A Term of
Commutative Algebra

By Allen ALTMAN
and Steven KLEIMAN

Contents

Preface

There is no shortage of books on Commutative Algebra, but the present book is different. Most books are monographs, with extensive coverage. There is one notable exception: Atiyah and Macdonald's 1969 classic [2]. It is a clear, concise, and efficient textbook, aimed at beginners, with a good selection of topics. So it has remained popular. However, its age and flaws do show. So there is need for an updated and improved version, which the present book aims to be.

Atiyah and Macdonald explain their philosophy in their introduction. They say their book "has the modest aim of providing a rapid introduction to the subject. It is designed to be read by students who have had a first elementary course in general algebra. On the other hand, it is not intended as a substitute for the more voluminous tracts on Commutative Algebra . . . The lecture-note origin of this book accounts for the rather terse style, with little general padding, and for the condensed account of many proofs." They "resisted the temptation to expand it in the hope that the brevity of [the] presentation will make clearer the mathematical structure of what is by now an elegant and attractive theory." They endeavor "to build up to the main theorems in a succession of simple steps and to omit routine verifications."

Their successful philosophy is wholeheartedly embraced below (it is a feature, not a flaw!), and also refined a bit. The present book also "grew out of a course of lectures." That course was based primarily on their book, but has been offered a number of times, and has evolved over the years, influenced by other publications and the reactions of the students. Their book comprises eleven chapters, split into forty-two sections. The present book comprises twenty-six sections; each represents a single lecture, and is self-contained.

Atiyah and Macdonald "provided . . . exercises at the end of each chapter." They "provided hints, and sometimes complete solutions, to the hard" exercises. Moreover, they developed a significant amount of the main content in the exercises. By contrast, in the present book, the exercises are integrated into the development, and complete solutions are given at the end of the book.

The exercises below are designed to provide a means for students to check, solidify, and expand their understanding of the material. The exercises are intentionally not difficult, tricky, or involved. Rarely do they introduce new techniques, although many statements are used afterwards. Students are encouraged to try to solve each exercise before looking up its solution. If they become stuck, then they should review the relevant material; if they remain stuck, then they should study the solution, making sure they can eventually solve the exercise on their own. However, students should read the given solution, even if they think they already know it, just to make sure; also, some exercises provide enlightening alternative solutions. Finally, instructors are encouraged to examine their students, possibly orally at a blackboard, on a small randomly chosen subset of exercises that have been assigned for the students to write up in their own words over the course of the term.

Atiyah and Macdonald explain that "a proper treatment of Homological Algebra is impossible within the confines of a small book; on the other hand, it is hardly sensible to ignore it completely." So they "use elementary homological methods —

exact sequence, diagrams, etc. — but . . . stop short of any results requiring a deep study of homology." Again, their philosophy is embraced and refined in the present book. Notably, below, elementary methods are used, not Tor's as they do, to prove the Ideal Criterion for flatness, and to relate flat modules and free modules over local rings. Also, projective modules are treated below, but not in their book.

In the present book, Category Theory is a basic tool; in Atiyah and Macdonald's, it seems like a foreign language. Thus they discuss the universal (mapping) property (UMP) of localization of a ring, but provide an ad hoc characterization. They also prove the UMP of tensor product of modules, but do not use the term this time. Below, the UMP is fundamental: there are many canonical constructions; each has a UMP, which serves to characterize the construction up to unique isomorphism owing to one general observation of Category Theory. For example, the Left Exactness of Hom is viewed simply as expressing in other words that the kernel and the cokernel of a map are characterized by their UMPs; by contrast, Atiyah and Macdonald prove the Left Exactness via a tedious elementary argument.

Atiyah and Macdonald prove the Adjoint-Associativity Formula. They note it says that Tensor Product is the left adjoint of Hom. From it and the Left Exactness of Hom, they deduce the Right Exactness of Tensor Product. They note that this derivation shows that any "left adjoint is right exact." More generally, as explained below, this derivation shows that any left adjoint preserves arbitrary direct limits, ones indexed by any small category. Atiyah and Macdonald consider only direct limits indexed by a directed set, and sketch an ad hoc argument showing that tensor product preserves direct limit. Also, arbitrary direct sums are direct limits indexed by a discrete category (it is not a directed set); hence, the general result yields that Tensor Product and other left adjoints preserve arbitrary Direct Sum.

Below, left adjoints are proved unique up to unique isomorphism. Therefore, the functor of localization of a module is canonically isomorphic to the functor of tensor product with the localized base ring, as both are left adjoints of the same functor, Restriction of Scalars from the localized ring to the base ring. There is an alternative argument. Since Localization is a left adjoint, it preserves Direct Sum and Cokernel; whence, it is isomorphic to that tensor-product functor by Watts Theorem, which characterizes all tensor-product functors as those linear functors that preserve Direct Sum and Cokernel. Atiyah and Macdonald's treatment is ad hoc. However, they do use the proof of Watts Theorem directly to show that, under the appropriate conditions, Completion of a module is Tensor Product with the completed base ring.

Below, Direct Limit is also considered as a functor, defined on the appropriate category of functors. As such, Direct Limit is a left adjoint. Hence, direct limits preserve other direct limits. Here the theory briefly reaches a higher level of abstraction. This discussion is completely elementary, but by far the most abstract part of the book. The extra abstraction can be difficult, especially for beginners.

Below, filtered direct limits are treated too. They are closer to the kind of limits treated by Atiyah and Macdonald. In particular, filtered direct limits preserve exactness and flatness. Further, they appear in the following lovely form of Lazard's Theorem: in a canonical way, every module is the direct limit of free modules of finite rank; moreover, the module is flat if and only if that direct limit is filtered.

Atiyah and Macdonald handle primary decomposition in a somewhat personal and dated fashion. First, they study primary decompositions of ideals in rings.

Then, in the exercises, they indicate how to translate the theory to modules. The decompositions need not exist, as the rings and modules need not be Noetherian. Associated primes play a secondary role: they are defined as the radicals of the primary components, and then characterized as the primes that are the radicals of annihilators of elements. Finally, they prove that, when the rings and modules are Noetherian, decompositions exist and the associated primes are annihilators. To prove existence, they study irreducible modules. Nowadays, associated primes are normally defined as prime annihilators, and studied on their own first; sometimes, as below, irreducible modules are not considered.

