2

Modules

One of the things which distinguishes the modern approach to Commutative Algebra is the greater emphasis on modules, rather than just on ideals. The extra "elbow-room" that this gives makes for greater clarity and simplicity. For instance, an ideal $\mathfrak{a}$ and its quotient ring $A/\mathfrak{a}$ are both examples of modules and so, to a certain extent, can be treated on an equal footing. In this chapter we give the definition and elementary properties of modules. We also give a brief treatment of tensor products, including a discussion of how they behave for exact sequences.

MODULES AND MODULE HOMOMORPHISMS

Let A be a ring (commutative, as always). An *A-module* is an abelian group M (written additively) on which A acts linearly: more precisely, it is a pair (M,μ), where M is an abelian group and μ is a mapping of $A \times M$ into M such that, if we write ax for $\mu(a, x)(a \in A, x \in M)$, the following axioms are satisfied:

$$\begin{aligned} a(x + y) &= ax + ay, \\ (a + b)x &= ax + bx, \\ (ab)x &= a(bx), \\ 1x &= x \qquad\qquad (a, b \in A; \quad x, y \in M). \end{aligned}$$

(Equivalently, M is an abelian group together with a ring homomorphism $A \to E(M)$, where $E(M)$ is the ring of endomorphisms of the abelian group M.)

The notion of a module is a common generalization of several familiar concepts, as the following examples show:

Examples. 1) An ideal $\mathfrak{a}$ of A is an A-module. In particular A itself is an A-module.

2) If A is a field k, then A-module $=$ k-vector space.

3) $A = \mathbf{Z}$, then $\mathbf{Z}$-module $=$ abelian group (define nx to be $x + \cdots + x$).

4) $A = k[x]$ where k is a field; an A-module is a k-vector space with a linear transformation.

5) $G =$ finite group, $A = k[G] =$ group-algebra of G over the field k (thus A is not commutative, unless G is). Then A-module $=$ k-representation of G.

Let M, N be A-modules. A mapping $f\colon M \to N$ is an *A-module homomorphism* (or is *A-linear*) if

$$f(x + y) = f(x) + f(y)$$
$$f(ax) = a \cdot f(x)$$

for all $a \in A$ and all $x, y \in M$. Thus f is a homomorphism of abelian groups which commutes with the action of each $a \in A$. If A is a field, an A-module homomorphism is the same thing as a linear transformation of vector spaces.

The composition of A-module homomorphisms is again an A-module homomorphism.

The set of all A-module homomorphisms from M to N can be turned into an A-module as follows: we define $f + g$ and af by the rules

$$(f + g)(x) = f(x) + g(x),$$
$$(af)(x) = a \cdot f(x)$$

for all $x \in M$. It is a trivial matter to check that the axioms for an A-module are satisfied. This A-module is denoted by $\mathrm{Hom}_A(M, N)$ (or just $\mathrm{Hom}(M, N)$ if there is no ambiguity about the ring A).

Homomorphisms $u\colon M' \to M$ and $v\colon N \to N''$ induce mappings

$$\bar{u}\colon \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N) \quad \text{and} \quad \bar{v}\colon \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'')$$

defined as follows:

$$\bar{u}(f) = f \circ u, \quad \bar{v}(f) = v \circ f.$$

These mappings are A-module homomorphisms.

For any module M there is a natural isomorphism $\mathrm{Hom}(A, M) \cong M$: any A-module homomorphism $f\colon A \to M$ is uniquely determined by $f(1)$, which can be any element of M.

SUBMODULES AND QUOTIENT MODULES

A *submodule* M' of M is a subgroup of M which is closed under multiplication by elements of A. The abelian group M/M' then inherits an A-module structure from M, defined by $a(x + M') = ax + M'$. The A-module M/M' is the *quotient* of M by M'. The natural map of M onto M/M' is an A-module homomorphism. There is a one-to-one order-preserving correspondence between submodules of M which contain M', and submodules of M'' (just as for ideals; the statement for ideals is a special case).

If $f\colon M \to N$ is an A-module homomorphism, the *kernel* of f is the set

$$\mathrm{Ker}(f) = \{x \in M : f(x) = 0\}$$

and is a submodule of M. The *image* of f is the set

$$\mathrm{Im}(f) = f(M)$$

and is a submodule of N. The *cokernel* of f is

$$\mathrm{Coker}(f) = N/\mathrm{Im}(f)$$

which is a quotient module of N.

If M' is a submodule of M such that $M' \subseteq \mathrm{Ker}(f)$, then f gives rise to a homomorphism $\bar{f}: M/M' \to N$, defined as follows: if $\bar{x} \in M/M'$ is the image of $x \in M$, then $\bar{f}(\bar{x}) = f(x)$. The kernel of $\bar{f}$ is $\mathrm{Ker}(f)/M'$. The homomorphism $\bar{f}$ is said to be *induced* by f. In particular, taking $M' = \mathrm{Ker}(f)$, we have an isomorphism of A-modules

$$M/\mathrm{Ker}(f) \cong \mathrm{Im}(f).$$

OPERATIONS ON SUBMODULES

Most of the operations on ideals considered in Chapter 1 have their counterparts for modules. Let M be an A-module and let $(M_i)_{i \in I}$ be a family of submodules of M. Their *sum* $\sum M_i$ is the set of all (finite) sums $\sum x_i$, where $x_i \in M_i$ for all $i \in I$, and almost all the x_i (that is, all but a finite number) are zero. $\sum M_i$ is the smallest submodule of M which contains all the M_i.

The intersection $\bigcap M_i$ is again a submodule of M. Thus the submodules of M form a complete lattice with respect to inclusion.

Proposition 2.1. i) *If $L \supseteq M \supseteq N$ are A-modules, then*

$$(L/N)/(M/N) \cong L/M.$$

ii) *If M_1, M_2 are submodules of M, then*

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

Proof. i) Define $\theta: L/N \to L/M$ by $\theta(x + N) = x + M$. Then θ is a well-defined A-module homomorphism of L/N onto L/M, and its kernel is M/N; hence (i).

ii) The composite homomorphism $M_2 \to M_1 + M_2 \to (M_1 + M_2)/M_1$ is surjective, and its kernel is $M_1 \cap M_2$; hence (ii). ∎

We cannot in general define the *product* of two submodules, but we can define the product $\mathfrak{a}M$, where $\mathfrak{a}$ is an ideal and M an A-module; it is the set of all finite sums $\sum a_i x_i$ with $a_i \in \mathfrak{a}$, $x_i \in M$, and is a submodule of M.

If N, P are submodules of M, we define $(N:P)$ to be the set of all $a \in A$ such that $aP \subseteq N$; it is an *ideal* of A. In particular, $(0:M)$ is the set of all $a \in A$ such that $aM = 0$; this ideal is called the *annihilator* of M and is also denoted by $\mathrm{Ann}(M)$. If $\mathfrak{a} \subseteq \mathrm{Ann}(M)$, we may regard M as an $A/\mathfrak{a}$-module, as follows: if $\bar{x} \in A/\mathfrak{a}$ is represented by $x \in A$, define $\bar{x}m$ to be xm $(m \in M)$: this is independent of the choice of the representative x of $\bar{x}$, since $\mathfrak{a}M = 0$.

An A-module is *faithful* if $\mathrm{Ann}(M)=0$. If $\mathrm{Ann}(M) = \mathfrak{a}$, then M is faithful as an $A/\mathfrak{a}$-module.

Exercise 2.2. i) $\mathrm{Ann}(M + N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$.

ii) $(N:P) = \mathrm{Ann}\big((N + P)/N\big)$.

If x is an element of M, the set of all multiples $ax (a \in A)$ is a submodule of M, denoted by Ax or (x). If $M = \sum_{i\in I} Ax_i$, the x_i are said to be a *set of generators* of M; this means that every element of M can be expressed (not necessarily uniquely) as a finite linear combination of the x_i with coefficients in A. An A-module M is said to be *finitely generated* if it has a finite set of generators.

DIRECT SUM AND PRODUCT

If M, N are A-modules, their *direct sum* $M \oplus N$ is the set of all pairs (x, y) with $x \in M$, $y \in N$. This is an A-module if we define addition and scalar multiplication in the obvious way:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$a(x, y) = (ax, ay).$$

More generally, if $(M_i)_{i\in I}$ is any family of A-modules, we can define their *direct sum* $\bigoplus_{i\in I} M_i$; its elements are families $(x_i)_{i\in I}$ such that $x_i \in M_i$ for each $i \in I$ and almost all x_i are 0. If we drop the restriction on the number of non-zero x's we have the *direct product* $\prod_{i\in I} M_i$. Direct sum and direct product are therefore the same if the index set I is finite, but not otherwise, in general.

Suppose that the ring A is a direct product $\prod_{i=1}^{n} A_i$ (Chapter 1). Then the set of all elements of A of the form

$$(0, \ldots, 0, a_i, 0, \ldots, 0)$$

with $a_i \in A_i$ is an *ideal* $\mathfrak{a}_i$ of A (it is *not* a subring of A—except in trivial cases—because it does not contain the identity element of A). The ring A, considered as an A-module, is the direct sum of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$. Conversely, given a module decomposition

$$A = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$$

of A as a direct sum of ideals, we have

$$A \cong \prod_{i=1}^{n} (A/\mathfrak{b}_i)$$

where $\mathfrak{b}_i = \bigoplus_{j\neq i} \mathfrak{a}_j$. Each ideal $\mathfrak{a}_i$ is a ring (isomorphic to $A/\mathfrak{b}_i$). The identity element e_i of $\mathfrak{a}_i$ is an idempotent in A, and $\mathfrak{a}_i = (e_i)$.

FINITELY GENERATED MODULES

A *free* A-module is one which is isomorphic to an A-module of the form $\bigoplus_{i \in I} M_i$, where each $M_i \cong A$ (as an A-module). The notation $A^{(I)}$ is sometimes used. A finitely generated free A-module is therefore isomorphic to $A \oplus \cdots \oplus A$ (n summands), which is denoted by A^n. (Conventionally, A^0 is the zero module, denoted by 0.)

Proposition 2.3. *M is a finitely generated A-module $\Leftrightarrow$ M is isomorphic to a quotient of A^n for some integer $n > 0$.*

Proof. $\Rightarrow$: Let $x_1, \ldots, x_n$ generate M. Define $\phi: A^n \to M$ by $\phi(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n$. Then ϕ is an A-module homomorphism *onto* M, and therefore $M \cong A^n/\mathrm{Ker}\,(\phi)$.

$\Leftarrow$: We have an A-module homomorphism ϕ of A^n onto M. If $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (the 1 being in the ith place), then the e_i ($1 \leqslant i \leqslant n$) generate A^n, hence the $\phi(e_i)$ generate M. ∎

Proposition 2.4. *Let M be a finitely generated A-module, let $\mathfrak{a}$ be an ideal of A, and let ϕ be an A-module endomorphism of M such that $\phi(M) \subseteq \mathfrak{a}M$. Then ϕ satisfies an equation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

where the a_i are in $\mathfrak{a}$.

Proof. Let $x_1, \ldots, x_n$ be a set of generators of M. Then each $\phi(x_i) \in \mathfrak{a}M$, so that we have say $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ ($1 \leqslant i \leqslant n$; $a_{ij} \in \mathfrak{a}$), i.e.,

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})x_j = 0$$

where δ_{ij} is the Kronecker delta. By multiplying on the left by the adjoint of the matrix $(\delta_{ij}\phi - a_{ij})$ it follows that $\det(\delta_{ij}\phi - a_{ij})$ annihilates each x_i, hence is the zero endomorphism of M. Expanding out the determinant, we have an equation of the required form. ∎

Corollary 2.5. *Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal of A such that $\mathfrak{a}M = M$. Then there exists $x \equiv 1 (\mathrm{mod}\ \mathfrak{a})$ such that $xM = 0$.*

Proof. Take ϕ = identity, $x = 1 + a_1 + \cdots + a_n$ in (2.4). ∎

Proposition 2.6. (*Nakayama's lemma*). *Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A contained in the Jacobson radical $\mathfrak{R}$ of A. Then $\mathfrak{a}M = M$ implies $M = 0$.*

First Proof. By (2.5) we have $xM = 0$ for some $x \equiv 1 \ (\mathrm{mod}\ \mathfrak{R})$. By (1.9) x is a unit in A, hence $M = x^{-1}xM = 0$. ∎

Second Proof. Suppose $M \neq 0$, and let $u_1, \dots, u_n$ be a minimal set of generators of M. Then $u_n \in \mathfrak{a}M$, hence we have an equation of the form $u_n = a_1u_1 + \cdots + a_nu_n$, with the $a_i \in \mathfrak{a}$. Hence

$$(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1};$$

since $a_n \in \mathfrak{R}$, it follows from (1.9) that $1 - a_n$ is a unit in A. Hence u_n belongs to the submodule of M generated by $u_1, \dots, u_{n-1}$: contradiction. ∎

Corollary 2.7. *Let M be a finitely generated A-module, N a submodule of M, $\mathfrak{a} \subseteq \mathfrak{R}$ an ideal. Then $M = \mathfrak{a}M + N \Rightarrow M = N$.*

Proof. Apply (2.6) to M/N, observing that $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N$. ∎

Let A be a local ring, $\mathfrak{m}$ its maximal ideal, $k = A/\mathfrak{m}$ its residue field. Let M be a finitely generated A-module. $M/\mathfrak{m}M$ is annihilated by $\mathfrak{m}$, hence is naturally an $A/\mathfrak{m}$-module, i.e., a k-vector space, and as such is finite-dimensional.

Proposition 2.8. *Let x_i $(1 \leqslant i \leqslant n)$ be elements of M whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then the x_i generate M.*

Proof. Let N be the submodule of M generated by the x_i. Then the composite map $N \to M \to M/\mathfrak{m}M$ maps N onto $M/\mathfrak{m}M$, hence $N + \mathfrak{m}M = M$, hence $N = M$ by (2.7). ∎

EXACT SEQUENCES

A sequence of A-modules and A-homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots \qquad (0)$$

is said to be *exact at* M_i if $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. The sequence is *exact* if it is exact at each M_i. In particular:

$0 \to M' \xrightarrow{f} M$ is exact $\Leftrightarrow f$ is injective; (1)

$M \xrightarrow{g} M'' \to 0$ is exact $\Leftrightarrow g$ is surjective; (2)

$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact $\Leftrightarrow f$ is injective, g is surjective and g induces an isomorphism of $\mathrm{Coker}(f) = M/f(M')$ onto M''. (3)

A sequence of type (3) is called a *short exact sequence*. Any long exact sequence (0) can be split up into short exact sequences: if $N_i = \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$, we have short exact sequences $0 \to N_i \to M_i \to N_{i+1} \to 0$ for each i.

Proposition 2.9. i) *Let*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0 \qquad (4)$$

be a sequence of A-modules and homomorphisms. Then the sequence (4) *is exact $\Leftrightarrow$ for all A-modules N, the sequence*

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N) \qquad (4')$$

is exact.

ii) *Let*

$$0 \to N' \xrightarrow{u} N \xrightarrow{v} N'' \tag{5}$$

be a sequence of A-modules and homomorphisms. Then the sequence (5) *is exact* $\Leftrightarrow$ *for all A-modules M, the sequence*

$$0 \to \operatorname{Hom}(M, N') \xrightarrow{\bar{u}} \operatorname{Hom}(M, N) \xrightarrow{\bar{v}} \operatorname{Hom}(M, N'') \tag{5'}$$

is exact.

