A, s, t \in S$, if and only if $(at - bs)u = 0$ for some $u \in S$. Indeed, this relation is reflexive, transitive, and symmetric, thus, an equivalence relation. Let a/s denote the equivalence class of (a, s), and let $S^{-1}A$ be the set of equivalence classes. Now define

$$(a/s) + (b/t) = (at + bs)/st \text{ resp. } (a/s) \cdot (b/t) = ab/st$$

verifying that addition and multiplication are well defined. The set $S^{-1}A$, endowed with this structure, forms a commutative ring with unity element $1/1$ and zero element $0/1$. We shall call $S^{-1}A$ the ring of fractions of A with respect to S .

There is a ring homomorphism $i\colon A \longrightarrow S^{-1}A$, defined by $i(a) = a/1$, where $a \in A$. This is not in general injective. However, if A is an integral domain, the morphism i is injective, and we may view A as embedded into $S^{-1}A$.

As usual in this context, given an ideal $\mathfrak{a}$ in A, we define the extension $\mathfrak{a}^e$ of $\mathfrak{a}$ to be the ideal $i(\mathfrak{a})S^{-1}A$ generated by $i(\mathfrak{a})$ in $S^{-1}A$; since any element in $\mathfrak{a}^e$ is of the form $\sum a_i/s_i$ with $a_i \in \mathfrak{a}, s_i \in S$ we have $\mathfrak{a}^e = S^{-1}\mathfrak{a}$. Reversely, if $\mathfrak{b}$ is an ideal in $S^{-1}A$, then $\mathfrak{b}^c := i^{-1}(\mathfrak{b})$ is an ideal, called the contraction of $\mathfrak{b}$. The following result describes the relation between the ideals in A and the ideals in $S^{-1}A$.

Proposition 1.3.1 *Let A be a commutative ring, and let S be a multiplicatively closed subset of A.*

(1) *Every ideal in $S^{-1}A$ is an ideal obtained via extension from an ideal in A; more precisely, given an ideal $\mathfrak{b}$ of $S^{-1}A$, then $\mathfrak{b} = \mathfrak{b}^{ce}$.*
(2) *The prime ideals of $S^{-1}A$ are in one-to-one correspondence via the assignment $\mathfrak{p} \longleftrightarrow \mathfrak{p}^e$ with the prime ideals of A which do not meet S.*

Proof Left as an exercise to the reader. □

The concept of a ring of fractions with respect to a multiplicatively closed subset S of A can be extended to A-modules M. Given a multiplicatively closed subset S of A, define, as before, an equivalence relation on $M \times S$ as follows: $(m, s) \sim (m', s')$, $m, m' \in M, s, s' \in S$, if and only if $u(sm' - s'm) = 0$ for some $u \in S$. Let m/s denote the equivalence class of the pair (m, s), and let $S^{-1}M$ be the

set of equivalence classes. We put the structure of an $S^{-1}A$-module on $S^{-1}M$ with the obvious definition of addition and scalar multiplication.

Using the canonical homomorphism $i\colon A \longrightarrow S^{-1}A$, we may view the $S^{-1}A$-module $S^{-1}M$ as an A-module. Then we may form the $S^{-1}A$-module $S^{-1}A \otimes_A M$. We observe that every element in $S^{-1}A \otimes_A M$ can be written in the form $s^{-1} \otimes m$ for some $s \in S$, $m \in M$. Namely, given $x = \sum(a_i/s_i) \otimes m_i$ where the sum ranges over a finite index set I, we set $s := \prod_{i\in I} s_i$, and $t_i := \prod_{j\neq i} s_j$ for all $i \in I$. Then we obtain

$$x = \sum_i s^{-1}(a_i s s_i^{-1}) \otimes m_i = \sum_i s^{-1} \otimes a_i t_i m_i = s^{-1} \otimes m,$$

with $m = \sum_i a_i t_i m_i$. Since the map $j'\colon S^{-1}A \times M \longrightarrow S^{-1}M$, defined by the assignment $((a/s), m) \mapsto am/s$, is A-bilinear, there exists a unique A-module homomorphism $j\colon S^{-1}A \otimes_A M \longrightarrow S^{-1}M$ satisfying $j((a/s) \otimes m) = am/s$ for all $a \in A$, $s \in S$, and $m \in M$.

Proposition 1.3.2 *Let M be an A-module, and let S be a multiplicatively closed subset of A. Then there exists a unique $S^{-1}A$-module isomorphism*

$$j\colon S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$$

such that $j((a/s) \otimes m) = am/s$ for all $a \in A$, $s \in S$, and $m \in M$.

Proof Left as an exercise to the reader. □

Let $i\colon M \longrightarrow S^{-1}M$ be the canonical map, defined by $m \mapsto m/1$. It is of interest to understand the relation between $S^{-1}A$-submodules of $S^{-1}M$ and A-submodules of M. Given an $S^{-1}A$-submodule N' of $S^{-1}M$, we denote by $N := i^{-1}(N')$ the inverse image of N' under i. We claim that $S^{-1}N = N'$. Obviously, $i(N) \subset N'$. Since N' is an $S^{-1}A$-module, $S^{-1}N \subset N'$. Conversely, if $x/s \in N'$, then $x/1 = s(x/s) \in N'$; thus, $x \in i^{-1}(N') = N$, and the claim follows.