There are several other significant differences between Atiyah and Macdonald's treatment and the one below. First, the Noether Normalization Lemma is proved below in a stronger form for nested sequences of ideals; consequently, for algebras that are finitely generated over a field, dimension theory can be developed directly without treating Noetherian local rings first. Second, in a number of results below, the modules are assumed to be finitely presented, rather than finitely generated over a Noetherian ring. Third, there is a rudimentary treatment of regular sequences below and a proof of Serre's Criterion for Normality. Fourth, below, the Adjoint-Associativity Formula is proved over a pair of base rings; hence, it yields both a left and a right adjoint to the functor restriction of scalars.

The present book is a beta edition. Please do the community a service by sending the authors lists of comments, corrections, and typos. Thanks!

1. Rings and Ideals

We begin by reviewing basic notions and conventions to set the stage. Throughout this book, we emphasize universal mapping properties (UMPs); they are used to characterize notions and to make constructions. So, although polynomial rings and residue rings should already be familiar in other ways, we present their UMPs immediately, and use them extensively. We close this section with a brief treatment of idempotents and the Chinese Remainder Theorem.

(1.1) (*Rings*). — Recall that a **ring** R is an abelian group, written additively, with an associative multiplication that is distributive over the addition.

Throughout this book, every ring has a multiplicative identity, denoted by 1. Further, every ring is commutative (that is, $xy = yx$ in it), with an occasional exception, which is always marked (normally, it's a ring of matrices).

As usual, the additive identity is denoted by 0. Note that, for any x in R,

$$x \cdot 0 = 0;$$

indeed, $x \cdot 0 = x(0 + 0) = x \cdot 0 + x \cdot 0$, and $x \cdot 0$ can be canceled by adding $-(x \cdot 0)$.

We allow $1 = 0$. *If* $1 = 0$, *then* $R = 0$; indeed, $x = x \cdot 1 = x \cdot 0 = 0$ for any x.

A **unit** is an element u with a **reciprocal** $1/u$ such that $u \cdot 1/u = 1$. Alternatively, $1/u$ is denoted u^{-1} and is called the **multiplicative inverse** of u. The units form a multiplicative group, denoted $R^\times$.

For example, the ordinary integers form a ring $\mathbb{Z}$, and its units are 1 and -1.

A ring **homomorphism**, or simply a **ring map**, $\varphi\colon R \to R'$ is a map preserving sums, products, and 1. Clearly, $\varphi(R^\times) \subset R'^\times$. We call φ an **isomorphism** if it is bijective, and then we write $\varphi : R \xrightarrow{\sim} R'$. We call φ an **endomorphism** if $R' = R$. We call φ an **automorphism** if it is bijective and if $R' = R$.

If there is an unspecified isomorphism between rings R and R', then we write $R = R'$ when it is **canonical** (that is, it does not depend on any artificial choices), and we write $R \simeq R'$ otherwise.

A subset $R'' \subset R$ is a **subring** if the inclusion $R'' \hookrightarrow R$ is a ring map. For example, given a ring map $\varphi\colon R \to R'$, its image $\mathrm{Im}(\varphi) := \varphi(R)$ is a subring of R'.

An R**-algebra** is a ring R' that comes equipped with a ring map $\varphi\colon R \to R'$, called the **structure map**. An R**-algebra homomorphism**, or R**-algebra map**, $R' \to R''$ is a ring map between R-algebras compatible with their structure maps.

(1.2) (*Polynomial rings*). — Let R be a ring, $P := R[X_1, \dots, X_n]$ the polynomial ring in n variables (see [1, pp. 352–3] or [4, p. 268]). Recall that P has this **Universal Mapping Property** (UMP): *given a ring map* $\varphi\colon R \to R'$ *and given an element* x_i *of* R' *for each* i, *there is a unique ring map* $\pi\colon P \to R'$ *with* $\pi|R = \varphi$ *and* $\pi(X_i) = x_i$. In fact, since π is a ring map, necessarily π is given by the formula:

$$\pi\Big(\sum a_{(i_1,\dots,i_n)} X_1^{i_1} \cdots X_n^{i_n}\Big) = \sum \varphi(a_{(i_1,\dots,i_n)}) x_1^{i_1} \cdots x_n^{i_n}.$$

In other words, P is the **universal example** of an R-algebra equipped with a list of n elements: P is one example, and it maps uniquely to any other [1, (3.4), p. 353].

Similarly, let $P' := R[\{X_\lambda\}_{\lambda\in\Lambda}]$ be the polynomial ring in an arbitrary set of variables: its elements are the polynomials in any finitely many of the X_λ; sum and product are defined as in P. Thus P' contains as a subring the polynomial ring

in any finitely many X_λ, and P' is the union of these subrings. Clearly, P' has essentially the same UMP as P: *given* $\varphi\colon R \to R'$ *and given* $x_\lambda \in R'$ *for each* λ, *there is a unique* $\pi\colon P' \to R'$ *with* $\pi|R = \varphi$ *and* $\pi(X_\lambda) = x_\lambda$.

(1.3) (*Ideals*). — Let R be a ring. Recall that a subset $\mathfrak{a}$ is called an **ideal** if

(1) $0 \in \mathfrak{a}$ (or $\mathfrak{a}$ is nonempty),
(2) whenever $a, b \in \mathfrak{a}$, also $a + b \in \mathfrak{a}$, and
(3) whenever $x \in R$ and $a \in \mathfrak{a}$, also $xa \in \mathfrak{a}$.

Given elements $a_\lambda \in R$ for $\lambda \in \Lambda$, by the ideal $\langle a_\lambda \rangle_{\lambda\in\Lambda}$ they **generate**, we mean the smallest ideal containing them all. If $\Lambda = \emptyset$, then this ideal consists just of 0.

Any ideal containing all the a_λ contains any (finite) **linear combination** $\sum x_\lambda a_\lambda$ with $x_\lambda \in R$ and almost all 0. Form the set $\mathfrak{a}$ of all such linear combinations; clearly, $\mathfrak{a}$ is an ideal containing all a_λ. Thus $\mathfrak{a}$ is the ideal generated by the a_λ.

Given a single element a, we say that the ideal $\langle a \rangle$ is **principal**. By the preceding observation, $\langle a \rangle$ is equal to the set of all multiples xa with $x \in R$.

Similarly, given ideals $\mathfrak{a}_\lambda$ of R, by the ideal they generate, we mean the smallest ideal $\sum \mathfrak{a}_\lambda$ that contains them all. Clearly, $\sum \mathfrak{a}_\lambda$ is equal to the set of all finite linear combinations $\sum x_\lambda a_\lambda$ with $x_\lambda \in R$ and $a_\lambda \in \mathfrak{a}_\lambda$.