All four parts of this proposition are easy exercises. For example, suppose that (4′) is exact for all N. First of all, since $\bar{v}$ is injective for all N it follows that v is surjective. Next, we have $\bar{u} \circ \bar{v} = 0$, that is $v \circ u \circ f = 0$ for all $f: M'' \to N$. Taking N to be M'' and f to be the identity mapping, it follows that $v \circ u = 0$, hence $\operatorname{Im}(u) \subseteq \operatorname{Ker}(v)$. Next take $N = M/\operatorname{Im}(u)$ and let $\phi: M \to N$ be the projection. Then $\phi \in \operatorname{Ker}(\bar{u})$, hence there exists $\psi: M'' \to N$ such that $\phi = \psi \circ v$. Consequently $\operatorname{Im}(u) = \operatorname{Ker}(\phi) \supseteq \operatorname{Ker}(v)$. ∎

Proposition 2.10. *Let*

$$\begin{array}{ccccccccc}
0 & \to & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \to & 0 \\
 & & {\scriptstyle f'}\downarrow & & {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f''} & & \\
0 & \to & N' & \xrightarrow[u']{} & N & \xrightarrow[v']{} & N'' & \to & 0
\end{array}$$

be a commutative diagram of A-modules and homomorphisms, with the rows exact. Then there exists an exact sequence

$$0 \to \operatorname{Ker}(f') \xrightarrow{\bar{u}} \operatorname{Ker}(f) \xrightarrow{\bar{v}} \operatorname{Ker}(f'') \xrightarrow{d} \operatorname{Coker}(f') \xrightarrow{\bar{u}'} \operatorname{Coker}(f) \xrightarrow{\bar{v}'} \operatorname{Coker}(f'') \to 0 \tag{6}$$

in which $\bar{u}$, $\bar{v}$ are restrictions of u, v, and $\bar{u}'$, $\bar{v}'$ are induced by u', v'.

The *boundary homomorphism* d is defined as follows: if $x'' \in \operatorname{Ker}(f'')$, we have $x'' = v(x)$ for some $x \in M$, and $v'(f(x)) = f''(v(x)) = 0$, hence $f(x) \in \operatorname{Ker}(v') = \operatorname{Im}(u')$, so that $f(x) = u'(y')$ for some $y' \in N'$. Then $d(x'')$ is defined to be the image of y' in $\operatorname{Coker}(f')$. The verification that d is well-defined, and that the sequence (6) is exact, is a straightforward exercise in diagram-chasing which we leave to the reader. ∎

Remark. (2.10) is a special case of the exact homology sequence of homological algebra.

Let C be a class of A-modules and let λ be a function on C with values in $\mathbf{Z}$ (or, more generally, with values in an abelian group G). The function λ is *additive* if, for each short exact sequence (3) in which all the terms belong to C, we have $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Example. Let A be a field k, and let C be the class of all finite-dimensional k-vector spaces V. Then $V \mapsto \dim V$ is an additive function on C.

Proposition 2.11. *Let $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ be an exact sequence of A-modules in which all the modules M_i and the kernels of all the homomorphisms belong to C. Then for any additive function λ on C we have*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

Proof. Split up the sequence into short exact sequences

$$0 \to N_i \to M_i \to N_{i+1} \to 0$$

($N_0 = N_{n+1} = 0$). Then we have $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$. Now take the alternating sum of the $\lambda(M_i)$, and everything cancels out. ∎

TENSOR PRODUCT OF MODULES

Let M, N, P be three A-modules. A mapping $f: M \times N \to P$ is said to be *A-bilinear* if for each $x \in M$ the mapping $y \mapsto f(x, y)$ of N into P is A-linear, and for each $y \in N$ the mapping $x \mapsto f(x, y)$ of M into P is A-linear.

We shall construct an A-module T, called the *tensor product* of M and N, with the property that the A-bilinear mappings $M \times N \to P$ are in a natural one-to-one correspondence with the A-linear mappings $T \to P$, for all A-modules P. More precisely:

Proposition 2.12. *Let M, N be A-modules. Then there exists a pair (T, g) consisting of an A-module T and an A-bilinear mapping $g: M \times N \to T$, with the following property:*

Given any A-module P and any A-bilinear mapping $f: M \times N \to P$, there exists a unique A-linear mapping $f': T \to P$ such that $f = f' \circ g$ (in other words, every bilinear function on $M \times N$ factors through T).

Moreover, if (T, g) and (T', g') are two pairs with this property, then there exists a unique isomorphism $j: T \to T'$ such that $j \circ g = g'$.

Proof. i) *Uniqueness.* Replacing (P, f) by (T', g') we get a unique $j: T \to T'$ such that $g' = j \circ g$. Interchanging the roles of T and T', we get $j': T' \to T$ such that $g = j' \circ g'$. Each of the compositions $j \circ j', j' \circ j$ must be the identity, and therefore j is an isomorphism.

ii) *Existence.* Let C denote the free A-module $A^{(M \times N)}$. The elements of C are formal linear combinations of elements of $M \times N$ with coefficients in A, i.e. they are expressions of the form $\sum_{i=1}^{n} a_i \cdot (x_i, y_i) (a_i \in A, x_i \in M, y_i \in N)$.

Let D be the submodule of C generated by all elements of C of the following types:

$$\begin{gathered}
(x + x', y) - (x, y) - (x', y) \\
(x, y + y') - (x, y) - (x, y') \\
(ax, y) - a \cdot (x, y) \\
(x, ay) - a \cdot (x, y).
\end{gathered}$$

Let $T = C/D$. For each basis element (x, y) of C, let $x \otimes y$ denote its image in T. Then T is generated by the elements of the form $x \otimes y$, and from our definitions we have

$$(x + x') \otimes y = x \otimes y + x' \otimes y, \quad x \otimes (y + y') = x \otimes y + x \otimes y',$$
$$(ax) \otimes y = x \otimes (ay) = a(x \otimes y)$$

Equivalently, the mapping $g: M \times N \to T$ defined by $g(x, y) = x \otimes y$ is A-bilinear.

Any map f of $M \times N$ into an A-module P extends by linearity to an A-module homomorphism $\bar{f}: C \to P$. Suppose in particular that f is A-bilinear. Then, from the definitions, $\bar{f}$ vanishes on all the generators of D, hence on the whole of D, and therefore induces a well-defined A-homomorphism f' of $T = C/D$ into P such that $f'(x \otimes y) = f(x, y)$. The mapping f' is uniquely defined by this condition, and therefore the pair (T, g) satisfy the conditions of the proposition. ∎

Remarks. i) The module T constructed above is called the *tensor product* of M and N, and is denoted by $M \otimes_A N$, or just $M \otimes N$ if there is no ambiguity about the ring A. It is generated as an A-module by the "products" $x \otimes y$. If $(x_i)_{i \in I}$, $(y_j)_{j \in J}$ are families of generators of M, N respectively, then the elements $x_i \otimes y_j$ generate $M \otimes N$. In particular, if M and N are finitely generated, so is $M \otimes N$.

ii) The notation $x \otimes y$ is inherently ambiguous unless we specify the tensor product to which it belongs. Let M', N' be submodules of M, N respectively, and let $x \in M'$ and $y \in N'$. Then it can happen that $x \otimes y$ as an element of $M \otimes N$ is zero whilst $x \otimes y$ *as an element of* $M' \otimes N'$ is non-zero. For example, take $A = \mathbf{Z}$, $M = \mathbf{Z}$, $N = \mathbf{Z}/2\mathbf{Z}$, and let M' be the submodule $2\mathbf{Z}$ of $\mathbf{Z}$, whilst $N' = N$. Let x be the non-zero element of N and consider $2 \otimes x$. As an element of $M \otimes N$, it is zero because $2 \otimes x = 1 \otimes 2x = 1 \otimes 0 = 0$. But as an element of $M' \otimes N'$ it is non-zero. See the example after (2.18).

However, there is the following result:

Corollary 2.13. *Let $x_i \in M$, $y_i \in N$ be such that $\sum x_i \otimes y_i = 0$ in $M \otimes N$. Then there exist finitely generated submodules M_0 of M and N_0 of N such that $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$.*

Proof. If $\sum x_i \otimes y_i = 0$ in $M \otimes N$, then in the notation of the proof of (2.11) we have $\sum (x_i, y_i) \in D$, and therefore $\sum (x_i, y_i)$ is a finite sum of generators of D. Let M_0 be the submodule of M generated by the x_i and all the elements of M which occur as first coordinates in these generators of D, and define N_0 similarly. Then $\sum x_i \otimes y_i = 0$ as an element of $M_0 \otimes N_0$. ∎

iii) We shall never again need to use the construction of the tensor product given in (2.12), and the reader may safely forget it if he prefers. What is essential to keep in mind is the defining property of the tensor product.

iv) Instead of starting with bilinear mappings we could have started with multilinear mappings $f: M_1 \times \cdots \times M_r \to P$ defined in the same way (i.e., linear in each variable). Following through the proof of (2.12) we should end up with a "multi-tensor product" $T = M_1 \otimes \cdots \otimes M_r$, generated by all products $x_1 \otimes \cdots \otimes x_r$ $(x_i \in M_i, 1 \leqslant i \leqslant r)$. The details may safely be left to the reader; the result corresponding to (2.12) is

Proposition 2.12*. *Let $M_1, \ldots, M_r$ be A-modules. Then there exists a pair (T, g) consisting of an A-module T and an A-multilinear mapping $g: M_1 \times \cdots \times M_r \to T$ with the following property:*

Given any A-module P and any A-multilinear mapping $f: M_1 \times \cdots \times M_r \to T$, there exists a unique A-homomorphism $f': T \to P$ such that $f' \circ g = f$.

Moreover, if (T, g) and (T', g') are two pairs with this property, then there exists a unique isomorphism $j: T \to T'$ such that $j \circ g = g'$. ∎

There are various so-called "canonical isomorphisms", some of which we state here:

Proposition 2.14. *Let M, N, P be A-modules. Then there exist unique isomorphisms*

i) $M \otimes N \to N \otimes M$

ii) $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$

iii) $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$

iv) $A \otimes M \to M$

such that, respectively,

a) $x \otimes y \mapsto y \otimes x$

b) $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$

c) $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$

d) $a \otimes x \mapsto ax$.

Proof. In each case the point is to show that the mappings so described are well defined. The technique is to construct suitable bilinear or multilinear mappings, and use the defining property (2.12) or (2.12*) to infer the existence of homomorphisms of tensor products. We shall prove half of ii) as an example of the method, and leave the rest to the reader.

We shall construct homomorphisms

$$(M \otimes N) \otimes P \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} (M \otimes N) \otimes P$$

such that $f((x \otimes y) \otimes z) = x \otimes y \otimes z$ and $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$ for all $x \in M, y \in N, z \in P$.

To construct f, fix the element $z \in P$. The mapping $(x, y) \mapsto x \otimes y \otimes z$ $(x \in M, y \in N)$ is bilinear in x and y and therefore induces a homomorphism

$f_z \colon M \otimes N \to M \otimes N \otimes P$ such that $f_z(x \otimes y) = x \otimes y \otimes z$. Next, consider the mapping $(t, z) \mapsto f_z(t)$ of $(M \otimes N) \times P$ into $M \otimes N \otimes P$. This is bilinear in t and z and therefore induces a homomorphism

$$f \colon (M \otimes N) \otimes P \to M \otimes N \otimes P$$

such that $f\big((x \otimes y) \otimes z\big) = x \otimes y \otimes z$.

To construct g, consider the mapping $(x, y, z) \mapsto (x \otimes y) \otimes z$ of $M \times N \times P$ into $(M \otimes N) \otimes P$. This is linear in each variable and therefore induces a homomorphism

$$g \colon M \otimes N \otimes P \to (M \otimes N) \otimes P$$

such that $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$.

Clearly $f \circ g$ and $g \circ f$ are identity maps, hence f and g are isomorphisms. ∎

Exercise 2.15. *Let A, B be rings, let M be an A-module, P a B-module and N an (A, B)-bimodule (that is, N is simultaneously an A-module and a B-module and the two structures are compatible in the sense that $a(xb) = (ax)b$ for all $a \in A$, $b \in B$, $x \in N$). Then $M \otimes_A N$ is naturally a B-module, $N \otimes_B P$ an A-module, and we have*

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

Let $f \colon M \to M'$, $g \colon N \to N'$ be homomorphisms of A-modules. Define $h \colon M \times N \to M' \otimes N'$ by $h(x, y) = f(x) \otimes g(y)$. It is easily checked that h is A-bilinear and therefore induces an A-module homomorphism

$$f \otimes g \colon M \otimes N \to M' \otimes N'$$

such that

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y) \qquad (x \in M, \quad y \in N).$$

Let $f' \colon M' \to M''$ and $g' \colon N' \to N''$ be homomorphisms of A-modules. Then clearly the homomorphisms $(f' \circ f) \otimes (g' \circ g)$ and $(f' \otimes g') \circ (f \otimes g)$ agree on all elements of the form $x \otimes y$ in $M \otimes N$. Since these elements generate $M \otimes N$, it follows that

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g).$$

RESTRICTION AND EXTENSION OF SCALARS

Let $f \colon A \to B$ be a homomorphism of rings and let N be a B-module. Then N has an A-module structure defined as follows: if $a \in A$ and $x \in N$, then ax is defined to be $f(a)x$. This A-module is said to be obtained from N by *restriction of scalars*. In particular, f defines in this way an A-module structure on B.

Proposition 2.16. *Suppose N is finitely generated as a B-module and that B is finitely generated as an A-module. Then N is finitely generated as an A-module.*

Proof. Let $y_1, \ldots, y_n$ generate N over B, and let $x_1, \ldots, x_m$ generate B as an A-module. Then the mn products $x_i y_j$ generate N over A. ∎

Now let M be an A-module. Since, as we have just seen, B can be regarded as an A-module, we can form the A-module $M_B = B \otimes_A M$. In fact M_B carries a B-module structure such that $b(b' \otimes x) = bb' \otimes x$ for all $b, b' \in B$ and all $x \in M$. The B-module M_B is said to be obtained from M by *extension of scalars*.

Proposition 2.17. *If M is finitely generated as an A-module, then M_B is finitely generated as a B-module.*

Proof. If $x_1, \ldots, x_m$ generate M over A, then the $1 \otimes x_i$ generate M_B over B. ∎

EXACTNESS PROPERTIES OF THE TENSOR PRODUCT

Let $f: M \times N \to P$ be an A-bilinear mapping. For each $x \in M$ the mapping $y \mapsto f(x, y)$ of N into P is A-linear, hence f gives rise to a mapping $M \to \operatorname{Hom}(N, P)$ which is A-linear because f is linear in the variable x. Conversely any A-homomorphism $\phi: M \to \operatorname{Hom}_A(N, P)$ defines a bilinear map, namely $(x, y) \mapsto \phi(x)(y)$. Hence the set S of A-bilinear mappings $M \times N \to P$ is in natural one-to-one correspondence with $\operatorname{Hom}(M, \operatorname{Hom}(N, P))$. On the other hand S is in one-to-one correspondence with $\operatorname{Hom}(M \otimes N, P)$, by the defining property of the tensor product. Hence we have a canonical isomorphism

$$\operatorname{Hom}(M \otimes N, P) \cong \operatorname{Hom}(M, \operatorname{Hom}(N, P)). \tag{1}$$

Proposition 2.18. *Let*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{2}$$

be an exact sequence of A-modules and homomorphisms, and let N be any A-module. Then the sequence

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0 \tag{3}$$

(where 1 denotes the identity mapping on N) is exact.

Proof. Let E denote the sequence (2), and let $E \otimes N$ denote the sequence (3). Let P be any A-module. Since (2) is exact, the sequence $\operatorname{Hom}(E, \operatorname{Hom}(N, P))$ is exact by (2.9); hence by (1) the sequence $\operatorname{Hom}(E \otimes N, P)$ is exact. By (2.9) again, it follows that $E \otimes N$ is exact. ∎

Remarks. i) Let $T(M) = M \otimes N$ and let $U(P) = \operatorname{Hom}(N, P)$. Then (1) takes the form $\operatorname{Hom}(T(M), P) = \operatorname{Hom}(M, U(P))$ for all A-modules M and P. In the language of abstract nonsense, the functor T is the left adjoint of U, and U is the right adjoint of T. The proof of (2.18) shows that any functor which is a left adjoint is right exact. Likewise any functor which is a right adjoint is left exact.

ii) It is *not* in general true that, if $M' \to M \to M''$ is an exact sequence of A-modules and homomorphisms, the sequence $M' \otimes N \to M \otimes N \to M'' \otimes N$ obtained by tensoring with an arbitrary A-module N is exact.

Example. Take $A = \mathbf{Z}$ and consider the exact sequence $0 \to \mathbf{Z} \xrightarrow{f} \mathbf{Z}$, where $(x) = 2x$ for all $x \in \mathbf{Z}$. If we tensor with $N = \mathbf{Z}/2\mathbf{Z}$, the sequence $0 \to \mathbf{Z} \otimes \xrightarrow{f\otimes 1} \mathbf{Z} \otimes N$ is *not* exact, because for any $x \otimes y \in \mathbf{Z} \otimes N$ we have

$$(f \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0,$$

so that $f \otimes 1$ is the zero mapping, whereas $\mathbf{Z} \otimes N \neq 0$.