We observe that the A-module $N = i^{-1}(N')$ has the following property: Let $s \in S$, $m \in M$ such that $sm \in N$. Then $i(sm) = sm/1 \in N'$. We obtain $s \cdot (m/1) \in N'$; hence $(1/s)s \cdot (m/1) \in N'$. This shows that $m \in N$.

This observation gives rise to the following conceptual approach:

Definition 1.3.3 Let S be a multiplicatively closed subset of A, and let M be an A-module. Given a submodule N of M, we call the submodule $i^{-1}(S^{-1}N)$ the saturation of N in M with respect to S. We say that N is saturated with respect to S if N equals its own saturation, equivalently, N has the property: if $s \in S$, $m \in M$ such that $sm \in N$, then $m \in N$.

Now, in view of these remarks, it is not difficult to see the following assertion: see Bourbaki (1985, Chap. II, §2, no.4, Prop. 10).

Proposition 1.3.4 *Let S be a multiplicatively closed subset of A, let M be an A-module, and let $i\colon M \longrightarrow S^{-1}M$ be the canonical map defined by $m \mapsto m/1$. The assignment $N' \mapsto i^{-1}(N')$ gives an inclusion-preserving bijection between the set of $S^{-1}A$-submodules N' of $S^{-1}M$ and the set of A-submodules N of M which have the following property: if $s \in S$, $m \in M$ such that $sm \in N$, then $m \in N$.*

Corollary *If M is a Noetherian (resp. Artinian) R-module, then the module of fractions $S^{-1}M$ of M with respect to a multiplicatively closed subset S of A is a Noetherian (resp. Artinian) $S^{-1}A$-module.*

Let $\psi\colon M \longrightarrow N$ be an A-module homomorphism. Then, given any multiplicatively closed subset S of A, there is a corresponding $S^{-1}A$-module homomorphism $S^{-1}\psi\colon S^{-1}M \longrightarrow S^{-1}N$, defined by $m/s \mapsto \psi(m)/s$, $m \in M$, $s \in S$. Evidently, the operation S^{-1} is compatible with the composition of A-module homomorphisms, and we have

Proposition 1.3.5 *Let $M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2$ be a sequence of A-modules such that $Im\, f_0 = Ker\, f_1$, i.e. the sequence is exact at M_1. Then the sequence*

$$S^{-1}M_0 \xrightarrow{S^{-1}f_0} S^{-1}M_1 \xrightarrow{S^{-1}f_1} S^{-1}M_2$$

is exact at $S^{-1}M_1$.

Examples 1.3.6 (1) Let $\mathfrak{p}$ be a prime ideal of A. Then $S = A \setminus \mathfrak{p}$ is multiplicatively closed. The set $\mathfrak{m} := \{a/s \mid a \in \mathfrak{p}, s \in S\}$ forms an ideal in $A_{\mathfrak{p}} := S^{-1}A$. If $b/t \notin \mathfrak{m}$, then $b \notin \mathfrak{p}$; hence $b \in S$ and therefore b/t is a unit in $A_{\mathfrak{p}}$. Consequently, given an ideal $\mathfrak{a}$ of $A_{\mathfrak{p}}$ such that $\mathfrak{a}$ is not contained in $\mathfrak{m}$, then $\mathfrak{a}$ contains a unit; thus $\mathfrak{a} = A_{\mathfrak{p}}$. It follows that $\mathfrak{m}$ is the only maximal ideal in $A_{\mathfrak{p}}$, that is, $A_{\mathfrak{p}}$ is a local ring, called the localisation of A at $\mathfrak{p}$.

Observe that the prime ideals of the ring $A_{\mathfrak{p}}$ are in one-to-one correspondence with the prime ideals of A which do not meet $S = A \setminus \mathfrak{p}$, that is, with the prime ideals of A contained in $\mathfrak{p}$.

If M is an A-module, $\mathfrak{p}$ a prime ideal of A, and $S = A \setminus \mathfrak{p}$, we write $M_{\mathfrak{p}}$ for the $S^{-1}A$-module $S^{-1}M$, to be called the localisation of M at $\mathfrak{p}$.

Given an A-module homomorphism $f\colon M \longrightarrow N$ and a prime ideal $\mathfrak{p}$ of A, we denote the corresponding $A_{\mathfrak{p}}$-module homomorphism $M_p \longrightarrow N_{\mathfrak{p}}$ by $f_{\mathfrak{p}}$.

(2) Let $a \in A$, $a \neq 0$, with a not nilpotent. Define S to be the set $\{a^n\}_{n\geq 0}$. Then S is multiplicatively closed, and we denote $S^{-1}A$ by $A[1/a]$. In the case of the ring $A = \mathbb{Z}$, $a = p$ a prime, the ring $\mathbb{Z}[1/p]$ is the ring of all rational integers whose denominator is a power of p.

The next result suggests a strong relation between an integral domain A and all localisations of A at prime ideals of A.