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, consider these three nested sets:

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &:= \{a + b \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\}, \\ \mathfrak{a} \cap \mathfrak{b} &:= \{a \mid a \in \mathfrak{a} \text{ and } a \in \mathfrak{b}\}, \\ \mathfrak{a}\mathfrak{b} &:= \{\textstyle\sum a_i b_i \mid a_i \in \mathfrak{a} \text{ and } b_i \in \mathfrak{b}\}. \end{aligned}$$

They are clearly ideals. They are known as the **sum**, **intersection**, and **product** of $\mathfrak{a}$ and $\mathfrak{b}$. Further, for any ideal $\mathfrak{c}$, the distributive law holds: $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.

Let $\mathfrak{a}$ be an ideal. Then $\mathfrak{a} = R$ *if and only if* $1 \in \mathfrak{a}$. Indeed, if $1 \in \mathfrak{a}$, then $x = x \cdot 1 \in \mathfrak{a}$ for every $x \in R$. It follows that $\mathfrak{a} = R$ *if and only if* $\mathfrak{a}$ *contains a unit.* Further, if $\langle x \rangle = R$, then x is a unit, since then there is an element y such that $xy = 1$. If $\mathfrak{a} \neq R$, then $\mathfrak{a}$ is said to be **proper**.

Let $\varphi\colon R \to R'$ be a ring map. Let $\mathfrak{a}R'$ denote the ideal of R' generated by $\varphi(\mathfrak{a})$; we call $\mathfrak{a}R'$ the **extension** of $\mathfrak{a}$. Let $\mathfrak{a}'$ be an ideal of R'. Clearly, the preimage $\varphi^{-1}(\mathfrak{a}')$ is an ideal of R; we call $\varphi^{-1}(\mathfrak{a}')$ the **contraction** of $\mathfrak{a}'$.

(1.4) (*Residue rings*). — Let $\varphi\colon R \to R'$ be a ring map. Recall its **kernel** $\operatorname{Ker}(\varphi)$ is defined to be the ideal $\varphi^{-1}(0)$ of R. Recall $\operatorname{Ker}(\varphi) = 0$ if and only if φ is injective.

Conversely, let $\mathfrak{a}$ be an ideal of R. Form the set of cosets of $\mathfrak{a}$:

$$R/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in R\}.$$

Recall that $R/\mathfrak{a}$ inherits a ring structure, and is called the **residue ring** (or **quotient ring** or **factor ring**) of R **modulo** $\mathfrak{a}$. Form the **quotient map**

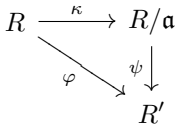
$$\kappa\colon R \to R/\mathfrak{a} \quad \text{by} \quad \kappa x := x + \mathfrak{a}.$$

The element $\kappa x \in R/\mathfrak{a}$ is called the **residue** of x. Clearly, κ is surjective, κ is a ring map, and κ has kernel $\mathfrak{a}$. Thus every ideal is a kernel!

Note that $\operatorname{Ker}(\varphi) \supset \mathfrak{a}$ if and only if $\varphi\mathfrak{a} = 0$.

Recall that, *if* $\operatorname{Ker}(\varphi) \supset \mathfrak{a}$, *then there is a ring map* $\psi\colon R/\mathfrak{a} \to R'$ *with* $\psi\kappa = \varphi$;

that is, the following diagram is **commutative**:



Conversely, *if ψ exists, then* $\operatorname{Ker}(\varphi) \supset \mathfrak{a}$, *or* $\varphi\mathfrak{a} = 0$, or $\mathfrak{a}R' = 0$, since $\kappa\mathfrak{a} = 0$.

Further, *if ψ exists, then ψ is unique* as κ is surjective.

Finally, as κ is surjective, *if ψ exists, then ψ is surjective if and only if φ is so.* In addition, then *ψ is injective if and only if* $\mathfrak{a} = \operatorname{Ker}(\varphi)$. Hence then *$\psi$ is an isomorphism if and only if φ is surjective and* $\mathfrak{a} = \operatorname{Ker}(\varphi)$. In particular, always

$$R/\operatorname{Ker}(\varphi) \xrightarrow{\sim} \operatorname{Im}(\varphi). \tag{1.4.1}$$

In practice, it is usually more convenient to view $R/\mathfrak{a}$ not as a set of cosets, but simply as another ring R' that comes equipped with a surjective ring map $\varphi\colon R \to R'$ whose kernel is the given ideal $\mathfrak{a}$.

Finally, $R/\mathfrak{a}$ has, as we saw, this UMP: $\kappa(\mathfrak{a}) = 0$ *and, given* $\varphi\colon R \to R'$ *such that* $\varphi(\mathfrak{a}) = 0$, *there is a unique ring map* $\psi\colon R/\mathfrak{a} \to R'$ *such that* $\psi\kappa = \varphi$. In other words, $R/\mathfrak{a}$ is the universal example of an R-algebra R' such that $\mathfrak{a}R' = 0$.

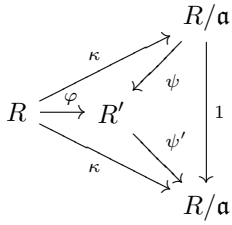
The UMP applies, first of all, to the underlying sets, providing a unique map ψ of sets. Now, φ and κ are ring maps, and $\psi\kappa = \varphi$; so

$$\psi\big(\kappa(a) + \kappa(b)\big) = \psi\kappa(a+b) = \psi\kappa(a) + \psi\kappa(b),$$
$$\psi\big(\kappa(a)\kappa(b)\big) = \psi\kappa(ab) = \psi\kappa(a) \cdot \psi\kappa(b), \quad \text{and} \quad \psi(1) = \psi\kappa(1) = 1.$$

But κ is surjective; so $\kappa(a), \kappa(b) \in R/\mathfrak{a}$ are arbitrary. Thus ψ is a ring map.

The UMP serves to determine $R/\mathfrak{a}$ up to unique isomorphism.

Indeed, say R', equipped with $\varphi\colon R \to R'$, has the UMP too. Then $\varphi(\mathfrak{a}) = 0$; so there is a unique $\psi\colon R/\mathfrak{a} \to R'$ with $\psi\kappa = \varphi$. And $\kappa(\mathfrak{a}) = 0$; so there is a unique $\psi'\colon R' \to R/\mathfrak{a}$ with $\psi'\varphi = \kappa$. Then, as shown, $(\psi'\psi)\kappa = \kappa$, but $1 \circ \kappa = \kappa$ where 1



is the identity map of $R/\mathfrak{a}$; hence, $\psi'\psi = 1$ by uniqueness. Similarly, $\psi\psi' = 1$ where 1 now stands for the identity map of R'. Thus ψ and ψ' are inverse isomorphisms.