The functor $T_N: M \mapsto M \otimes_A N$ on the category of A-modules and homomorphisms is therefore not in general exact. If T_N is exact, that is to say if tensoring with N transforms all exact sequences into exact sequences, then N is said to be a *flat* A-module.

Proposition 2.19. *The following are equivalent, for an A-module N:*

i) *N is flat.*

ii) *If $0 \to M' \to M \to M'' \to 0$ is any exact sequence of A-modules, the tensored sequence $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact.*

iii) *If f: $M' \to M$ is injective, then $f \otimes 1: M' \otimes N \to M \otimes N$ is injective.*

iv) *If f: $M' \to M$ is injective and M, M' are finitely generated, then $f \otimes 1: M' \otimes N \to M \otimes N$ is injective.*

Proof. i) $\Leftrightarrow$ ii) by splitting up a long exact sequence into short exact sequences.

ii) $\Leftrightarrow$ iii) by (2.18).

iii) $\Rightarrow$ iv): clear.

iv) $\Rightarrow$ iii). Let f: $M' \to M$ be injective and let $u = \sum x_i \otimes y_i \in \operatorname{Ker}(f \otimes 1)$, so that $\sum f(x_i') \otimes y_i = 0$ in $M \otimes N$. Let M_0' be the submodule of M' generated by the x_i' and let u_0 denote $\sum x_i' \otimes y_i$ as an element of $M_0' \otimes N$. By (2.14) there exists a finitely generated submodule M_0 of M containing $f(M_0')$ and such that $\sum f(x_i') \otimes y_i = 0$ as an element of $M_0 \otimes N$. If f_0: $M_0' \to M_0$ is the restriction of f, this means that $(f_0 \otimes 1)(u_0) = 0$. Since M_0 and M_0' are finitely generated, $f_0 \otimes 1$ is injective and therefore $u_0 = 0$, hence $u = 0$. ∎

Exercise 2.20. *If f: $A \to B$ is a ring homomorphism and M is a flat A-module, then $M_B = B \otimes_A M$ is a flat B-module.* (Use the canonical isomorphisms (2.14), (2.15).)

ALGEBRAS

Let f: $A \to B$ be a ring homomorphism. If $a \in A$ and $b \in B$, define a product

$$ab = f(a)b.$$

This definition of scalar multiplication makes the ring B into an A-module (it is a particular example of restriction of scalars). Thus B has an A-module structure as well as a ring structure, and these two structures are compatible in a sense which the reader will be able to formulate for himself. The ring B, equipped with this A-module structure, is said to be an *A-algebra*. Thus an A-algebra is, by definition, a ring B together with a ring homomorphism $f: A \to B$.

Remarks. i) In particular, if A is a field K (and $B \neq 0$) then f is injective by (1.2) and therefore K can be canonically identified with its image in B. Thus a K-algebra (K a field) is effectively a ring containing K as a subring.

ii) Let A be any ring. Since A has an identity element there is a unique homomorphism of the ring of integers $\mathbf{Z}$ into A, namely $n \mapsto n.1$. Thus every ring is automatically a $\mathbf{Z}$-algebra.

Let $f: A \to B$, $g: A \to C$ be two ring homomorphisms. An *A-algebra homomorphism* $h: B \to C$ is a ring homomorphism which is also an A-module homomorphism. The reader should verify that h is an A-algebra homomorphism if and only if $h \circ f = g$.

A ring homomorphism $f: A \to B$ is *finite*, and B is a *finite* A-algebra, if B is finitely generated as an A-module. The homomorphism f is *of finite type*, and B is a *finitely-generated A-algebra*, if there exists a finite set of elements $x_1, \ldots x_n$ in B such that every element of B can be written as a polynomial in $x_1, \ldots, x_n$ with coefficients in $f(A)$; or equivalently if there is an A-algebra homomorphism from a polynomial ring $A[t_1, \ldots, t_n]$ *onto* B.

A ring A is said to be *finitely generated* if it is finitely generated as a $\mathbf{Z}$-algebra. This means that there exist finitely many elements $x_1, \ldots, x_n$ in A such that every element of A can be written as a polynomial in the x_i with rational integer coefficients.

TENSOR PRODUCT OF ALGEBRAS

Let B, C be two A-algebras, $f: A \to B$, $g: A \to C$ the corresponding homomorphisms. Since B and C are A-modules we may form their tensor product $D = B \otimes_A C$, which is an A-module. We shall now define a multiplication on D.

Consider the mapping $B \times C \times B \times C \to D$ defined by

$$(b, c, b', c') \mapsto bb' \otimes cc'.$$

This is A-linear in each factor and therefore, by (2.12*), induces an A-module homomorphism

$$B \otimes C \otimes B \otimes C \to D,$$

hence by (2.14) an A-module homomorphism

$$D \otimes D \to D$$

and this in turn by (2.11) corresponds to an A-bilinear mapping

$$\mu: D \times D \to D$$

which is such that

$$\mu(b \otimes c, b' \otimes c') = bb' \otimes cc'.$$

Of course, we could have written down this formula directly, but without some such argument as we have given there would be no guarantee that μ was well-defined.

We have therefore defined a multiplication on the tensor product $D = B \otimes_A C$: for elements of the form $b \otimes c$ it is given by

$$(b \otimes c)(b' \otimes c') = bb' \otimes cc',$$

and in general by

$$\Big(\sum_i (b_i \otimes c_i)\Big)\Big(\sum_j (b'_j \otimes c'_j)\Big) = \sum_{i,j} (b_i b'_j \otimes c_i c'_j).$$

The reader should check that with this multiplication D is a commutative ring, with identity element $1 \otimes 1$. Furthermore, D is an A-algebra: the mapping $a \mapsto f(a) \otimes g(a)$ is a ring homomorphism $A \to D$.

In fact there is a commutative diagram of ring homomorphisms

$$\begin{tikzcd} & B \arrow[dr, "u"] & \\ A \arrow[ur, "f"] \arrow[dr, "g"'] & & D \\ & C \arrow[ur, "v"'] & \end{tikzcd}$$

in which u, for example, is defined by $u(b) = b \otimes 1$.

EXERCISES

1. Show that $(\mathbf{Z}/m\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) = 0$ if m, n are coprime.

2. Let A be a ring, $\mathfrak{a}$ an ideal, M an A-module. Show that $(A/\mathfrak{a}) \otimes_A M$ is isomorphic to $M/\mathfrak{a}M$.
[Tensor the exact sequence $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ with M.]

3. Let A be a local ring, M and N finitely generated A-modules. Prove that if $M \otimes N = 0$, then $M = 0$ or $N = 0$.
[Let $\mathfrak{m}$ be the maximal ideal, $k = A/\mathfrak{m}$ the residue field. Let $M_k = k \otimes_A M \cong M/\mathfrak{m}M$ by Exercise 2. By Nakayama's lemma, $M_k = 0 \Rightarrow M = 0$. But $M \otimes_A N = 0 \Rightarrow (M \otimes_A N)_k = 0 \Rightarrow M_k \otimes_k N_k = 0 \Rightarrow M_k = 0$ or $N_k = 0$, since M_k, N_k are vector spaces over a field.]

4. Let M_i $(i \in I)$ be any family of A-modules, and let M be their direct sum. Prove that M is flat $\Leftrightarrow$ each M_i is flat.

5. Let $A[x]$ be the ring of polynomials in one indeterminate over a ring A. Prove that $A[x]$ is a flat A-algebra. [Use Exercise 4.]

6. For any A-module, let $M[x]$ denote the set of all polynomials in x with coefficients in M, that is to say expressions of the form

$$m_0 + m_1 x + \cdots + m_r x^r \qquad (m_i \in M).$$

Defining the product of an element of $A[x]$ and an element of $M[x]$ in the obvious way, show that $M[x]$ is an $A[x]$-module.

Show that $M[x] \cong A[x] \otimes_A M$.

7. Let $\mathfrak{p}$ be a prime ideal in A. Show that $\mathfrak{p}[x]$ is a prime ideal in $A[x]$. If $\mathfrak{m}$ is a maximal ideal in A, is $\mathfrak{m}[x]$ a maximal ideal in $A[x]$?

8. i) If M and N are flat A-modules, then so is $M \otimes_A N$.
ii) If B is a flat A-algebra and N is a flat B-module, then N is flat as an A-module.

9. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of A-modules. If M' and M'' are finitely generated, then so is M.

10. Let A be a ring, $\mathfrak{a}$ an ideal contained in the Jacobson radical of A; let M be an A-module and N a finitely generated A-module, and let $u: M \to N$ be a homomorphism. If the induced homomorphism $M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, then u is surjective.

11. Let A be a ring $\neq 0$. Show that $A^m \cong A^n \Rightarrow m = n$.
[Let $\mathfrak{m}$ be a maximal ideal of A and let $\phi: A^m \to A^n$ be an isomorphism. Then $1 \otimes \phi: (A/\mathfrak{m}) \otimes A^m \to (A/\mathfrak{m}) \otimes A^n$ is an isomorphism between vector spaces of dimensions m and n over the field $k = A/\mathfrak{m}$. Hence $m = n$.] (Cf. Chapter 3, Exercise 15.)

If $\phi: A^m \to A^n$ is surjective, then $m \geqslant n$.

If $\phi: A^m \to A^n$ is injective, is it always the case that $m \leqslant n$?

12. Let M be a finitely generated A-module and $\phi: M \to A^n$ a surjective homomorphism. Show that Ker (ϕ) is finitely generated.
[Let $e_1, \ldots, e_n$ be a basis of A^n and choose $u_i \in M$ such that $\phi(u_i) = e_i$ $(1 \leqslant i \leqslant n)$. Show that M is the direct sum of Ker (ϕ) and the submodule generated by $u_1, \ldots, u_n$.]

13. Let $f: A \to B$ be a ring homomorphism, and let N be a B-module. Regarding N as an A-module by restriction of scalars, form the B-module $N_B = B \otimes_A N$. Show that the homomorphism $g: N \to N_B$ which maps y to $1 \otimes y$ is injective and that $g(N)$ is a direct summand of N_B.
[Define $p: N_B \to N$ by $p(b \otimes y) = by$, and show that $N_B = \text{Im}(g) \oplus \text{Ker}(p)$.]

Direct limits

14. A partially ordered set I is said to be a *directed* set if for each pair i, j in I there exists $k \in I$ such that $i \leqslant k$ and $j \leqslant k$.

Let A be a ring, let I be a directed set and let $(M_i)_{i \in I}$ be a family of A-modules indexed by I. For each pair i, j in I such that $i \leqslant j$, let $\mu_{ij}: M_i \to M_j$ be an A-homomorphism, and suppose that the following axioms are satisfied:

(1) μ_{ii} is the identity mapping of M_i, for all $i \in I$;

(2) $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ whenever $i \leqslant j \leqslant k$.

Then the modules M_i and homomorphisms μ_{ij} are said to form a *direct system* $\mathbf{M} = (M_i, \mu_{ij})$ over the directed set I.

We shall construct an A-module M called the *direct limit* of the direct system $\mathbf{M}$. Let C be the direct sum of the M_i, and identify each module M_i with its canonical image in C. Let D be the submodule of C generated by all elements of the form $x_i - \mu_{ij}(x_i)$ where $i \leqslant j$ and $x_i \in M_i$. Let $M = C/D$, let $\mu: C \to M$ be the projection and let μ_i be the restriction of μ to M_i.

The module M, or more correctly the pair consisting of M and the family of homomorphisms $\mu_i: M_i \to M$, is called the *direct limit* of the direct system $\mathbf{M}$, and is written $\varinjlim M_i$. From the construction it is clear that $\mu_i = \mu_j \circ \mu_{ij}$ whenever $i \leqslant j$.

15. In the situation of Exercise 14, show that every element of M can be written in the form $\mu_i(x_i)$ for some $i \in I$ and some $x_i \in M_i$.

Show also that if $\mu_i(x_i) = 0$ then there exists $j \geqslant i$ such that $\mu_{ij}(x_i) = 0$ in M_j.

16. Show that the direct limit is characterized (up to isomorphism) by the following property. Let N be an A-module and for each $i \in I$ let $\alpha_i: M_i \to N$ be an A-module homomorphism such that $\alpha_i = \alpha_j \circ \mu_{ij}$ whenever $i \leqslant j$. Then there exists a unique homomorphism $\alpha: M \to N$ such that $\alpha_i = \alpha \circ \mu_i$ for all $i \in I$.

17. Let $(M_i)_{i \in I}$ be a family of submodules of an A-module, such that for each pair of indices i, j in I there exists $k \in I$ such that $M_i + M_j \subseteq M_k$. Define $i \leqslant j$ to mean $M_i \subseteq M_j$ and let $\mu_{ij}: M_i \to M_j$ be the embedding of M_i in M_j. Show that

$$\varinjlim M_i = \sum M_i = \bigcup M_i.$$

In particular, any A-module is the direct limit of its finitely generated submodules.

18. Let $\mathbf{M} = (M_i, \mu_{ij})$, $\mathbf{N} = (N_i, \nu_{ij})$ be direct systems of A-modules over the same directed set. Let M, N be the direct limits and $\mu_i: M_i \to M$, $\nu_i: N_i \to N$ the associated homomorphisms.

A *homomorphism* $\boldsymbol{\phi}: \mathbf{M} \to \mathbf{N}$ is by definition a family of A-module homomorphisms $\phi_i: M_i \to N_i$ such that $\phi_j \circ \mu_{ij} = \nu_{ij} \circ \phi_i$ whenever $i \leqslant j$. Show that $\boldsymbol{\phi}$ defines a unique homomorphism $\phi = \varinjlim \phi_i: M \to N$ such that $\phi \circ \mu_i = \nu_i \circ \phi_i$ for all $i \in I$.

19. A sequence of direct systems and homomorphisms

$$\mathbf{M} \to \mathbf{N} \to \mathbf{P}$$

is *exact* if the corresponding sequence of modules and module homomorphisms is exact for each $i \in I$. Show that the sequence $M \quad N \to P$ of direct limits is then exact. [Use Exercise 15.]

Tensor products commute with direct limits

20. Keeping the same notation as in Exercise 14, let N be any A-module. Then $(M_i \otimes N, \mu_{ij} \otimes 1)$ is a direct system; let $P = \varinjlim (M_i \otimes N)$ be its direct limit.

For each $i \in I$ we have a homomorphism $\mu_i \otimes 1 : M_i \otimes N \to M \otimes N$, hence by Exercise 16 a homomorphism $\psi: P \to M \otimes N$. Show that ψ is an isomorphism, so that

$$\varinjlim (M_i \otimes N) \cong (\varinjlim M_i) \otimes N.$$

[For each $i \in I$, let $g_i: M_i \times N \to M_i \otimes N$ be the canonical bilinear mapping. Passing to the limit we obtain a mapping $g: M \times N \to P$. Show that g is A-bilinear and hence define a homomorphism $\phi: M \otimes N \to P$. Verify that $\phi \circ \psi$ and $\psi \circ \phi$ are identity mappings.]

21. Let $(A_i)_{i \in I}$ be a family of rings indexed by a directed set I, and for each pair $i \leqslant j$ in I let $\alpha_{ij}: A_i \to A_j$ be a ring homomorphism, satisfying conditions (1) and (2) of Exercise 14. Regarding each A_i as a $\mathbf{Z}$-module we can then form the direct limit $A = \varinjlim A_i$. Show that A inherits a ring structure from the A_i so that the mappings $A_i \to A$ are ring homomorphisms. The ring A is the *direct limit* of the system (A_i, α_{ij}).

If $A = 0$ prove that $A_i = 0$ for some $i \in I$. [Remember that all rings have identity elements!]

22. Let (A_i, α_{ij}) be a direct system of rings and let $\mathfrak{N}_i$ be the nilradical of A_i. Show that $\varinjlim \mathfrak{N}_i$ is the nilradical of $\varinjlim A_i$.

If each A_i is an integral domain, then $\varinjlim A_i$ is an integral domain.