The preceding proof is completely formal, and so works widely. There are many more constructions to come, and each one has an associated UMP, which therefore serves to determine the construction up to unique isomorphism.

Exercise **(1.5)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and $P := R[X_1, \dots, X_n]$ the polynomial ring. Construct an isomorphism ψ from $P/\mathfrak{a}P$ onto $(R/\mathfrak{a})[X_1, \dots, X_n]$.

Proposition **(1.6)**. — *Let R be a ring, $P := R[X]$ the polynomial ring in one variable, $a \in R$, and $\pi\colon P \to R$ the ring map defined by $\pi|R = 1_R$, the identity map, and $\pi(X) := a$. Then* $\operatorname{Ker}(\pi) = \langle X - a \rangle$, *and* $R[X]/\langle X - a\rangle \xrightarrow{\sim} R$.

PROOF: Given $F(X) \in P$, the Division Algorithm yields $F(X) = G(X)(X-a)+b$ with $G(X) \in P$ and $b \in R$. Then $\pi(F(X)) = b$. Hence $\mathrm{Ker}(\pi) = \langle X - a \rangle$. Finally, **(1.4.1)** yields $R[X]/\langle X - a \rangle \xrightarrow{\sim} R$. □

(1.7) (*Nested ideals*). — Let R be a ring, $\mathfrak{a}$ an ideal, and $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Given an ideal $\mathfrak{b} \supset \mathfrak{a}$, form the corresponding set of cosets of $\mathfrak{a}$:

$$\mathfrak{b}/\mathfrak{a} := \{b + \mathfrak{a} \mid b \in \mathfrak{b}\} = \kappa(\mathfrak{b}).$$

Clearly, $\mathfrak{b}/\mathfrak{a}$ is an ideal of $R/\mathfrak{a}$. Also $\mathfrak{b}/\mathfrak{a} = \mathfrak{b}(R/\mathfrak{a})$.

Clearly, *the operations* $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ *and* $\mathfrak{b}' \mapsto \kappa^{-1}(\mathfrak{b}')$ *are inverse to each other, and establish a bijective correspondence between the set of ideals* $\mathfrak{b}$ *of* R *containing* $\mathfrak{a}$ *and the set of all ideals* $\mathfrak{b}'$ *of* $R/\mathfrak{a}$. *Moreover, this correspondence preserves inclusions.*

Given an ideal $\mathfrak{b} \supset \mathfrak{a}$, form the composition of the quotient maps

$$\varphi\colon R \to R/\mathfrak{a} \to (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}).$$

Clearly, φ is surjective, and $\mathrm{Ker}(\varphi) = \mathfrak{b}$. Hence, owing to **(1.4)**, φ factors through the canonical isomorphism ψ in this commutative diagram:

$$\begin{array}{ccc} R & \longrightarrow & R/\mathfrak{b} \\ \big\downarrow & & \psi\big\downarrow\simeq \\ R/\mathfrak{a} & \to & (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \end{array}$$

EXERCISE **(1.8)**. — Let R be ring, and $P := R[X_1, \dots, X_n]$ the polynomial ring. Let $m \le n$ and $a_1, \dots, a_m \in R$. Set $\mathfrak{p} := \langle X_1 - a_1, \dots, X_m - a_m \rangle$. Prove that $P/\mathfrak{p} = R[X_{m+1}, \dots, X_n]$.

(1.9) (*Idempotents*). — Let R be a ring. Let $e \in R$ be an **idempotent**; that is, $e^2 = e$. Then Re is a ring with e as 1, because $(xe)e = xe$. But Re is not a subring of R unless $e = 1$, although Re is an ideal. Set $e' := 1 - e$. Then e' is idempotent, and $e \cdot e' = 0$. We call e and e' **complementary** and **orthogonal** idempotents

EXAMPLE **(1.10)**. — Let $R := R' \times R''$ be a **product** of two rings: its operations are performed componentwise. The additive identity is $(0, 0)$; the multiplicative identity is $(1, 1)$. Set $e := (1, 0)$ and $e' := (0, 1)$. Then e and e' are complementary idempotents. The next proposition shows this example is the only one possible.

PROPOSITION **(1.11)**. — *Let* R *be a ring with complementary idempotents* e *and* e'. *Set* $R' := Re$ *and* $R'' := Re'$, *and form the map* $\varphi\colon R \to R' \times R''$ *defined by* $\varphi(x) := (xe, xe')$. *Then* φ *is a ring isomorphism.*

PROOF: Define a map $\varphi'\colon R \to R'$ by $\varphi'(x) := xe$. Then φ' is a ring map since $xye = xye^2 = (xe)(ye)$. Hence φ is a ring map. Further, φ is surjective, since $(xe, x'e') = \varphi(xe + x'e')$. Also φ is injective, since if $xe = 0$ and $xe' = 0$, then $x = xe + xe' = 0$. Thus φ is an isomorphism. □

EXERCISE **(1.12)** (*Chinese Remainder Theorem*). — Let R be a ring.

(1) Let $\mathfrak{a}$ and $\mathfrak{b}$ be **comaximal** ideals; that is, $\mathfrak{a} + \mathfrak{b} = R$. Prove

$$(a)\ \ \mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} \quad \text{and} \quad (b)\ \ R/\mathfrak{a}\mathfrak{b} = (R/\mathfrak{a}) \times (R/\mathfrak{b}).$$

(2) Let $\mathfrak{a}$ be comaximal to both $\mathfrak{b}$ and $\mathfrak{b}'$. Prove $\mathfrak{a}$ is also comaximal to $\mathfrak{b}\mathfrak{b}'$.
(3) Let $\mathfrak{a}$, $\mathfrak{b}$ be comaximal, and $m, n \ge 1$. Prove $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are comaximal.

(4) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise comaximal. Prove
   (a) $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ are comaximal;
   (b) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$;
   (c) $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\sim} \prod(R/\mathfrak{a}_i)$.

EXERCISE **(1.13)**. — First, given a prime number p and a $k \geq 1$, find the idempotents in $\mathbb{Z}/\langle p^k \rangle$. Second, find the idempotents in $\mathbb{Z}/\langle 12 \rangle$. Third, find the number of idempotents in $\mathbb{Z}/\langle n \rangle$ where $n = \prod_{i=1}^{N} p_i^{n_i}$ with p_i distinct prime numbers.