23. Let $(B_\lambda)_{\lambda \in \Lambda}$ be a family of A-algebras. For each finite subset of Λ let B_J denote the tensor product (over A) of the B_λ for $\lambda \in J$. If J' is another finite subset of Λ and $J \subseteq J'$, there is a canonical A-algebra homomorphism $B_J \to B_{J'}$. Let B denote the direct limit of the rings B_J as J runs through all finite subsets of Λ. The ring B has a natural A-algebra structure for which the homomorphisms $B_J \to B$ are A-algebra homomorphisms. The A-algebra B is the *tensor product* of the family $(B_\lambda)_{\lambda \in \Lambda}$.

Flatness and Tor

In these Exercises it will be assumed that the reader is familiar with the definition and basic properties of the Tor functor.

24. If M is an A-module, the following are equivalent:
i) M is flat;
ii) $\mathrm{Tor}_n^A(M, N) = 0$ for all $n > 0$ and all A-modules N;
iii) $\mathrm{Tor}_1^A(M, N) = 0$ for all A-modules N.
[To show that (i) $\Rightarrow$ (ii), take a free resolution of N and tensor it with M. Since M is flat, the resulting sequence is exact and therefore its homology groups, which are the $\mathrm{Tor}_n^A(M, N)$, are zero for $n > 0$. To show that (iii) $\Rightarrow$ (i), let $0 \to N' \to N \to N'' \to 0$ be an exact sequence. Then, from the Tor exact sequence,

$$\mathrm{Tor}_1(M, N'') \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$

is exact. Since $\mathrm{Tor}_1(M, N'') = 0$ it follows that M is flat.]

25. Let $0 \to N' \to N \to N'' \to 0$ be an exact sequence, with N'' flat. Then N' is flat $\Leftrightarrow$ N is flat. [Use Exercise 24 and the Tor exact sequence.]

26. Let N be an A-module. Then N is flat $\Leftrightarrow$ $\mathrm{Tor}_1(A/\mathfrak{a}, N) = 0$ for all finitely generated ideals $\mathfrak{a}$ in A.
[Show first that N is flat if $\mathrm{Tor}_1(M, N) = 0$ for all *finitely generated* A-modules M, by using (2.19). If M is finitely generated, let $x_1, \ldots, x_n$ be a set of generators of M, and let M_i be the submodule generated by $x_1, \ldots, x_i$. By considering the successive quotients M_i/M_{i-1} and using Exercise 25, deduce that N is flat if $\mathrm{Tor}_1(M, N) = 0$ for all *cyclic* A-modules M, i.e., all M generated by a single element, and therefore of the form $A/\mathfrak{a}$ for some ideal $\mathfrak{a}$. Finally use (2.19) again to reduce to the case where $\mathfrak{a}$ is a finitely generated ideal.]

27. A ring A is *absolutely flat* if every A-module is flat. Prove that the following are equivalent:
i) A is absolutely flat.
ii) Every principal ideal is idempotent.
iii) Every finitely generated ideal is a direct summand of A.
[i) $\Rightarrow$ ii). Let $x \in A$. Then $A/(x)$ is a flat A-module, hence in the diagram

$$\begin{array}{ccc} (x) \otimes A & \xrightarrow{\beta} & (x) \otimes A/(x) \\ \downarrow & & \downarrow\alpha \\ A & \longrightarrow & A/(x) \end{array}$$

the mapping α is injective. Hence $\mathrm{Im}(\beta) = 0$, hence $(x) = (x^2)$. ii) $\Rightarrow$ iii). Let $x \in A$. Then $x = ax^2$ for some $a \in A$, hence $e = ax$ is idempotent and we have $(e) = (x)$. Now if e, f are idempotents, then $(e, f) = (e + f - ef)$. Hence every finitely generated ideal is principal, and generated by an idempotent e, hence is a direct summand because $A = (e) \oplus (1 - e)$. iii) $\Rightarrow$ i). Use the criterion of Exercise 26.]

28. A Boolean ring is absolutely flat. The ring of Chapter 1, Exercise 7 is absolutely flat. Every homomorphic image of an absolutely flat ring is absolutely flat. If a local ring is absolutely flat, then it is a field.
If A is absolutely flat, every non-unit in A is a zero-divisor.

3

Rings and Modules of Fractions

The formation of rings of fractions and the associated process of localization are perhaps the most important technical tools in commutative algebra. They correspond in the algebro-geometric picture to concentrating attention on an open set or near a point, and the importance of these notions should be self-evident. This chapter gives the definitions and simple properties of the formation of fractions.

The procedure by which one constructs the rational field **Q** from the ring of integers **Z** (and embeds **Z** in **Q**) extends easily to any integral domain A and produces the *field of fractions* of A. The construction consists in taking all ordered pairs (a, s) where $a, s \in A$ and $s \neq 0$, and setting up an equivalence relation between such pairs:

$$(a, s) \equiv (b, t) \Leftrightarrow at - bs = 0.$$

This works only if A is an integral domain, because the verification that the relation is transitive involves canceling, i.e. the fact that A has no zero-divisor $\neq 0$. However, it can be generalized as follows:

Let A be any ring. A *multiplicatively closed subset* of A is a subset S of A such that $1 \in S$ and S is closed under multiplication: in other words S is a sub-semigroup of the multiplicative semigroup of A. Define a relation $\equiv$ on $A \times S$ as follows:

$$(a, s) \equiv (b, t) \Leftrightarrow (at - bs)u = 0 \text{ for some } u \in S.$$

Clearly this relation is reflexive and symmetric. To show that it is transitive, suppose $(a, s) \equiv (b, t)$ and $(b, t) \equiv (c, u)$. Then there exist v, w in S such that $(at - bs)v = 0$ and $(bu - ct)w = 0$. Eliminate b from these two equations and we have $(au - cs)tvw = 0$. Since S is closed under multiplication, we have $tvw \in S$, hence $(a, s) \equiv (c, u)$. Thus we have an equivalence relation. Let a/s denote the equivalence class of (a, s), and let $S^{-1}A$ denote the set of equivalence classes. We put a ring structure on $S^{-1}A$ by defining addition and multiplication of these "fractions" a/s in the same way as in elementary algebra: that is,

$$(a/s) + (b/t) = (at + bs)/st,$$
$$(a/s)(b/t) = ab/st.$$

Exercise. *Verify that these definitions are independent of the choices of representatives (a, s) and (b, t), and that $S^{-1}A$ satisfies the axioms of a commutative ring with identity.*

We also have a ring homomorphism $f: A \to S^{-1}A$ defined by $f(x) = x/1$. This is *not* in general injective.

Remark. If A is an integral domain and $S = A - \{0\}$, then $S^{-1}A$ is the field of fractions of A.

The ring $S^{-1}A$ is called the *ring of fractions* of A with respect to S. It has a *universal property*:

Proposition 3.1. *Let $g: A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$. Then there exists a unique ring homomorphism $h: S^{-1}A \to B$ such that $g = h \circ f$.*

Proof. i) *Uniqueness.* If h satisfies the conditions, then $h(a/1) = hf(a) = g(a)$ for all $a \in A$; hence, if $s \in S$,

$$h(1/s) = h\big((s/1)^{-1}\big) = h(s/1)^{-1} = g(s)^{-1}$$

and therefore $h(a/s) = h(a/1)\cdot h(1/s) = g(a)g(s)^{-1}$, so that h is uniquely determined by g.

ii) *Existence.* Let $h(a/s) = g(a)g(s)^{-1}$. Then h will clearly be a ring homomorphism provided that it is well-defined. Suppose then that $a/s = a'/s'$; then there exists $t \in S$ such that $(as' - a's)t = 0$, hence

$$\big(g(a)g(s') - g(a')g(s)\big)g(t) = 0;$$

now $g(t)$ is a unit in B, hence $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. ∎

The ring $S^{-1}A$ and the homomorphism $f: A \to S^{-1}A$ have the following properties:

1) $s \in S \Rightarrow f(s)$ is a unit in $S^{-1}A$;
2) $f(a) = 0 \Rightarrow as = 0$ for some $s \in S$;
3) Every element of $S^{-1}A$ is of the form $f(a)f(s)^{-1}$ for some $a \in A$ and some $s \in S$.

Conversely, these three conditions determine the ring $S^{-1}A$ up to isomorphism. Precisely:

Corollary 3.2. *If $g: A \to B$ is a ring homomorphism such that*

i) *$s \in S \Rightarrow g(s)$ is a unit in B;*

ii) *$g(a) = 0 \Rightarrow as = 0$ for some $s \in S$;*

iii) *Every element of B is of the form $g(a)g(s)^{-1}$; then there is a unique isomorphism $h\colon S^{-1}A \to B$ such that $g = h \circ f$.*

Proof. By (3.1) we have to show that $h\colon S^{-1}A \to B$, defined by

$$h(a/s) = g(a)g(s)^{-1}$$

(this definition uses i)) is an isomorphism. By iii), h is surjective. To show h is injective, look at the kernel of h: if $h(a/s) = 0$, then $g(a) = 0$, hence by ii) we have $at = 0$ for some $t \in S$, hence $(a, s) \equiv (0, 1)$, i.e., $a/s = 0$ in $S^{-1}A$. ∎

Examples. 1) Let $\mathfrak{p}$ be a prime ideal of A. Then $S = A - \mathfrak{p}$ is multiplicatively closed (in fact $A - \mathfrak{p}$ is multiplicatively closed $\Leftrightarrow$ $\mathfrak{p}$ is prime). We write $A_{\mathfrak{p}}$ for $S^{-1}A$ in this case. The elements a/s with $a \in \mathfrak{p}$ form an ideal $\mathfrak{m}$ in $A_{\mathfrak{p}}$. If $b/t \notin \mathfrak{m}$, then $b \notin \mathfrak{p}$, hence $b \in S$ and therefore b/t is a unit in $A_{\mathfrak{p}}$. It follows that if $\mathfrak{a}$ is an ideal in $A_{\mathfrak{p}}$ and $\mathfrak{a} \nsubseteq \mathfrak{m}$, then $\mathfrak{a}$ contains a unit and is therefore the whole ring. Hence $\mathfrak{m}$ is the only maximal ideal in $A_{\mathfrak{p}}$; in other words, $A_{\mathfrak{p}}$ is a *local ring.*

The process of passing from A to $A_{\mathfrak{p}}$ is called *localization* at $\mathfrak{p}$.

2) $S^{-1}A$ is the zero ring $\Leftrightarrow 0 \in S$.

3) Let $f \in A$ and let $S = \{f^n\}_{n \geqslant 0}$. We write A_f for $S^{-1}A$ in this case.

4) Let $\mathfrak{a}$ be any ideal in A, and let $S = 1 + \mathfrak{a} =$ set of all $1 + x$ where $x \in \mathfrak{a}$. Clearly S is multiplicatively closed.

5) Special cases of 1) and 3):

i) $A = \mathbf{Z}$, $\mathfrak{p} = (p)$, p a prime number; $A_{\mathfrak{p}} =$ set of all rational numbers m/n where n is prime to p; if $f \in \mathbf{Z}$ and $f \neq 0$, then A_f is the set of all rational numbers whose denominator is a power of f.

ii) $A = k[t_1, \ldots, t_n]$, where k is a field and the t_i are independent indeterminates, $\mathfrak{p}$ a prime ideal in A. Then $A_{\mathfrak{p}}$ is the ring of all rational functions f/g, where $g \notin \mathfrak{p}$. If V is the variety defined by the ideal $\mathfrak{p}$, that is to say the set of all $x = (x_1, \ldots, x_n) \in k^n$ such that $f(x) = 0$ whenever $f \in \mathfrak{p}$, then (provided k is infinite) $A_{\mathfrak{p}}$ can be identified with the ring of all rational functions on k^n which are defined at almost all points of V; it is the local ring of k^n *along the variety V.* This is the prototype of the local rings which arise in algebraic geometry.

The construction of $S^{-1}A$ can be carried through with an A-module M in place of the ring A. Define a relation $\equiv$ on $M \times S$ as follows:

$$(m, s) \equiv (m', s') \Leftrightarrow \exists t \in S \text{ such that } t(sm' - s'm) = 0.$$

As before, this is an equivalence relation. Let m/s denote the equivalence class of the pair (m, s), let $S^{-1}M$ denote the set of such fractions, and make $S^{-1}M$ into an $S^{-1}A$-module with the obvious definitions of addition and scalar multiplication. As in Examples 1) and 3) above, we write $M_{\mathfrak{p}}$ instead of $S^{-1}M$ when $S = A - \mathfrak{p}$ ($\mathfrak{p}$ prime) and M_f when $S = \{f^n\}_{n > 0}$.

Let $u\colon M \to N$ be an A-module homomorphism. Then it gives rise to an $S^{-1}A$-module homomorphism $S^{-1}u\colon S^{-1}M \to S^{-1}N$, namely $S^{-1}u$ maps m/s to $u(m)/s$. We have $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$.

Proposition 3.3. *The operation S^{-1} is exact, i.e., if $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact at M, then $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ is exact at $S^{-1}M$.*

Proof. We have $g \circ f = 0$, hence $S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0$, hence $\mathrm{Im}\,(S^{-1}f) \subseteq \mathrm{Ker}\,(S^{-1}g)$. To prove the reverse inclusion, let $m/s \in \mathrm{Ker}\,(S^{-1}g)$, then $g(m)/s = 0$ in $S^{-1}M''$, hence there exists $t \in S$ such that $tg(m) = 0$ in M''. But $tg(m) = g(tm)$ since g is an A-module homomorphism, hence $tm \in \mathrm{Ker}\,(g) = \mathrm{Im}\,(f)$ and therefore $tm = f(m')$ for some $m' \in M'$. Hence in $S^{-1}M$ we have $m/s = f(m')/st = (S^{-1}f)(m'/st) \in \mathrm{Im}\,(S^{-1}f)$. Hence $\mathrm{Ker}\,(S^{-1}g) \subseteq \mathrm{Im}\,(S^{-1}f)$. ∎

In particular, it follows from (3.3) that if M' is a submodule of M, the mapping $S^{-1}M' \to S^{-1}M$ is *injective* and therefore $S^{-1}M'$ can be regarded as a submodule of $S^{-1}M$. With this convention,

Corollary 3.4. *Formation of fractions commutes with formation of finite sums, finite intersections and quotients. Precisely, if N, P are submodules of an A-module M, then*

i) $S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$

ii) $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$

iii) *the $S^{-1}A$-modules $S^{-1}(M/N)$ and $(S^{-1}M)/(S^{-1}N)$ are isomorphic.*

Proof. i) follows readily from the definitions and ii) is easy to verify: if $y/s = z/t$ ($y \in N, z \in P, s, t \in S$) then $u(ty - sz) = 0$ for some $u \in S$, hence $w = uty = usz \in N \cap P$ and therefore $y/s = w/stu \in S^{-1}(N \cap P)$. Consequently $S^{-1}N \cap S^{-1}P \subseteq S^{-1}(N \cap P)$, and the reverse inclusion is obvious.

iii) Apply S^{-1} to the exact sequence $0 \to N \to M \to M/N \to 0$. ∎

Proposition 3.5. *Let M be an A-module. Then the $S^{-1}A$ modules $S^{-1}M$ and $S^{-1}A \otimes_A M$ are isomorphic; more precisely, there exists a unique isomorphism $f: S^{-1}A \otimes_A M \to S^{-1}M$ for which*

$$f\big((a/s) \otimes m\big) = am/s \text{ for all } a \in A, m \in M, s \in S. \tag{1}$$

Proof. The mapping $S^{-1}A \times M \to S^{-1}M$ defined by

$$(a/s, m) \mapsto am/s$$

is A-bilinear, and therefore by the universal property (2.12) of the tensor product induces an A-homomorphism

$$f: S^{-1}A \otimes_A M \to S^{-1}M$$

satisfying (1). Clearly f is surjective, and is uniquely defined by (1).

Let $\sum_i (a_i/s_i) \otimes m_i$ be any element of $S^{-1}A \otimes M$. If $s = \prod_i s_i \in S$, $t_i = \prod_{j \neq i} s_j$, we have

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s} \otimes m = \sum_i \frac{1}{s} \otimes a_i t_i m = \frac{1}{s} \otimes \sum_i a_i t_i m,$$

so that every element of $S^{-1}A \otimes M$ is of the form $(1/s) \otimes m$. Suppose that $f((1/s) \otimes m) = 0$. Then $m/s = 0$, hence $tm = 0$ for some $t \in S$, and therefore

$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0.$$

Hence f is injective and therefore an isomorphism. ∎

Corollary 3.6. *$S^{-1}A$ is a flat A-module.*

Proof. (3.3), (3.5). ∎

Proposition 3.7. *If M, N are A-modules, there is a unique isomorphism of $S^{-1}A$-modules $f: S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ such that*

$$f((m/s) \otimes (n/t)) = (m \otimes n)/st.$$

In particular, if $\mathfrak{p}$ is any prime ideal, then

$$M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \cong (M \otimes_A N)_\mathfrak{p}$$

as $A_\mathfrak{p}$-modules.

Proof. Use (3.5) and the canonical isomorphisms of Chapter 2. ∎

LOCAL PROPERTIES

A property P of a ring A (or of an A-module M) is said to be a *local property* if the following is true:

A (or M) has $P \Leftrightarrow A_\mathfrak{p}$ (or $M_\mathfrak{p}$) has P, for each prime ideal $\mathfrak{p}$ of A. The following propositions give examples of local properties:

Proposition 3.8. *Let M be an A-module. Then the following are equivalent:*

i) $M = 0$;

ii) $M_\mathfrak{p} = 0$ *for all prime ideals* $\mathfrak{p}$ *of* A;

iii) $M_\mathfrak{m} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* A.

Proof. Clearly i) $\Rightarrow$ ii) $\Rightarrow$ iii). Suppose iii) satisfied and $M \neq 0$. Let x be a non-zero element of M, and let $\mathfrak{a} = \mathrm{Ann}(x)$; $\mathfrak{a}$ is an ideal $\neq (1)$, hence is contained in a maximal ideal $\mathfrak{m}$ by (1.4). Consider $x/1 \in M_\mathfrak{m}$. Since $M_\mathfrak{m} = 0$ we have $x/1 = 0$, hence x is killed by some element of $A - \mathfrak{m}$; but this is impossible since $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. ∎

Proposition 3.9. *Let $\phi: M \to N$ be an A-module homomorphism. Then the following are equivalent:*

i) ϕ *is injective;*

ii) $\phi_\mathfrak{p}: M_\mathfrak{p} \to N_\mathfrak{p}$ *is injective for each prime ideal* $\mathfrak{p}$;

iii) $\phi_\mathfrak{m}: M_\mathfrak{m} \to N_\mathfrak{m}$ *is injective for each maximal ideal* $\mathfrak{m}$.

Similarly with "injective" replaced by "surjective" throughout.

Proof. i) $\Rightarrow$ ii). $0 \to M \to N$ is exact, hence $0 \to M_\mathfrak{p} \to N_\mathfrak{p}$ is exact, i.e., $\phi_\mathfrak{p}$ is injective.

ii) $\Rightarrow$ iii) because a maximal ideal is prime.

iii) $\Rightarrow$ i). Let $M' = \operatorname{Ker}(\phi)$, then the sequence $0 \to M' \to M \to N$ is exact, hence $0 \to M'_\mathfrak{m} \to M_\mathfrak{m} \to N_\mathfrak{m}$ is exact by (3.3) and therefore $M'_\mathfrak{m} \cong \operatorname{Ker}(\phi_\mathfrak{m}) = 0$ since $\phi_\mathfrak{m}$ is injective. Hence $M' = 0$ by (3.8), hence ϕ is injective.

For the other part of the proposition, just reverse all the arrows. ∎

Flatness is a local property:

Proposition 3.10. *For any A-module M, the following statements are equivalent:*

i) *M is a flat A-module:*

ii) *$M_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module for each prime ideal $\mathfrak{p}$;*

iii) *$M_\mathfrak{m}$ is a flat $A_\mathfrak{m}$-module for each maximal ideal $\mathfrak{m}$.*

Proof. i) $\Rightarrow$ ii) by (3.5) and (2.20).

ii) $\Rightarrow$ iii) O.K.

iii) $\Rightarrow$ i). If $N \to P$ is a homomorphism of A-modules, and $\mathfrak{m}$ is any maximal ideal of A, then

$$\begin{aligned} N \to P \text{ injective } &\Rightarrow N_\mathfrak{m} \to P_\mathfrak{m} \text{ injective, by (3.9)} \\ &\Rightarrow N_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} \to P_\mathfrak{m} \otimes_{A_\mathfrak{m}} M_\mathfrak{m} \text{ injective, by (2.19)} \\ &\Rightarrow (N \otimes_A M)_\mathfrak{m} \to (P \otimes_A M)_\mathfrak{m} \text{ injective, by (3.7)} \\ &\Rightarrow N \otimes_A M \to P \otimes_A M \text{ injective, by (3.9).} \end{aligned}$$

Hence M is flat by (2.19). ∎

EXTENDED AND CONTRACTED IDEALS IN RINGS OF FRACTIONS

Let A be a ring, S a multiplicatively closed subset of A and $f\colon A \to S^{-1}A$ the natural homomorphism, defined by $f(a) = a/1$. Let C be the set of contracted ideals in A, and let E be the set of extended ideals in $S^{-1}A$ (cf. (1.17)). If $\mathfrak{a}$ is an ideal in A, its extension $\mathfrak{a}^e$ in $S^{-1}A$ is $S^{-1}\mathfrak{a}$ (for any $y \in \mathfrak{a}^e$ is of the form $\sum a_i/s_i$, where $a_i \in \mathfrak{a}$ and $s_i \in S$; bring this fraction to a common denominator).

Proposition 3.11. i) *Every ideal in $S^{-1}A$ is an extended ideal.*

ii) *If $\mathfrak{a}$ is an ideal in A, then $\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a}:s)$. Hence $\mathfrak{a}^e = (1)$ if and only if $\mathfrak{a}$ meets S.*

iii) *$\mathfrak{a} \in C \Leftrightarrow$ no element of S is a zero-divisor in $A/\mathfrak{a}$.*

iv) *The prime ideals of $S^{-1}A$ are in one-to-one correspondence ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) with the prime ideals of A which don't meet S.*

v) *The operation S^{-1} commutes with formation of finite sums, products, intersections and radicals.*

Proof. i) Let $\mathfrak{b}$ be an ideal in $S^{-1}A$, and let $x/s \in \mathfrak{b}$. Then $x/1 \in \mathfrak{b}$, hence $x \in \mathfrak{b}^c$ and therefore $x/s \in \mathfrak{b}^{ce}$. Since $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$ in any case (1.17), it follows that $\mathfrak{b} = \mathfrak{b}^{ce}$.

ii) $x \in \mathfrak{a}^{ec} = (S^{-1}\mathfrak{a})^c \Leftrightarrow x/1 = a/s$ for some $a \in \mathfrak{a}, s \in S \Leftrightarrow (xs - a)t = 0$ for some $t \in S \Leftrightarrow xst \in \mathfrak{a} \Leftrightarrow x \in \bigcup_{s \in S} (\mathfrak{a}:s)$.

iii) $\mathfrak{a} \in C \Leftrightarrow \mathfrak{a}^{ec} \subseteq \mathfrak{a} \Leftrightarrow (sx \in \mathfrak{a}$ for some $s \in S \Rightarrow x \in \mathfrak{a}) \Leftrightarrow$ no $s \in S$ is a zero-divisor in $A/\mathfrak{a}$.

iv) If $\mathfrak{q}$ is a prime ideal in $S^{-1}A$, then $\mathfrak{q}^c$ is a prime ideal in A (this much is true for any ring homomorphism). Conversely, if $\mathfrak{p}$ is a prime ideal in A, then $A/\mathfrak{p}$ is an integral domain; if $\bar{S}$ is the image of S in $A/\mathfrak{p}$, we have $S^{-1}A/S^{-1}\mathfrak{p} \cong \bar{S}^{-1}(A/\mathfrak{p})$ which is either 0 or else is contained in the field of fractions of $A/\mathfrak{p}$ and is therefore an integral domain, and therefore $S^{-1}\mathfrak{p}$ is either prime or is the unit ideal; by i) the latter possibility occurs if and only if $\mathfrak{p}$ meets S.

v) For sums and products, this follows from (1.18); for intersections, from (3.4). As to radicals, we have $S^{-1}r(\mathfrak{a}) \subseteq r(S^{-1}\mathfrak{a})$ from (1.18), and the proof of the reverse inclusion is a routine verification which we leave to the reader. ∎

Remarks. 1) If $\mathfrak{a}, \mathfrak{b}$ are ideals of A, the formula

$$S^{-1}(\mathfrak{a}:\mathfrak{b}) = (S^{-1}\mathfrak{a}:S^{-1}\mathfrak{b})$$

is true provided the ideal $\mathfrak{b}$ is finitely generated: see (3.15).

2) The proof in (1.8) that if $f \in A$ is not nilpotent there is a prime ideal of A which does not contain f can be expressed more concisely in the language of rings of fractions. Since the set $S = (f^n)_{n \geq 0}$ does not contain 0, the ring $S^{-1}A = A_f$ is not the zero ring and therefore by (1.3) has a maximal ideal, whose contraction in A is a prime ideal $\mathfrak{p}$ which does not meet S by (3.11); hence $f \notin \mathfrak{p}$.

Corollary 3.12. *If $\mathfrak{N}$ is the nilradical of A, the nilradical of $S^{-1}A$ is $S^{-1}\mathfrak{N}$.* ∎

Corollary 3.13. *If $\mathfrak{p}$ is a prime ideal of A, the prime ideals of the local ring $A_\mathfrak{p}$ are in one-to-one correspondence with the prime ideals of A contained in $\mathfrak{p}$.*

Proof. Take $S = A - \mathfrak{p}$ in (3.11) (iv). ∎

Remark. Thus the passage from A to $A_\mathfrak{p}$ cuts out all prime ideals except those contained in $\mathfrak{p}$. In the other direction, the passage from A to $A/\mathfrak{p}$ cuts out all prime ideals except those containing $\mathfrak{p}$. Hence if $\mathfrak{p}, \mathfrak{q}$ are prime ideals such that $\mathfrak{p} \supseteq \mathfrak{q}$, then by localizing with respect to $\mathfrak{p}$ and taking the quotient mod $\mathfrak{q}$ (in either order: these two operations commute, by (3.4)), we restrict our attention to those prime ideals which lie between $\mathfrak{p}$ and $\mathfrak{q}$. In particular, if $\mathfrak{p} = \mathfrak{q}$ we end up with a field, called the *residue field at* $\mathfrak{p}$, which can be obtained either as the field of fractions of the integral domain $A/\mathfrak{p}$ or as the residue field of the local ring $A_\mathfrak{p}$.

Proposition 3.14. *Let M be a finitely generated A-module, S a multiplicatively closed subset of A. Then $S^{-1}(\mathrm{Ann}\,(M)) = \mathrm{Ann}\,(S^{-1}M)$.*

Proof. If this is true for two A-modules, M, N, it is true for $M + N$:

$$\begin{aligned} S^{-1}(\mathrm{Ann}\,(M+N)) &= S^{-1}(\mathrm{Ann}\,(M) \cap \mathrm{Ann}\,(N)) \text{ by (2.2)} \\ &= S^{-1}(\mathrm{Ann}\,(M)) \cap S^{-1}(\mathrm{Ann}\,(N)) \text{ by (3.4)} \\ &= \mathrm{Ann}\,(S^{-1}M) \cap \mathrm{Ann}\,(S^{-1}N) \text{ by hypothesis} \\ &= \mathrm{Ann}\,(S^{-1}M + S^{-1}N) = \mathrm{Ann}\,(S^{-1}(M+N)). \end{aligned}$$

Hence it is enough to prove (3.14) for M generated by a single element: then $M \cong A/\mathfrak{a}$ (as A-module), where $\mathfrak{a} = \mathrm{Ann}\,(M)$; $S^{-1}M \cong (S^{-1}A)/(S^{-1}\mathfrak{a})$ by (3.4), so that $\mathrm{Ann}\,(S^{-1}M) = S^{-1}\mathfrak{a} = S^{-1}(\mathrm{Ann}\,(M))$. ∎

Corollary 3.15. *If N, P are submodules of an A-module M and if P is finitely generated, then $S^{-1}(N:P) = (S^{-1}N : S^{-1}P)$.*

Proof. $(N:P) = \mathrm{Ann}\,((N+P)/N)$ by (2.2); now apply (3.14). ∎

Proposition 3.16. *Let $A \to B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}$ is the contraction of a prime ideal of B if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. If $\mathfrak{p} = \mathfrak{q}^c$ then $\mathfrak{p}^{ec} = \mathfrak{p}$ by (1.17). Conversely, if $\mathfrak{p}^{ec} = \mathfrak{p}$, let S be the image of $A - \mathfrak{p}$ in B. Then $\mathfrak{p}^e$ does not meet S, therefore by (3.11) its extension in $S^{-1}B$ is a proper ideal and hence is contained in a maximal ideal $\mathfrak{m}$ of $S^{-1}B$. If $\mathfrak{q}$ is the contraction of $\mathfrak{m}$ in B, then $\mathfrak{q}$ is prime, $\mathfrak{q} \supseteq \mathfrak{p}^e$ and $\mathfrak{q} \cap S = \varnothing$. Hence $\mathfrak{q}^c = \mathfrak{p}$. ∎

EXERCISES

1. Let S be a multiplicatively closed subset of a ring A, and let M be a finitely generated A-module. Prove that $S^{-1}M = 0$ if and only if there exists $s \in S$ such that $sM = 0$.

2. Let $\mathfrak{a}$ be an ideal of a ring A, and let $S = 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ is contained in the Jacobson radical of $S^{-1}A$.

   Use this result and Nakayama's lemma to give a proof of (2.5) which does not depend on determinants. [If $M = \mathfrak{a}M$, then $S^{-1}M = (S^{-1}\mathfrak{a})(S^{-1}M)$, hence by Nakayama we have $S^{-1}M = 0$. Now use Exercise 1.]

3. Let A be a ring, let S and T be two multiplicatively closed subsets of A, and let U be the image of T in $S^{-1}A$. Show that the rings $(ST)^{-1}A$ and $U^{-1}(S^{-1}A)$ are isomorphic.

4. Let $f: A \to B$ be a homomorphism of rings and let S be a multiplicatively closed subset of A. Let $T = f(S)$. Show that $S^{-1}B$ and $T^{-1}B$ are isomorphic as $S^{-1}A$-modules.

5. Let A be a ring. Suppose that, for each prime ideal $\mathfrak{p}$, the local ring $A_\mathfrak{p}$ has no nilpotent element $\neq 0$. Show that A has no nilpotent element $\neq 0$. If each $A_\mathfrak{p}$ is an integral domain, is A necessarily an integral domain?

6. Let A be a ring $\neq 0$ and let Σ be the set of all multiplicatively closed subsets S of A such that $0 \notin S$. Show that Σ has maximal elements, and that $S \in \Sigma$ is maximal if and only if $A - S$ is a minimal prime ideal of A.

7. A multiplicatively closed subset S of a ring A is said to be *saturated* if

$$xy \in S \Leftrightarrow x \in S \text{ and } y \in S.$$

Prove that

i) S is saturated $\Leftrightarrow A - S$ is a union of prime ideals.

ii) If S is any multiplicatively closed subset of A, there is a unique smallest saturated multiplicatively closed subset $\bar{S}$ containing S, and that $\bar{S}$ is the complement in A of the union of the prime ideals which do not meet S. ($\bar{S}$ is called the *saturation* of S.)

If $S = 1 + \mathfrak{a}$, where $\mathfrak{a}$ is an ideal of A, find $\bar{S}$.

8. Let S, T be multiplicatively closed subsets of A, such that $S \subseteq T$. Let $\phi: S^{-1}A \to T^{-1}A$ be the homomorphism which maps each $a/s \in S^{-1}A$ to a/s considered as an element of $T^{-1}A$. Show that the following statements are equivalent:

i) ϕ is bijective.

ii) For each $t \in T$, $t/1$ is a unit in $S^{-1}A$.

iii) For each $t \in T$ there exists $x \in A$ such that $xt \in S$.

iv) T is contained in the saturation of S (Exercise 7).

v) Every prime ideal which meets T also meets S.

9. The set S_0 of all non-zero-divisors in A is a saturated multiplicatively closed subset of A. Hence the set D of zero-divisors in A is a union of prime ideals (see Chapter 1, Exercise 14). Show that every minimal prime ideal of A is contained in D. [Use Exercise 6.]