EXERCISE **(1.14)**. — Let $R := R' \times R''$ be a **product** of rings, $\mathfrak{a} \subset R$ an ideal. Show $\mathfrak{a} = \mathfrak{a}' \times \mathfrak{a}''$ with $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ ideals. Show $R/\mathfrak{a} = (R'/\mathfrak{a}') \times (R''/\mathfrak{a}'')$.

2. Prime Ideals

Prime ideals are the key to the structure of commutative rings. So we review the basic theory. Specifically, we define prime ideals, and show their residue rings are domains. We show maximal ideals are prime, and discuss examples. Then we use Zorn's Lemma to prove the existence of maximal ideals in every nonzero ring.

DEFINITION **(2.1)**. — Let R be a ring. An element x is called a **zerodivisor** if there is a nonzero y with $xy = 0$; otherwise, x is called a **nonzerodivisor**. Denote the set of zerodivisors by $\mathrm{z.div}(R)$.

A subset S is called **multiplicative** if $1 \in S$ and if $x, y \in S$ implies $xy \in S$.

An ideal $\mathfrak{p}$ is called **prime** if its complement $R - \mathfrak{p}$ is multiplicative, or equivalently, if $1 \notin \mathfrak{p}$ and if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

EXERCISE **(2.2)**. — Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals, and $\mathfrak{p}$ a prime ideal. Prove that these conditions are equivalent: (1) $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$; and (2) $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p}$; and (3) $\mathfrak{ab} \subset \mathfrak{p}$.

(2.3) (*Fields, Domains*). — A ring is called a **field** if $1 \neq 0$ and if every nonzero element is a unit. Standard examples include the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.

A ring is called an **integral domain**, or simply a **domain**, if $\langle 0 \rangle$ is prime, or equivalently, if R is nonzero and has no nonzero zerodivisors.

Every domain R is a subring of its **fraction field** $\mathrm{Frac}(R)$, which consists of the fractions x/y with $x, y \in R$ and $y \neq 0$. Conversely, any subring R of a field K, including K itself, is a domain; indeed, any nonzero $x \in R$ cannot be a zerodivisor, because, if $xy = 0$, then $(1/x)(xy) = 0$, so $y = 0$. Further, $\mathrm{Frac}(R)$ has this UMP: the inclusion of R into any field L extends uniquely to an inclusion of $\mathrm{Frac}(R)$ into L. For example, the ring of integers $\mathbb{Z}$ is a domain, and $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Let R be a domain, and $R[X]$ the polynomial ring in one variable. Then $R[X]$ is a domain too; in fact, given any two nonzero polynomials f and g, not only is their product fg nonzero, but its leading coefficient is the product of the leading coefficients of f and g.

By induction, the polynomial ring in n variables $R[X_1, \ldots, X_n]$ is a domain, since

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n].$$

A similar argument proves $(R[X_1, \ldots, X_n])^\times = R^\times$. This equation can fail if R is not a domain. For example, if $a^2 = 0$, then $(1 + aX_1)(1 - aX_1) = 1$.

The fraction field $\mathrm{Frac}(R[X_1, \ldots, X_n])$ is called the field of **rational functions,** and is also denoted by $K(X_1, \ldots, X_n)$ where $K := \mathrm{Frac}(R)$.

EXERCISE **(2.4)**. — Given a prime number p and an integer $n \geq 2$, prove that the residue ring $\mathbb{Z}/\langle p^n \rangle$ does not contain a domain.

EXERCISE **(2.5)**. — Let $R := R' \times R''$ be a **product** of two rings. Show that R is a domain if and only if either R' or R'' is a domain and the other is 0.

(2.6) (*Unique factorization*). — Let R be a domain, p a nonzero nonunit. We call p **prime** if, whenever $p \mid xy$ (that is, there exists $z \in R$ such that $pz = xy$), either $p \mid x$ or $p \mid y$. Clearly, *p is prime if and only if the ideal $\langle p \rangle$ is prime.*

We call p **irreducible** if, whenever $p = yz$, either y or z is a unit. We call

R a **Unique Factorization Domain** (UFD) if every nonzero element can be written as a product of irreducible elements in a unique way up to order and units. In general, a prime element is irreducible, and in a UFD, irreducible elements are prime. Standard examples of UFDs include any field, the integers $\mathbb{Z}$, and a polynomial ring in n variables over a UFD; see [1, p. 398, p. 401], [4, Cor. 18.23, p. 297].

LEMMA **(2.7)**. — *Let $\varphi\colon R \to R'$ be a ring map, and $T \subset R'$ a subset. If T is multiplicative, then $\varphi^{-1}T$ is multiplicative; the converse holds if φ is surjective.*

PROOF: Both assertions are easy to check. □

PROPOSITION **(2.8)**. — *Let $\varphi\colon R \to R'$ be a ring map, and $\mathfrak{q} \subset R'$ an ideal. If $\mathfrak{q}$ is prime, then $\varphi^{-1}\mathfrak{q}$ is prime; the converse holds if φ is surjective.*

PROOF: By **(2.7)**, $R - \mathfrak{p}$ is multiplicative if and only if $R' - \mathfrak{q}$ is. So the assertion results from Definitions **(2.1)**. □

PROPOSITION **(2.9)**. — *Let R be a ring, $\mathfrak{p}$ an ideal. Then $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is a domain.*

PROOF: By **(2.8)**, $\mathfrak{p}$ is prime if and only if $\langle 0\rangle \subset R/\mathfrak{p}$ is. So the assertion results from the definition of domain in **(2.3)**. □

EXERCISE **(2.10)**. — Let R be a domain, and $R[X_1, \dots, X_n]$ the polynomial ring in n variables. Let $m \le n$, and set $\mathfrak{p} := \langle X_1, \dots, X_m\rangle$. Prove $\mathfrak{p}$ is a prime ideal.

EXERCISE **(2.11)**. — Let $R := R' \times R''$ be a **product** of rings. Show every prime ideal of R has the form $\mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime.

DEFINITION **(2.12)**. — Let R be a ring. An ideal $\mathfrak{m}$ is said to be **maximal** if $\mathfrak{m}$ is proper and if there is no proper ideal $\mathfrak{a}$ with $\mathfrak{m} \subsetneqq \mathfrak{a}$.

EXAMPLE **(2.13)**. — Let R be a domain. In the polynomial ring $R[X, Y]$ in two variables, $\langle X\rangle$ is prime by **(2.10)**. However, $\langle X\rangle$ is not maximal since $\langle X\rangle \subsetneqq \langle X, Y\rangle$.