The ring $S_0^{-1}A$ is called the *total ring of fractions* of A. Prove that

i) S_0 is the largest multiplicatively closed subset of A for which the homomorphism $A \to S_0^{-1}A$ is injective.

ii) Every element in $S_0^{-1}A$ is either a zero-divisor or a unit.

iii) Every ring in which every non-unit is a zero-divisor is equal to its total ring of fractions (i.e., $A \to S_0^{-1}A$ is bijective).

10. Let A be a ring.

i) If A is absolutely flat (Chapter 2, Exercise 27) and S is any multiplicatively closed subset of A, then $S^{-1}A$ is absolutely flat.

ii) A is absolutely flat $\Leftrightarrow A_\mathfrak{m}$ is a field for each maximal ideal $\mathfrak{m}$.

11. Let A be a ring. Prove that the following are equivalent:

i) $A/\mathfrak{N}$ is absolutely flat ($\mathfrak{N}$ being the nilradical of A).

ii) Every prime ideal of A is maximal.

iii) Spec (A) is a T_1-space (i.e., every subset consisting of a single point is closed).
iv) Spec (A) is Hausdorff.

If these conditions are satisfied, show that Spec (A) is compact and totally disconnected (i.e. the only connected subsets of Spec (A) are those consisting of a single point).

12. Let A be an integral domain and M an A-module. An element $x \in M$ is a *torsion element* of M if Ann $(x) \neq 0$, that is if x is killed by some non-zero element of A. Show that the torsion elements of M form a submodule of M. This submodule is called the *torsion submodule* of M and is denoted by $T(M)$. If $T(M) = 0$, the module M is said to be torsion-free. Show that

i) If M is any A-module, then $M/T(M)$ is torsion-free.
ii) If $f: M \to N$ is a module homomorphism, then $f(T(M)) \subseteq T(N)$.
iii) If $0 \to M' \to M \to M''$ is an exact sequence, then the sequence $0 \to T(M') \to T(M) \to T(M'')$ is exact.
iv) If M is any A-module, then $T(M)$ is the kernel of the mapping $x \mapsto 1 \otimes x$ of M into $K \otimes_A M$, where K is the field of fractions of A.

[For iv), show that K may be regarded as the direct limit of its submodules $A\xi$ $(\xi \in K)$; using Chapter 1, Exercise 15 and Exercise 20, show that if $1 \otimes x = 0$ in $K \otimes M$ then $1 \otimes x = 0$ in $A\xi \otimes M$ for some $\xi \neq 0$. Deduce that $\xi^{-1}x = 0$.]

13. Let S be a multiplicatively closed subset of an integral domain A. In the notation of Exercise 12, show that $T(S^{-1}M) = S^{-1}(TM)$. Deduce that the following are equivalent:

i) M is torsion-free.
ii) $M_{\mathfrak{p}}$ is torsion-free for all prime ideals $\mathfrak{p}$.
iii) $M_{\mathfrak{m}}$ is torsion-free for all maximal ideals $\mathfrak{m}$.

14. Let M be an A-module and $\mathfrak{a}$ an ideal of A. Suppose that $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \supseteq \mathfrak{a}$. Prove that $M = \mathfrak{a}M$. [Pass to the $A/\mathfrak{a}$-module $M/\mathfrak{a}M$ and use (3.8).]

15. Let A be a ring, and let F be the A-module A^n. Show that every set of n generators of F is a basis of F. [Let $x_1, \ldots, x_n$ be a set of generators and $e_1, \ldots, e_n$ the canonical basis of F. Define $\phi: F \to F$ by $\phi(e_i) = x_i$. Then ϕ is surjective and we have to prove that it is an isomorphism. By (3.9) we may assume that A is a local ring. Let N be the kernel of ϕ and let $k = A/\mathfrak{m}$ be the residue field of A. Since F is a flat A-module, the exact sequence $0 \to N \to F \to F \to 0$ gives an exact sequence $0 \longrightarrow k \otimes N \longrightarrow k \otimes F \xrightarrow{1 \otimes \phi} k \otimes F \longrightarrow 0$. Now $k \otimes F = k^n$ is an n-dimensional vector space over k; $1 \otimes \phi$ is surjective, hence bijective, hence $k \otimes N = 0$.

Also N is finitely generated, by Chapter 2, Exercise 12, hence $N = 0$ by Nakayama's lemma. Hence ϕ is an isomorphism.]

Deduce that every set of generators of F has at least n elements.

16. Let B be a flat A-algebra. Then the following conditions are equivalent:

i) $\mathfrak{a}^{ec} = a$ for all ideals $\mathfrak{a}$ of A.
ii) Spec $(B) \to$ Spec (A) is surjective.
iii) For every maximal ideal $\mathfrak{m}$ of A we have $\mathfrak{m}^e \neq (1)$.

iv) If M is any non-zero A-module, then $M_B \neq 0$.
v) For every A-module M, the mapping $x \mapsto 1 \otimes x$ of M into M_B is injective.
[For i) $\Rightarrow$ ii), use (3.16). ii) $\Rightarrow$ iii) is clear.
iii) $\Rightarrow$ iv): Let x be a non-zero element of M and let $M' = Ax$. Since B is flat over A it is enough to show that $M'_B \neq 0$. We have $M' \cong A/\mathfrak{a}$ for some ideal $\mathfrak{a} \neq (1)$, hence $M'_B \cong B/\mathfrak{a}^e$. Now $\mathfrak{a} \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, hence $\mathfrak{a}^e \subseteq \mathfrak{m}^e \neq (1)$. Hence $M'_B \neq 0$.
iv) $\Rightarrow$ v): Let M' be the kernel of $M \to M_B$. Since B is flat over A, the sequence $0 \to M'_B \to M_B \to (M_B)_B$ is exact. But (Chapter 2, Exercise 13, with $N = M_B$) the mapping $M_B \to (M_B)_B$ is injective, hence $M'_B = 0$ and therefore $M' = 0$.
v) $\Rightarrow$ i): Take $M = A/\mathfrak{a}$.]
B is said to be *faithfully flat* over A.

17. Let $A \xrightarrow{f} B \xrightarrow{g} C$ be ring homomorphisms. If $g \circ f$ is flat and g is faithfully flat, then f is flat.

18. Let $f: A \to B$ be a flat homomorphism of rings, let $\mathfrak{q}$ be a prime ideal of B and let $\mathfrak{p} = \mathfrak{q}^c$. Then f^*: Spec $(B_\mathfrak{q}) \to$ Spec $(A_\mathfrak{p})$ is surjective. [For $B_\mathfrak{p}$ is flat over $A_\mathfrak{p}$ by (3.10), and $B_\mathfrak{q}$ is a local ring of $B_\mathfrak{p}$, hence is flat over $B_\mathfrak{p}$. Hence $B_\mathfrak{q}$ is flat over $A_\mathfrak{p}$ and satisfies condition (3) of Exercise 16.]

19. Let A be a ring, M an A-module. The *support* of M is defined to be the set Supp (M) of prime ideals $\mathfrak{p}$ of A such that $M_\mathfrak{p} \neq 0$. Prove the following results:
i) $M \neq 0 \Leftrightarrow$ Supp $(M) \neq \varnothing$.
ii) $V(\mathfrak{a}) =$ Supp $(A/\mathfrak{a})$.
iii) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then Supp $(M) =$ Supp $(M') \cup$ Supp (M'').
iv) If $M = \sum M_i$, then Supp $(M) = \bigcup$ Supp (M_i).
v) If M is finitely generated, then Supp $(M) = V(\mathrm{Ann}\,(M))$ (and is therefore a closed subset of Spec (A)).
vi) If M, N are finitely generated, then Supp $(M \otimes_A N) =$ Supp $(M) \cap$ Supp (N). [Use Chapter 2, Exercise 3.]
vii) If M is finitely generated and $\mathfrak{a}$ is an ideal of A, then Supp $(M/\mathfrak{a}M) = V(\mathfrak{a} + \mathrm{Ann}\,(M))$.
viii) If $f: A \to B$ is a ring homomorphism and M is a finitely generated A-module, then Supp $(B \otimes_A M) = f^{*-1}(\text{Supp}\,(M))$.

20. Let $f: A \to B$ be a ring homomorphism, f^*: Spec $(B) \to$ Spec (A) the associated mapping. Show that
i) Every prime ideal of A is a contracted ideal $\Leftrightarrow f^*$ is surjective.
ii) Every prime ideal of B is an extended ideal $\Rightarrow f^*$ is injective.
Is the converse of ii) true?

21. i) Let A be a ring, S a multiplicatively closed subset of A, and $\phi: A \to S^{-1}A$ the canonical homomorphism. Show that ϕ^*: Spec $(S^{-1}A) \to$ Spec (A) is a homeomorphism of Spec $(S^{-1}A)$ onto its image in $X =$ Spec (A). Let this image be denoted by $S^{-1}X$.
In particular, if $f \in A$, the image of Spec (A_f) in X is the basic open set X_f (Chapter 1, Exercise 17).

ii) Let $f\colon A \to B$ be a ring homomorphism. Let $X = \operatorname{Spec}(A)$ and $Y = \operatorname{Spec}(B)$, and let $f^*\colon Y \to X$ be the mapping associated with f. Identifying $\operatorname{Spec}(S^{-1}A)$ with its canonical image $S^{-1}X$ in X, and $\operatorname{Spec}(S^{-1}B)$ $(= \operatorname{Spec}(f(S)^{-1}B))$ with its canonical image $S^{-1}Y$ in Y, show that $S^{-1}f^*$: $\operatorname{Spec}(S^{-1}B) \to \operatorname{Spec}(S^{-1}A)$ is the restriction of f^* to $S^{-1}Y$, and that $S^{-1}Y = f^{*-1}(S^{-1}X)$.

iii) Let $\mathfrak{a}$ be an ideal of A and let $\mathfrak{b} = \mathfrak{a}^e$ be its extension in B. Let $\bar{f}\colon A/\mathfrak{a} \to B/\mathfrak{b}$ be the homomorphism induced by f. If $\operatorname{Spec}(A/\mathfrak{a})$ is identified with its canonical image $V(\mathfrak{a})$ in X, and $\operatorname{Spec}(B/\mathfrak{b})$ with its image $V(\mathfrak{b})$ in Y, show that $\bar{f}^*$ is the restriction of f^* to $V(\mathfrak{b})$.

iv) Let $\mathfrak{p}$ be a prime ideal of A. Take $S = A - \mathfrak{p}$ in ii) and then reduce mod $S^{-1}\mathfrak{p}$ as in iii). Deduce that the subspace $f^{*-1}(\mathfrak{p})$ of Y is naturally homeomorphic to $\operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = \operatorname{Spec}(k(\mathfrak{p}) \otimes_A B)$, where $k(\mathfrak{p})$ is the residue field of the local ring $A_\mathfrak{p}$.

Spec $(k(\mathfrak{p}) \otimes_A B)$ is called the *fiber* of f^* over $\mathfrak{p}$.

22. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Then the canonical image of $\operatorname{Spec}(A_\mathfrak{p})$ in $\operatorname{Spec}(A)$ is equal to the intersection of all the open neighborhoods of $\mathfrak{p}$ in $\operatorname{Spec}(A)$.

23. Let A be a ring, let $X = \operatorname{Spec}(A)$ and let U be a basic open set in X (i.e., $U = X_f$ for some $f \in A$: Chapter 1, Exercise 17).

i) If $U = X_f$, show that the ring $A(U) = A_f$ depends only on U and not on f.

ii) Let $U' = X_g$ be another basic open set such that $U' \subseteq U$. Show that there is an equation of the form $g^n = uf$ for some integer $n > 0$ and some $u \in A$, and use this to define a homomorphism $\rho\colon A(U) \to A(U')$ (i.e., $A_f \to A_g$) by mapping a/f^m to au^m/g^{mn}. Show that ρ depends only on U and U'. This homomorphism is called the *restriction* homomorphism.

iii) If $U = U'$, then ρ is the identity map.

iv) If $U \supseteq U' \supseteq U''$ are basic open sets in X, show that the diagram

$$\begin{tikzcd} A(U) \arrow[rr] \arrow[dr] & & A(U'') \\ & A(U') \arrow[ur] & \end{tikzcd}$$

(in which the arrows are restriction homomorphisms) is commutative.

v) Let x $(= \mathfrak{p})$ be a point of X. Show that

$$\varinjlim_{U \ni x} A(U) \cong A_\mathfrak{p}.$$

The assignment of the ring $A(U)$ to each basic open set U of X, and the restriction homomorphisms ρ, satisfying the conditions iii) and iv) above, constitutes a *presheaf of rings* on the basis of open sets $(X_f)_{f \in A}$. v) says that the stalk of this presheaf at $x \in X$ is the corresponding local ring $A_\mathfrak{p}$.

24. Show that the presheaf of Exercise 23 has the following property. Let $(U_i)_{i \in I}$ be a covering of X by basic open sets. For each $i \in I$ let $s_i \in A(U_i)$ be such that, for each pair of indices i, j, the images of s_i and s_j in $A(U_i \cap U_j)$ are equal. Then there exists a unique $s \in A$ $(= A(X))$ whose image in $A(U_i)$ is s_i, for all $i \in I$. (This essentially implies that the presheaf is a *sheaf*.)

25. Let $f: A \to B$, $g: A \to C$ be ring homomorphisms and let $h: A \to B \otimes_A C$ be defined by $h(x) = f(x) \otimes g(x)$. Let X, Y, Z, T be the prime spectra of $A, B, C, B \otimes_A C$ respectively. Then $h^*(T) = f^*Y \cap g^*(Z)$.
[Let $\mathfrak{p} \in X$, and let $k = k(\mathfrak{p})$ be the residue field at $\mathfrak{p}$. By Exercise 21, the fiber $h^{*-1}(\mathfrak{p})$ is the spectrum of $(B \otimes_A C) \otimes_A k \cong (B \otimes_A k) \otimes_k (C \otimes_A k)$. Hence $\mathfrak{p} \in h^*(T) \Leftrightarrow (B \otimes_A k) \otimes_k (C \otimes_A k) \neq 0 \Leftrightarrow B \otimes_A k \neq 0$ and $C \otimes_A k \neq 0 \Leftrightarrow \mathfrak{p} \in f^*(Y) \cap g^*(Z)$.]

26. Let $(B_\alpha, g_{\alpha\beta})$ be a direct system of rings and B the direct limit. For each α, let $f_\alpha: A \to B_\alpha$ be a ring homomorphism such that $g_{\alpha\beta} \circ f_\alpha = f_\beta$ whenever $\alpha \leqslant \beta$ (i.e. the B_α form a direct system of A-algebras). The f_α induce $f: A \to B$. Show that

$$f^*(\operatorname{Spec}(B)) = \bigcap_\alpha f_\alpha^*(\operatorname{Spec}(B_\alpha)).$$

[Let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $f^{*-1}(\mathfrak{p})$ is the spectrum of

$$B \otimes_A k(\mathfrak{p}) \cong \varinjlim (B_\alpha \otimes_A k(\mathfrak{p}))$$

(since tensor products commute with direct limits: Chapter 2, Exercise 20). By Exercise 21 of Chapter 2 it follows that $f^{*-1}(\mathfrak{p}) = \varnothing$ if and only if $B_\alpha \otimes_A k(\mathfrak{p}) = 0$ for some α, i.e., if and only if $f_\alpha^{*-1}(\mathfrak{p}) = \varnothing$.]

27. i) Let $f_\alpha: A \to B_\alpha$ be any family of A-algebras and let $f: A \to B$ be their tensor product over A (Chapter 2, Exercise 23). Then

$$f^*(\operatorname{Spec}(B)) = \bigcap_\alpha f_\alpha^*(\operatorname{Spec}(B_\alpha)).$$

[Use Examples 25 and 26.]

ii) Let $f_\alpha: A \to B_\alpha$ be any finite family of A-algebras and let $B = \prod_\alpha B_\alpha$. Define $f: A \to B$ by $f(x) = (f_\alpha(x))$. Then $f^*(\operatorname{Spec}(B)) = \bigcup_\alpha f_\alpha^*(\operatorname{Spec}(B_\alpha))$.

iii) Hence the subsets of $X = \operatorname{Spec}(A)$ of the form $f^*(\operatorname{Spec}(B))$, where $f: A \to B$ is a ring homomorphism, satisfy the axioms for closed sets in a topological space. The associated topology is the *constructible* topology on X. It is finer than the Zariski topology (i.e., there are more open sets, or equivalently more closed sets).

iv) Let X_C denote the set X endowed with the constructible topology. Show that X_C is quasi-compact.