PROPOSITION **(2.14)**. — *A ring R is a field if and only if $\langle 0\rangle$ is a maximal ideal.*

PROOF: Suppose R is a field. Let $\mathfrak{a}$ be a nonzero ideal, and a a nonzero element of $\mathfrak{a}$. Since R is a field, $a \in R^\times$. So **(1.3)** yields $\mathfrak{a} = R$.

Conversely, suppose $\langle 0\rangle$ is maximal. Take $x \neq 0$. Then $\langle x\rangle \neq \langle 0\rangle$. So $\langle x\rangle = R$. So x is a unit by **(1.3)**. Thus R is a field. □

EXERCISE **(2.15)**. — Let k be a field, R a nonzero ring, $\varphi\colon k \to R$ a ring map. Prove φ is injective.

PROPOSITION **(2.16)**. — *Let R be a ring, $\mathfrak{m}$ an ideal. Then $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

PROOF: Clearly, $\mathfrak{m}$ is maximal in R if and only if $\langle 0\rangle$ is maximal in $R/\mathfrak{m}$ by **(1.7)**. Hence the assertion results from **(2.14)**. □

EXAMPLE **(2.17)**. — Let k be a field, $a_1, \dots, a_n \in k$, and $P := k[X_1, \dots, X_n]$ the polynomial ring in n variables. Set $\mathfrak{m} := \langle X_1 - a_1, \dots, X_n - a_n\rangle$. Then $P/\mathfrak{m} = k$ by **(1.8)**; so $\mathfrak{m}$ is maximal by **(2.16)**.

EXERCISE **(2.18)**. — Prove the following statements or give a counterexample.

(1) The complement of a multiplicative set is a prime ideal.
(2) Given two prime ideals, their intersection is prime.
(3) Given two prime ideals, their sum is prime.
(4) Given a ring map $\varphi\colon R \to R'$, the operation φ^{-1} carries maximal ideals of R' to maximal ideals of R.
(5) In **(1.7)**, κ^{-1} takes maximal ideals of $R/\mathfrak{a}$ to maximal ideals of R.

COROLLARY **(2.19)**. — *In a ring, every maximal ideal is prime.*

PROOF: A field is a domain by **(2.3)**. So **(2.9)** and **(2.16)** yield the result. □

(2.20) (*PIDs*). — A domain R is called a **Principal Ideal Domain** (PID) if every ideal is principal. Examples include the polynomial ring $k[X]$ in one variable over a field k, and the ring $\mathbb{Z}$ of integers. Every PID is a UFD by [1, (2.12), p. 396], [4, Thm. 18.11, p. 291].

Let R be a PID, and $p \in R$ irreducible. Then $\langle p\rangle$ is maximal; indeed, if $\langle p\rangle \subsetneqq \langle x\rangle$, then $p = xy$ for some nonunit y, and so x must be a unit since p is irreducible. So **(2.16)** implies that $R/\langle p\rangle$ is a field.

EXERCISE **(2.21)**. — Prove that, in a PID, elements x and y are **relatively prime** (share no prime factor) if and only if the ideals $\langle x\rangle$ and $\langle y\rangle$ are comaximal.

EXAMPLE **(2.22)**. — Let R be a PID, and $p \in R$ a prime. Set $k := R/\langle p\rangle$. Let $P := R[X]$ be the polynomial ring in one variable. Take $g \in P$, let g' be its image in $k[X]$, and assume g' is irreducible. Set $\mathfrak{m} := \langle p, g\rangle$. Then $\mathfrak{m}$ is maximal by **(2.16)**; indeed, $P/\mathfrak{m} \xrightarrow{\sim} k[X]/\langle g'\rangle$ by **(1.4)**, and $k[X]/\langle g'\rangle$ is a field by **(2.20)**.

THEOREM **(2.23)**. — *Let R be a* PID. *Let $P := R[X]$ be the polynomial ring in one variable, and $\mathfrak{p}$ a prime ideal of P.*

(1) *Then $\mathfrak{p} = \langle 0\rangle$, or $\mathfrak{p} = \langle f\rangle$ with f prime, or $\mathfrak{p}$ is maximal.*

(2) *Assume $\mathfrak{p}$ is maximal. Then either $\mathfrak{p} = \langle f\rangle$ with f prime, or $\mathfrak{p} = \langle p, g\rangle$ with $p \in R$ prime and $g \in P$ with image $g' \in \big(R/\langle p\rangle\big)[X]$ prime.*

PROOF: Assume $\mathfrak{p} \neq \langle 0\rangle$. Take a nonzero $f_1 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\mathfrak{p}$ contains a prime factor f_1' of f_1. Replace f_1 by f_1'. Assume $\mathfrak{p} \neq \langle f_1\rangle$. Then there is an prime $f_2 \in \mathfrak{p} - \langle f_1\rangle$. Set $K := \operatorname{Frac}(R)$. Gauss's Lemma [1, p. 401], [4, Thm. 18.15, p. 295] implies that f_1 and f_2 are also prime in $K[X]$. So f_1 and f_2 are relatively prime in $K[X]$. So **(2.20)** and **(2.21)** yield $g_1, g_2 \in P$ and $c \in R$ with $(g_1/c)f_1 + (g_2/c)f_2 = 1$. So $c = g_1f_1 + g_2f_2 \in R \cap \mathfrak{p}$. Hence $R \cap \mathfrak{p} \neq 0$. But $R \cap \mathfrak{p}$ is prime, and R is a PID; so $R \cap \mathfrak{p} = \langle p\rangle$ where p is prime by **(2.6)**.

Set $k := R/\langle p\rangle$. Then k is a field by **(2.20)**. Set $\mathfrak{q} := \mathfrak{p}/\langle p\rangle \subset k[X]$. Then $k[X]/\mathfrak{q} = P/\mathfrak{p}$ by **(1.5)** and **(1.7)**. But $P/\mathfrak{p}$ is a domain as $\mathfrak{p}$ is prime. Hence $\mathfrak{q} = \langle g'\rangle$ where g' is prime in $k[X]$ by **(2.6)**. Then $\mathfrak{q}$ is maximal by **(2.20)**. So $\mathfrak{p}$ is maximal by **(1.6)**. Take $g \in \mathfrak{p}$ with image g'. Then $\mathfrak{p} = \langle p, g\rangle$ as $\mathfrak{p}/\langle p\rangle = \langle g'\rangle$. □

EXERCISE **(2.24)**. — Preserve the setup of **(2.23)**. Let $f := a_0X^n + \cdots + a_n$ be a polynomial of positive degree n. Assume that R has infinitely many prime elements p, or simply that there is a p such that $p \nmid a_0$. Show that $\langle f\rangle$ is not maximal.

THEOREM **(2.25)**. — *Every proper ideal $\mathfrak{a}$ is contained in some maximal ideal.*

PROOF: Set $\mathcal{S} := \{\text{ideals } \mathfrak{b} \mid \mathfrak{b} \supset \mathfrak{a} \text{ and } \mathfrak{b} \not\ni 1\}$. Then $\mathfrak{a} \in \mathcal{S}$, and $\mathcal{S}$ is partially ordered by inclusion. Given a totally ordered subset $\{\mathfrak{b}_\lambda\}$ of $\mathcal{S}$, set $\mathfrak{b} := \bigcup \mathfrak{b}_\lambda$. Then $\mathfrak{b}$ is clearly an ideal, and $1 \notin \mathfrak{b}$; so $\mathfrak{b}$ is an upper bound of $\{\mathfrak{b}_\lambda\}$ in $\mathcal{S}$. Hence by Zorn's Lemma [7, pp. 25, 26], [6, p. 880, p. 884], $\mathcal{S}$ has a maximal element, and it is the desired maximal ideal. □

COROLLARY **(2.26)**. — *Let R be a ring, $x \in R$. Then x is a unit if and only if x belongs to no maximal ideal.*

PROOF: By **(1.3)**, x is a unit if and only if $\langle x \rangle$ is not proper. So **(2.25)** yields the assertion. □

3. Radicals

Two radicals of a ring are commonly used in Commutative Algebra: the Jacobson radical, which is the intersection of all maximal ideals, and the nilradical, which is the set of all nilpotent elements. Closely related to the nilradical is the radical of a subset. We define these three radicals, and discuss examples. In particular, we study local rings; a local ring has only one maximal ideal, which is then its Jacobson radical. We prove two important general results: *Prime Avoidance*, which states that, if an ideal lies in a finite union of primes, then it lies in one of them, and the *Scheinnullstellensatz*, which states that the nilradical of an ideal is equal to the intersection of all the prime ideals containing it.

DEFINITION **(3.1)**. — Let R be a ring. Its (Jacobson) **radical** $\operatorname{rad}(R)$ is defined to be the intersection of all its maximal ideals.

PROPOSITION **(3.2)**. — *Let R be a ring, $x \in R$. Then $x \in \operatorname{rad}(R)$ if and only if $1 - xy$ is a unit for all $y \in R$.*

PROOF: Assume $x \in \operatorname{rad}(R)$. Let $\mathfrak{m}$ be a maximal ideal. Suppose $1 - xy \in \mathfrak{m}$. Since $x \in \mathfrak{m}$ too, also $1 \in \mathfrak{m}$, a contradiction. So $1 - xy$ is a unit by **(2.26)**.

Conversely, assume $x \notin \operatorname{rad}(R)$. Then there is a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$. So $\langle x \rangle + \mathfrak{m} = R$. Hence there exist $y \in R$ and $m \in \mathfrak{m}$ such that $xy + m = 1$. Then $1 - xy = m \in \mathfrak{m}$. So $1 - xy$ is not a unit by **(2.26)**, or directly by **(1.3)**. □

DEFINITION **(3.3)**. — A ring A is called **local** if it has exactly one maximal ideal, and **semilocal** if it has at least one and at most finitely many.

LEMMA **(3.4)** (Nonunit Criterion). — *Let A be a ring, $\mathfrak{n}$ the set of nonunits. Then A is local if and only if $\mathfrak{n}$ is an ideal; if so, then $\mathfrak{n}$ is the maximal ideal.*

PROOF: Every proper ideal $\mathfrak{a}$ lies in $\mathfrak{n}$ as $\mathfrak{a}$ contains no unit. So, if $\mathfrak{n}$ is an ideal, then it is a maximal ideal, and the only one. Thus A is local.

Conversely, assume A is local with maximal ideal $\mathfrak{m}$. Then $A - \mathfrak{n} = A - \mathfrak{m}$ by **(2.26)**. So $\mathfrak{n} = \mathfrak{m}$. Thus $\mathfrak{n}$ is an ideal. □

EXAMPLE **(3.5)**. — The product ring $R' \times R''$ is not local by **(3.4)** if both R' and R'' are nonzero. Indeed, $(1, 0)$ and $(0, 1)$ are nonunits, but their sum is a unit.

EXERCISE **(3.6)**. — Let A be a ring, $\mathfrak{m}$ a maximal ideal such that $1 + m$ is a unit for every $m \in \mathfrak{m}$. Prove A is local. Is this assertion still true if $\mathfrak{m}$ is not maximal?

EXAMPLE **(3.7)**. — Let R be a ring. A **formal power series** in the n variables $X_1, \dots, X_n$ is a formal infinite sum of the form $\sum a_{(i)} X_1^{i_1} \cdots X_n^{i_n}$ where $a_{(i)} \in R$ and where $(i) = (i_1, \dots, i_n)$ with each $i_j \geq 0$. Addition and multiplication are performed as for polynomials; with these operations, these series form a ring $R[[X_1, \dots, X_n]]$.

Set $P := R[[X_1, \dots, X_n]]$ and $\mathfrak{a} := \langle X_1, \dots, X_n \rangle$. Then $\sum a_{(i)} X_1^{i_1} \cdots X_n^{i_n} \mapsto a_{(0)}$ is a canonical surjective ring map $P \to R$ with kernel $\mathfrak{a}$; hence, $P/\mathfrak{a} = R$.

Given an ideal $\mathfrak{m} \subset R$, set $\mathfrak{n} := \mathfrak{a} + \mathfrak{m}P$. Then **(1.7)** yields $P/\mathfrak{n} = R/\mathfrak{m}$.

Suppose R is a local ring with maximal ideal $\mathfrak{m}$. Then any power series $f \notin \mathfrak{n}$ is of the form $f = a(1 - g)$ with $a \in R^\times$ and $g \in \mathfrak{a}$. Set $h := a^{-1}(1 + g + g^2 + \cdots)$; this sum makes sense as the component of degree d involves only the first $d + 1$

summands. Clearly $f \cdot h = 1$. Hence the nonunits constitute $\mathfrak{n}$. Thus P *is local with maximal ideal* $\mathfrak{n}$ *by* **(3.4)**.