28. (Continuation of Exercise 27.)

i) For each $g \in A$, the set X_g (Chapter 1, Exercise 17) is both open and closed in the constructible topology.

ii) Let C' denote the smallest topology on X for which the sets X_g are both open and closed, and let $X_{C'}$ denote the set X endowed with this topology. Show that $X_{C'}$ is Hausdorff.

iii) Deduce that the identity mapping $X_C \to X_{C'}$ is a homeomorphism. Hence a subset E of X is of the form $f^*(\operatorname{Spec}(B))$ for some $f: A \to B$ if and only if it is closed in the topology C'.

iv) The topological space X_C is compact, Hausdorff and totally disconnected.

29. Let $f: A \to B$ be a ring homomorphism. Show that $f^*: \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a continuous *closed* mapping (i.e., maps closed sets to closed sets) for the constructible topology.

30. Show that the Zariski topology and the constructible topology on $\operatorname{Spec}(A)$ are the same if and only if $A/\mathfrak{N}$ is absolutely flat (where $\mathfrak{N}$ is the nilradical of A). [Use Exercise 11.]

4

Primary Decomposition

The decomposition of an ideal into primary ideals is a traditional pillar of ideal theory. It provides the algebraic foundation for decomposing an algebraic variety into its irreducible components—although it is only fair to point out that the algebraic picture is more complicated than naïve geometry would suggest. From another point of view primary decomposition provides a generalization of the factorization of an integer as a product of prime-powers. In the modern treatment, with its emphasis on localization, primary decomposition is no longer such a central tool in the theory. It is still, however, of interest in itself and in this chapter we establish the classical uniqueness theorems.

The prototypes of commutative rings are $\mathbf{Z}$ and the ring of polynomials $k[x_1, \ldots, x_n]$ where k is a field; both these are unique factorization domains. This is not true of arbitrary commutative rings, even if they are integral domains (the classical example is the ring $\mathbf{Z}[\sqrt{-5}]$, in which the element 6 has two essentially distinct factorizations, $2 \cdot 3$ and $(1 + \sqrt{-5})(1 - \sqrt{-5})$). However, there is a generalized form of "unique factorization" of *ideals* (not of elements) in a wide class of rings (the Noetherian rings).

A prime ideal in a ring A is in some sense a generalization of a prime number. The corresponding generalization of a power of a prime number is a primary ideal. An ideal $\mathfrak{q}$ in a ring A is *primary* if $\mathfrak{q} \neq A$ and if

$$xy \in \mathfrak{q} \Rightarrow \text{either } x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n > 0.$$

In other words,

$$\mathfrak{q} \text{ is primary} \Leftrightarrow A/\mathfrak{q} \neq 0 \text{ and every zero-divisor in } A/\mathfrak{q} \text{ is nilpotent.}$$

Clearly every prime ideal is primary. Also the contraction of a primary ideal is primary, for if $f: A \to B$ and if $\mathfrak{q}$ is a primary ideal in B, then $A/\mathfrak{q}^c$ is isomorphic to a subring of $B/\mathfrak{q}$.

Proposition 4.1. *Let $\mathfrak{q}$ be a primary ideal in a ring A. Then $r(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.*

Proof. By (1.8) it is enough to show that $\mathfrak{p} = r(\mathfrak{q})$ is prime. Let $xy \in r(\mathfrak{q})$, then $(xy)^m \in \mathfrak{q}$ for some $m > 0$, and therefore either $x^m \in \mathfrak{q}$ or $y^{mn} \in \mathfrak{q}$ for some $n > 0$; i.e., either $x \in r(\mathfrak{q})$ or $y \in r(\mathfrak{q})$. ∎

If $\mathfrak{p} = r(\mathfrak{q})$, then $\mathfrak{q}$ is said to be *$\mathfrak{p}$-primary*.

Examples. 1) The primary ideals in $\mathbf{Z}$ are (0) and (p^n), where p is prime. For these are the only ideals in $\mathbf{Z}$ with prime radical, and it is immediately checked that they are primary.

2) Let $A = k[x, y]$, $\mathfrak{q} = (x, y^2)$. Then $A/\mathfrak{q} \cong k[y]/(y^2)$, in which the zero-divisors are all the multiples of y, hence are nilpotent. Hence $\mathfrak{q}$ is primary, and its radical $\mathfrak{p}$ is (x, y). We have $\mathfrak{p}^2 \subset \mathfrak{q} \subset \mathfrak{p}$ (strict inclusions), so that a primary ideal is not necessarily a prime-power.

3) Conversely, a prime power $\mathfrak{p}^n$ is not necessarily primary, although its radical is the prime ideal $\mathfrak{p}$. For example, let $A = k[x, y, z]/(xy - z^2)$ and let $\bar{x}, \bar{y}, \bar{z}$ denote the images of x, y, z respectively in A. Then $\mathfrak{p} = (\bar{x}, \bar{z})$ is prime (since $A/\mathfrak{p} \cong k[y]$, an integral domain); we have $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$ but $\bar{x} \notin \mathfrak{p}^2$ and $\bar{y} \notin r(\mathfrak{p}^2) = \mathfrak{p}$; hence $\mathfrak{p}^2$ is not primary. However, there is the following result:

Proposition 4.2. *If $r(\mathfrak{a})$ is maximal, then $\mathfrak{a}$ is primary. In particular, the powers of a maximal ideal $\mathfrak{m}$ are $\mathfrak{m}$-primary.*

Proof. Let $r(\mathfrak{a}) = \mathfrak{m}$. The image of $\mathfrak{m}$ in $A/\mathfrak{a}$ is the nilradical of $A/\mathfrak{a}$, hence $A/\mathfrak{a}$ has only one prime ideal, by (1.8). Hence every element of $A/\mathfrak{a}$ is either a unit or nilpotent, and so every zero-divisor in $A/\mathfrak{a}$ is nilpotent. ∎

We are going to study presentations of an ideal as an *intersection of primary ideals*. First, a couple of lemmas:

Lemma 4.3. *If $\mathfrak{q}_i$ $(1 \leqslant i \leqslant n)$ are $\mathfrak{p}$-primary, then $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary.*

Proof. $r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap r(\mathfrak{q}_i) = \mathfrak{p}$. Let $xy \in \mathfrak{q}$, $y \notin \mathfrak{q}$. Then for some i we have $xy \in \mathfrak{q}_i$ and $y \notin \mathfrak{q}_i$, hence $x \in \mathfrak{p}$, since $\mathfrak{q}_i$ is primary. ∎

Lemma 4.4. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, x an element of A. Then*

i) *if $x \in \mathfrak{q}$ then $(\mathfrak{q}:x) = (1)$;*

ii) *if $x \notin \mathfrak{q}$ then $(\mathfrak{q}:x)$ is $\mathfrak{p}$-primary, and therefore $r(\mathfrak{q}:x) = \mathfrak{p}$;*

iii) *if $x \notin \mathfrak{p}$ then $(\mathfrak{q}:x) = \mathfrak{q}$.*

Proof. i) and iii) follow immediately from the definitions.

ii): if $y \in (\mathfrak{q}:x)$ then $xy \in \mathfrak{q}$, hence (as $x \notin \mathfrak{q}$) we have $y \in \mathfrak{p}$. Hence $\mathfrak{q} \subseteq (\mathfrak{q}:x) \subseteq \mathfrak{p}$; taking radicals, we get $r(\mathfrak{q}:x) = \mathfrak{p}$. Let $yz \in (\mathfrak{q}:x)$ with $y \notin \mathfrak{p}$; then $xyz \in \mathfrak{q}$, hence $xz \in \mathfrak{q}$, hence $z \in (\mathfrak{q}:x)$. ∎

A *primary decomposition* of an ideal $\mathfrak{a}$ in A is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals, say

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i. \tag{1}$$

(In general such a primary decomposition need not exist; in this chapter we shall restrict our attention to ideals which have a primary decomposition.) If moreover (i) the $r(\mathfrak{q}_i)$ are all distinct, and (ii) we have $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ $(1 \leqslant i \leqslant n)$ the primary decomposition (1) is said to be *minimal* (or irredundant, or reduced, or normal, . . .). By (4.3) we can achieve (i) and then we can omit any superfluous terms to achieve (ii); thus any primary decomposition can be reduced to a minimal one. We shall say that $\mathfrak{a}$ is *decomposable* if it has a primary decomposition.

Theorem 4.5. (1st uniqueness theorem). *Let $\mathfrak{a}$ be a decomposable ideal and let $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$ $(1 \leqslant i \leqslant n)$. Then the $\mathfrak{p}_i$ are precisely the prime ideals which occur in the set of ideals $r(\mathfrak{a}:x)$ $(x \in A)$, and hence are independent of the particular decomposition of $\mathfrak{a}$.*

Proof. For any $x \in A$ we have $(\mathfrak{a}:x) = (\bigcap \mathfrak{q}_i : x) = \bigcap (\mathfrak{q}_i : x)$, hence $r(\mathfrak{a}:x) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i : x) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$ by (4.4). Suppose $r(\mathfrak{a}:x)$ is prime; then by (1.11) we have $r(\mathfrak{a}:x) = \mathfrak{p}_j$ for some j. Hence every prime ideal of the form $r(\mathfrak{a}:x)$ is one of the $\mathfrak{p}_j$. Conversely, for each i there exists $x_i \notin \mathfrak{q}_i$, $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j$, since the decomposition is minimal; and we have $r(\mathfrak{a}:x_i) = \mathfrak{p}_i$. ∎

Remarks. 1) The above proof, coupled with the last part of (4.4), shows that for each i there exists x_i in A such that $(\mathfrak{a}:x_i)$ is $\mathfrak{p}_i$-primary.

2) Considering $A/\mathfrak{a}$ as an A-module, (4.5) is equivalent to saying that the $\mathfrak{p}_i$ are precisely the prime ideals which occur as radicals of annihilators of elements of $A/\mathfrak{a}$.

Example. Let $\mathfrak{a} = (x^2, xy)$ in $A = k[x, y]$. Then $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$ where $\mathfrak{p}_1 = (x)$, $\mathfrak{p}_2 = (x, y)$. The ideal $\mathfrak{p}_2^2$ is primary by (4.2). So the prime ideals are $\mathfrak{p}_1, \mathfrak{p}_2$. In this example $\mathfrak{p}_1 \subset \mathfrak{p}_2$; we have $r(\mathfrak{a}) = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1$, but $\mathfrak{a}$ is not a primary ideal.

The prime ideals $\mathfrak{p}_i$ in (4.5) are said to *belong* to $\mathfrak{a}$, or to be *associated* with $\mathfrak{a}$. The ideal $\mathfrak{a}$ is primary if and only if it has only one associated prime ideal. The minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ are called the *minimal* or *isolated* prime ideals belonging to $\mathfrak{a}$. The others are called *embedded* prime ideals. In the example above, $\mathfrak{p}_2 = (x, y)$ is embedded.

Proposition 4.6. *Let $\mathfrak{a}$ be a decomposable ideal. Then any prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ contains a minimal prime ideal belonging to $\mathfrak{a}$, and thus the minimal prime ideals of $\mathfrak{a}$ are precisely the minimal elements in the set of all prime ideals containing $\mathfrak{a}$.*

Proof. If $\mathfrak{p} \supseteq \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$, then $\mathfrak{p} = r(\mathfrak{p}) \supseteq \bigcap r(\mathfrak{q}_i) = \bigcap \mathfrak{p}_i$. Hence by (1.11) we have $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i; hence $\mathfrak{p}$ contains a minimal prime ideal of $\mathfrak{a}$. ∎

Remarks. 1) The names *isolated* and *embedded* come from geometry. Thus if $A = k[x_1, \ldots, x_n]$ where k is a field, the ideal $\mathfrak{a}$ gives rise to a variety $X \subseteq k^n$ (see Chapter 1, Exercise 25). The minimal primes $\mathfrak{p}_i$ correspond to the irreducible components of X, and the embedded primes correspond to subvarieties of these, i.e., varieties *embedded* in the irreducible components. Thus in the example before (4.6) the variety defined by $\mathfrak{a}$ is the line $x = 0$, and the embedded ideal $\mathfrak{p}_2 = (x, y)$ corresponds to the origin $(0, 0)$.

2) It is *not* true that all the primary components are independent of the decomposition. For example $(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$ are two distinct minimal primary decompositions. However, there are some uniqueness properties: see (4.10).

Proposition 4.7. *Let $\mathfrak{a}$ be a decomposable ideal, let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition, and let $r(\mathfrak{q}_i) = \mathfrak{p}_i$. Then*

$$\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A : (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

In particular, if the zero ideal is decomposable, the set D of zero-divisors of A is the union of the prime ideals belonging to 0.

Proof. If $\mathfrak{a}$ is decomposable, then 0 is decomposable in $A/\mathfrak{a}$: namely $0 = \bigcap \bar{\mathfrak{q}}_i$ where $\bar{\mathfrak{q}}_i$ is the image of $\mathfrak{q}_i$ in $A/\mathfrak{a}$, and is primary. Hence it is enough to prove the last statement of (4.7). By (1.15) we have $D = \bigcup_{x \neq 0} r(0:x)$; from the proof of (4.5), we have $r(0:x) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \subseteq \mathfrak{p}_j$ for some j, hence $D \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. But also from (4.5) each $\mathfrak{p}_i$ is of the form $r(0:x)$ for some $x \in A$, hence $\bigcup \mathfrak{p}_i \subseteq D$. ∎

Thus (the zero ideal being decomposable)

$$\begin{aligned} D &= \text{set of zero-divisors} \\ &= \textstyle\bigcup \text{ of all prime ideals belonging to } 0; \\ \mathfrak{N} &= \text{set of nilpotent elements} \\ &= \textstyle\bigcap \text{ of all minimal primes belonging to } 0. \end{aligned}$$

Next we investigate the behavior of primary ideals under localization.

Proposition 4.8. *Let S be a multiplicatively closed subset of A, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.*

i) *If $S \cap \mathfrak{p} \neq \varnothing$, then $S^{-1}\mathfrak{q} = S^{-1}A$.*

ii) *If $S \cap \mathfrak{p} = \varnothing$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and its contraction in A is $\mathfrak{q}$.*

Hence primary ideals correspond to primary ideals in the correspondence (3.11) *between ideals in $S^{-1}A$ and contracted ideals in A.*

Proof. i) If $s \in S \cap \mathfrak{p}$, then $s^n \in S \cap \mathfrak{q}$ for some $n > 0$; hence $S^{-1}\mathfrak{q}$ contains $s^n/1$, which is a unit in $S^{-1}A$.

ii) If $S \cap \mathfrak{p} = \varnothing$, then $s \in S$ and $as \in \mathfrak{q}$ imply $a \in \mathfrak{q}$, hence $\mathfrak{q}^{ec} = \mathfrak{q}$ by (3.11). Also from (3.11) we have $r(\mathfrak{q}^e) = r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$. The verification that $S^{-1}\mathfrak{q}$ is primary is straightforward. Finally, the contraction of a primary ideal is primary. ∎

For any ideal $\mathfrak{a}$ and any multiplicatively closed subset S in A, the contraction in A of the ideal $S^{-1}\mathfrak{a}$ is denoted by $S(\mathfrak{a})$.

Proposition 4.9. *Let S be a multiplicatively closed subset of A and let $\mathfrak{a}$ be a decomposable ideal. Let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$ and suppose the $\mathfrak{q}_i$ numbered so that S meets $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$ but not $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Then*

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i, \qquad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

and these are minimal primary decompositions.

Proof. $S^{-1}\mathfrak{a} = \bigcap_{i=1}^n S^{-1}\mathfrak{q}_i$ by (3.11) $= \bigcap_{i=1}^m S^{-1}\mathfrak{q}_i$ by (4.8), and $S^{-1}\mathfrak{q}_i$ is $S^{-1}\mathfrak{p}_i$-primary for $i = 1, \ldots, m$. Since the $\mathfrak{p}_i$ are distinct, so are the $S^{-1}\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$, hence we have a minimal primary decomposition. Contracting both sides, we get

$$S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = \bigcap_{i=1}^{m} (S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

by (4.8) again. ∎

A set Σ of prime ideals belonging to $\mathfrak{a}$ is said to be *isolated* if it satisfies the following condition: if $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ and $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.

Let Σ be an isolated set of prime ideals belonging to $\mathfrak{a}$, and let $S = A - \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$. Then S is multiplicatively closed and, for any prime ideal $\mathfrak{p}'$ belonging to $\mathfrak{a}$, we have

$$\mathfrak{p}' \in \Sigma \Rightarrow \mathfrak{p}' \cap S = \varnothing;$$

$$\mathfrak{p}' \notin \Sigma \Rightarrow \mathfrak{p}' \nsubseteq \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \text{ (by (1.11))} \Rightarrow \mathfrak{p}' \cap S \neq \varnothing.$$

Hence, from (4.9), we deduce

Theorem 4.10. (2nd uniqueness theorem). *Let $\mathfrak{a}$ be a decomposable ideal, let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ be an isolated set of prime ideals of $\mathfrak{a}$. Then $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ is independent of the decomposition.*

In particular:

Corollary 4.11. *The isolated primary components (i.e., the primary components $\mathfrak{q}_i$ corresponding to minimal prime ideals $\mathfrak{p}_i$) are uniquely determined by $\mathfrak{a}$.*

Proof of (4.10). We have $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m} = S(\mathfrak{a})$ where $S = A - \mathfrak{p}_{i_1} \cup \cdots \cup \mathfrak{p}_{i_m}$, hence depends only on $\mathfrak{a}$ (since the $\mathfrak{p}_i$ depend only on $\mathfrak{a}$). ∎

Remark. On the other hand, the embedded primary components are in general not uniquely determined by $\mathfrak{a}$. If A is a Noetherian ring, there are in fact infinitely many choices for each embedded component (see Chapter 8, Exercise 1).

EXERCISES

1. If an ideal $\mathfrak{a}$ has a primary decomposition, then Spec $(A/\mathfrak{a})$ has only finitely many irreducible components.

2. If $\mathfrak{a} = r(\mathfrak{a})$, then $\mathfrak{a}$ has no embedded prime ideals.

3. If A is absolutely flat, every primary ideal is maximal.

4. In the polynomial ring $\mathbf{Z}[t]$, the ideal $\mathfrak{m} = (2, t)$ is maximal and the ideal $\mathfrak{q} = (4, t)$ is $\mathfrak{m}$-primary, but is not a power of $\mathfrak{m}$.

5. In the polynomial ring $K[x, y, z]$ where K is a field and x, y, z are independent indeterminates, let $\mathfrak{p}_1 = (x, y)$, $\mathfrak{p}_2 = (x, z)$, $\mathfrak{m} = (x, y, z)$; $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime, and $\mathfrak{m}$ is maximal. Let $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$. Show that $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a reduced primary decomposition of $\mathfrak{a}$. Which components are isolated and which are embedded?

6. Let X be an infinite compact Hausdorff space, $C(X)$ the ring of real-valued continuous functions on X (Chapter 1, Exercise 26). Is the zero ideal decomposable in this ring?

7. Let A be a ring and let $A[x]$ denote the ring of polynomials in one indeterminate over A. For each ideal $\mathfrak{a}$ of A, let $\mathfrak{a}[x]$ denote the set of all polynomials in $A[x]$ with coefficients in $\mathfrak{a}$.
   i) $\mathfrak{a}[x]$ is the extension of $\mathfrak{a}$ to $A[x]$.
   ii) If $\mathfrak{p}$ is a prime ideal in A, then $\mathfrak{p}[x]$ is a prime ideal in $A[x]$.
   iii) If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in A, then $\mathfrak{q}[x]$ is a $\mathfrak{p}[x]$-primary ideal in $A[x]$. [Use Chapter 1, Exercise 2.]
   iv) If $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ is a minimal primary decomposition in A, then $\mathfrak{a}[x] = \bigcap_{i=1}^n \mathfrak{q}_i[x]$ is a minimal primary decomposition in $A[x]$.
   v) If $\mathfrak{p}$ is a minimal prime ideal of $\mathfrak{a}$, then $\mathfrak{p}[x]$ is a minimal prime ideal of $\mathfrak{a}[x]$.

8. Let k be a field. Show that in the polynomial ring $k[x_1, \dots, x_n]$ the ideals $\mathfrak{p}_i = (x_1, \dots, x_i)$ $(1 \leqslant i \leqslant n)$ are prime and all their powers are primary. [Use Exercise 7.]

9. In a ring A, let $D(A)$ denote the set of prime ideals $\mathfrak{p}$ which satisfy the following condition: there exists $a \in A$ such that $\mathfrak{p}$ is minimal in the set of prime ideals containing $(0:a)$. Show that $x \in A$ is a zero divisor $\Leftrightarrow x \in \mathfrak{p}$ for some $\mathfrak{p} \in D(A)$.

   Let S be a multiplicatively closed subset of A, and identify Spec $(S^{-1}A)$ with its image in Spec (A) (Chapter 3, Exercise 21). Show that
   $$D(S^{-1}A) = D(A) \cap \operatorname{Spec}(S^{-1}A).$$
   If the zero ideal has a primary decomposition, show that $D(A)$ is the set of associated prime ideals of 0.

10. For any prime ideal $\mathfrak{p}$ in a ring A, let $S_\mathfrak{p}(0)$ denote the kernel of the homomorphism $A \to A_\mathfrak{p}$. Prove that
    i) $S_\mathfrak{p}(0) \subseteq \mathfrak{p}$.
    ii) $r(S_\mathfrak{p}(0)) = \mathfrak{p} \Leftrightarrow \mathfrak{p}$ is a minimal prime ideal of A.
    iii) If $\mathfrak{p} \supseteq \mathfrak{p}'$, then $S_\mathfrak{p}(0) \subseteq S_{\mathfrak{p}'}(0)$.
    iv) $\bigcap_{\mathfrak{p} \in D(A)} S_\mathfrak{p}(0) = 0$, where $D(A)$ is defined in Exercise 9.

11. If $\mathfrak{p}$ is a minimal prime ideal of a ring A, show that $S_{\mathfrak{p}}(0)$ (Exercise 10) is the smallest $\mathfrak{p}$-primary ideal.

Let $\mathfrak{a}$ be the intersection of the ideals $S_{\mathfrak{p}}(0)$ as $\mathfrak{p}$ runs through the minimal prime ideals of A. Show that $\mathfrak{a}$ is contained in the nilradical of A.

Suppose that the zero ideal is decomposable. Prove that $\mathfrak{a} = 0$ if and only if every prime ideal of 0 is isolated.

12. Let A be a ring, S a multiplicatively closed subset of A. For any ideal $\mathfrak{a}$, let $S(\mathfrak{a})$ denote the contraction of $S^{-1}\mathfrak{a}$ in A. The ideal $S(\mathfrak{a})$ is called the *saturation* of $\mathfrak{a}$ with respect to S. Prove that

i) $S(\mathfrak{a}) \cap S(\mathfrak{b}) = S(\mathfrak{a} \cap \mathfrak{b})$

ii) $S(r(\mathfrak{a})) = r(S(\mathfrak{a}))$

iii) $S(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a}$ meets S

iv) $S_1(S_2(\mathfrak{a})) = (S_1S_2)(\mathfrak{a})$.

If $\mathfrak{a}$ has a primary decomposition, prove that the set of ideals $S(\mathfrak{a})$ (where S runs through all multiplicatively closed subsets of A) is finite.

13. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. The *nth symbolic power of* $\mathfrak{p}$ is defined to be the ideal (in the notation of Exercise 12)

$$\mathfrak{p}^{(n)} = S_{\mathfrak{p}}(\mathfrak{p}^n)$$

where $S_{\mathfrak{p}} = A - \mathfrak{p}$. Show that

i) $\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary ideal;

ii) if $\mathfrak{p}^n$ has a primary decomposition, then $\mathfrak{p}^{(n)}$ is its $\mathfrak{p}$-primary component;

iii) if $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ has a primary decomposition, then $\mathfrak{p}^{(m+n)}$ is its $\mathfrak{p}$-primary component;

iv) $\mathfrak{p}^{(n)} = \mathfrak{p}^n \Leftrightarrow \mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

14. Let $\mathfrak{a}$ be a decomposable ideal in a ring A and let $\mathfrak{p}$ be a maximal element of the set of ideals $(\mathfrak{a}:x)$, where $x \in A$ and $x \notin \mathfrak{a}$. Show that $\mathfrak{p}$ is a prime ideal belonging to $\mathfrak{a}$.

15. Let $\mathfrak{a}$ be a decomposable ideal in a ring A, let Σ be an isolated set of prime ideals belonging to $\mathfrak{a}$, and let $\mathfrak{q}_\Sigma$ be the intersection of the corresponding primary components. Let f be an element of A such that, for each prime ideal $\mathfrak{p}$ belonging to $\mathfrak{a}$, we have $f \in \mathfrak{p} \Leftrightarrow \mathfrak{p} \notin \Sigma$, and let S_f be the set of all powers of f. Show that $\mathfrak{q}_\Sigma = S_f(\mathfrak{a}) = (\mathfrak{a}:f^n)$ for all large n.

16. If A is a ring in which every ideal has a primary decomposition, show that every ring of fractions $S^{-1}A$ has the same property.

17. Let A be a ring with the following property.

(L1) For every ideal $\mathfrak{a} \neq (1)$ in A and every prime ideal $\mathfrak{p}$, there exists $x \notin \mathfrak{p}$ such that $S_{\mathfrak{p}}(\mathfrak{a}) = (\mathfrak{a}:x)$, where $S_{\mathfrak{p}} = A - \mathfrak{p}$.

Then every ideal in A is an intersection of (possibly infinitely many) primary ideals.

[Let $\mathfrak{a}$ be an ideal $\neq (1)$ in A, and let $\mathfrak{p}_1$ be a minimal element of the set of prime ideals containing $\mathfrak{a}$. Then $\mathfrak{q}_1 = S_{\mathfrak{p}_1}(\mathfrak{a})$ is $\mathfrak{p}_1$-primary (by Exercise 11), and $\mathfrak{q}_1 = (\mathfrak{a}:x)$ for some $x \notin \mathfrak{p}_1$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap (\mathfrak{a} + (x))$.

Now let $\mathfrak{a}_1$ be a maximal element of the set of ideals $\mathfrak{b} \supseteq \mathfrak{a}$ such that $\mathfrak{q}_1 \cap \mathfrak{b} = \mathfrak{a}$, and choose $\mathfrak{a}_1$ so that $x \in \mathfrak{a}_1$, and therefore $\mathfrak{a}_1 \not\subseteq \mathfrak{p}_1$. Repeat the construction starting with $\mathfrak{a}_1$, and so on. At the nth stage we have $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{a}_n$ where the $\mathfrak{q}_i$ are primary ideals, $\mathfrak{a}_n$ is maximal among the ideals $\mathfrak{b}$ containing $\mathfrak{a}_{n-1} = \mathfrak{a}_n \cap \mathfrak{q}_n$ such that $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{b}$, and $\mathfrak{a}_n \nsubseteq \mathfrak{p}_n$. If at any stage we have $\mathfrak{a}_n = (1)$, the process stops, and $\mathfrak{a}$ is a finite intersection of primary ideals. If not, continue by transfinite induction, observing that each $\mathfrak{a}_n$ strictly contains $\mathfrak{a}_{n-1}$.]

18. Consider the following condition on a ring A:
(L2) Given an ideal $\mathfrak{a}$ and a descending chain $S_1 \supseteq S_2 \supseteq \cdots \supseteq S_n \supseteq \cdots$ of multiplicatively closed subsets of A, there exists an integer n such that $S_n(\mathfrak{a}) = S_{n+1}(\mathfrak{a}) = \cdots$. Prove that the following are equivalent:
i) Every ideal in A has a primary decomposition;
ii) A satisfies (L1) and (L2).
[For i) $\Rightarrow$ ii), use Exercises 12 and 15. For ii) $\Rightarrow$ i) show, with the notation of the proof of Exercise 17, that if $S_n = S_{\mathfrak{p}_1} \cap \cdots \cap S_{\mathfrak{p}_n}$ then S_n meets $\mathfrak{a}_n$, hence $S_n(\mathfrak{a}_n) = (1)$, and therefore $S_n(\mathfrak{a}) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. Now use (L2) to show that the construction must terminate after a finite number of steps.]

19. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Show that every $\mathfrak{p}$-primary ideal contains $S_{\mathfrak{p}}(0)$, the kernel of the canonical homomorphism $A \to A_{\mathfrak{p}}$.

Suppose that A satisfies the following condition: for every prime ideal $\mathfrak{p}$, the intersection of all $\mathfrak{p}$-primary ideals of A is equal to $S_{\mathfrak{p}}(0)$. (Noetherian rings satisfy this condition: see Chapter 10.) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct prime ideals, none of which is a minimal prime ideal of A. Then there exists an ideal $\mathfrak{a}$ in A whose associated prime ideals are $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.
[Proof by induction on n. The case $n = 1$ is trivial (take $\mathfrak{a} = \mathfrak{p}_1$). Suppose $n > 1$ and let $\mathfrak{p}_n$ be maximal in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By the inductive hypothesis there exists an ideal $\mathfrak{b}$ and a minimal primary decomposition $\mathfrak{b} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{n-1}$, where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. If $\mathfrak{b} \subseteq S_{\mathfrak{p}_n}(0)$, let $\mathfrak{p}$ be a minimal prime ideal of A contained in $\mathfrak{p}_n$. Then $S_{\mathfrak{p}_n}(0) \subseteq S_{\mathfrak{p}}(0)$, hence $\mathfrak{b} \subseteq S_{\mathfrak{p}}(0)$. Taking radicals and using Exercise 10, we have $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n-1} \subseteq \mathfrak{p}$, hence some $\mathfrak{p}_i \subseteq \mathfrak{p}$, hence $\mathfrak{p}_i = \mathfrak{p}$ since $\mathfrak{p}$ is minimal. This is a contradiction since no $\mathfrak{p}_i$ is minimal. Hence $\mathfrak{b} \nsubseteq S_{\mathfrak{p}_n}(0)$ and therefore there exists a $\mathfrak{p}_n$-primary ideal $\mathfrak{q}_n$ such that $\mathfrak{b} \nsubseteq \mathfrak{q}_n$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ has the required properties.]

Primary decomposition of modules

Practically the whole of this chapter can be transposed to the context of modules over a ring A. The following exercises indicate how this is done.

20. Let M be a fixed A-module, N a submodule of M. The *radical* of N in M is defined to be

$$r_M(N) = \{x \in A : x^q M \subseteq N \text{ for some } q > 0\}.$$

Show that $r_M(N) = r(N:M) = r(\mathrm{Ann}(M/N))$. In particular, $r_M(N)$ is an *ideal.*

State and prove the formulas for r_M analogous to (1.13).

21. An element $x \in A$ defines an endomorphism ϕ_x of M, namely $m \mapsto xm$. The element x is said to be a *zero-divisor* (resp. *nilpotent*) *in* M if ϕ_x is not injective (resp. is nilpotent). A submodule Q of M is *primary in M* if $Q \neq M$ and every zero-divisor in M/Q is nilpotent.

Show that if Q is primary in M, then $(Q:M)$ is a primary ideal and hence $r_M(Q)$ is a prime ideal $\mathfrak{p}$. We say that Q is $\mathfrak{p}$-*primary* (in M).

Prove the analogues of (4.3) and (4.4).

22. A *primary decomposition of N in M* is a representation of N as an intersection

$$N = Q_1 \cap \cdots \cap Q_n$$

of primary submodules of M; it is a *minimal primary decomposition* if the ideals $\mathfrak{p}_i = r_M(Q_i)$ are all distinct and if none of the components Q_i can be omitted from the intersection, that is if $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$ $(1 \leqslant i \leqslant n)$.

Prove the analogue of (4.5), that the prime ideals $\mathfrak{p}_i$ depend only on N (and M). They are called the *prime ideals belonging to N in M*. Show that they are also the prime ideals belonging to 0 in M/N.

23. State and prove the analogues of (4.6)–(4.11) inclusive. (There is no loss of generality in taking $N = 0$.)