EXAMPLE **(3.8)**. — Let k be a ring, and $A := k[[X]]$ the formal power series ring in one variable. A **Laurent series** is a formal sum of the form $\sum_{i=-m}^{\infty} a_i X^i$ with $a_i \in k$ and $m \in \mathbb{Z}$. The Laurent series form a ring $k\{\{X\}\}$. Set $K := k\{\{X\}\}$.

Set $f := \sum_{i=-m}^{\infty} a_i X^i$. If $a_{-m} \in k^\times$, then $f \in K^\times$; indeed, $f = a_{-m}X^{-m}(1-g)$ where $g \in A$, and $f \cdot a_{-m}^{-1}X^m(1+g+g^2+\cdots) = 1$.

Assume k is a field. If $f \neq 0$, then $f = X^{-m}u$ where $u \in A^\times$. Let $\mathfrak{a} \subset A$ be a nonzero ideal. Suppose $f \in \mathfrak{a}$. Then $X^{-m} \in \mathfrak{a}$. Let n be the smallest integer such that $X^n \in \mathfrak{a}$. Then $-m \geq n$. Set $b := X^{-m-n}u$. Then $b \in A$ and $f = bX^n$. Hence $\mathfrak{a} = \langle X^n \rangle$. Thus A *is a* PID.

Further, K is a field. In fact, $K = \mathrm{Frac}(A)$ as any nonzero $f \in K$ is of the form $f = u/X^m$ where u, $X^m \in A$.

Let $A[Y]$ be the polynomial ring in one variable, and $\iota\colon A \hookrightarrow K$ the inclusion. Define $\varphi\colon A[Y] \to K$ by $\varphi|A = \iota$ and $\varphi(Y) := X^{-1}$. Then φ is surjective. Set $\mathfrak{m} := \mathrm{Ker}(\varphi)$. Then $\mathfrak{m}$ is maximal by **(2.16)** and **(1.4)**. So by **(2.23)**, $\mathfrak{m}$ has the form $\langle f \rangle$ with f irreducible, or the form $\langle p, g \rangle$ with $p \in A$ irreducible and $g \in A[Y]$. But $\mathfrak{m} \cap A = 0$ as ι is injective. So $\mathfrak{m} = \langle f \rangle$. But $XY - 1$ belongs to $\mathfrak{m}$, and is clearly irreducible; hence, $XY - 1 = fu$ with u a unit. Thus $\langle XY - 1 \rangle$ is maximal.

In addition, $\langle X, Y \rangle$ is maximal. Indeed, $A[Y]/\langle Y \rangle = A$ by **(1.6)**, and so **(3.7)** yields $A[Y]/\langle X, Y \rangle = A/\langle X \rangle = k$. However, $\langle X, Y \rangle$ is not principal, as no nonunit of $A[Y]$ divides both X and Y. Thus $A[Y]$ *has both principal and nonprincipal maximal ideals, the two types allowed by* **(2.23)**.

PROPOSITION **(3.9)**. — *Let R be a ring, S a multiplicative set, and $\mathfrak{a}$ an ideal with $\mathfrak{a} \cap S = \emptyset$. Then there exists a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ with $\mathfrak{p} \cap S = \emptyset$.*

PROOF: Set $\mathcal{S} := \{\text{ideals } \mathfrak{b} \mid \mathfrak{b} \supset \mathfrak{a} \text{ and } \mathfrak{b} \cap S = \emptyset\}$. Then $\mathfrak{a} \in \mathcal{S}$, and $\mathcal{S}$ is partially ordered by inclusion. Given a totally ordered subset $\{\mathfrak{b}_\lambda\}$ of $\mathcal{S}$, set $\mathfrak{b} := \bigcup \mathfrak{b}_\lambda$. Then $\mathfrak{b}$ is an upper bound for $\{\mathfrak{b}_\lambda\}$ in $\mathcal{S}$. So by Zorn's Lemma, $\mathcal{S}$ has a maximal element $\mathfrak{p}$. Let's show $\mathfrak{p}$ is prime.

Take $x, y \in R - \mathfrak{p}$. Then $\mathfrak{p} + \langle x \rangle$ and $\mathfrak{p} + \langle y \rangle$ are strictly larger than $\mathfrak{p}$. So there are $p, q \in \mathfrak{p}$ and $a, b \in R$ with $p + ax \in S$ and $q + by \in S$. Since S is multiplicative, $pq + pby + qax + abxy \in S$. But $pq + pby + qax \in \mathfrak{p}$, so $xy \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is prime. □

EXERCISE **(3.10)**. — Let $\varphi\colon R \to R'$ be a ring map, $\mathfrak{p}$ an ideal of R. Prove

(1) there is an ideal $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ if and only if $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$;
(2) if $\mathfrak{p}$ is prime with $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$, then there's a prime $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

EXERCISE **(3.11)**. — Use Zorn's lemma to prove that any prime ideal $\mathfrak{p}$ contains a minimal prime ideal.

LEMMA **(3.12)** (Prime Avoidance). — *Let R be a ring, $\mathfrak{a}$ a subset of R that is stable under addition and multiplication, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideals such that $\mathfrak{p}_3, \ldots, \mathfrak{p}_n$ are prime. If $\mathfrak{a} \not\subset \mathfrak{p}_j$ for all j, then there is an $x \in \mathfrak{a}$ such that $x \notin \mathfrak{p}_j$ for all j; or equivalently, if $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$, then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.*

PROOF: Proceed by induction on n. If $n = 1$, the assertion is trivial. Assume that $n \geq 2$ and by induction that, for every i, there is an $x_i \in \mathfrak{a}$ such that $x_i \notin \mathfrak{p}_j$ for all $j \neq i$. We may assume $x_i \in \mathfrak{p}_i$ for every i, else we're done. If $n = 2$, then

clearly $x_1 + x_2 \notin \mathfrak{p}_j$ for $j = 1, 2$. If $n \geq 3$, then $(x_1 \cdots x_{n-1}) + x_n \notin \mathfrak{p}_j$ for all j as, if $j = n$, then $x_n \in \mathfrak{p}_n$ and $\mathfrak{p}_n$ is prime, and if $j < n$, then $x_n \notin \mathfrak{p}_j$ and $x_j \in \mathfrak{p}_j$. □

(3.13) (*Nilradical*). — Let R be a ring, $\mathfrak{a}$ a subset. Then the **radical** of $\mathfrak{a}$ is the set $\sqrt{\mathfrak{a}}$ defined by the formula $\sqrt{\mathfrak{a}} := \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n = n(x) \geq 1\}$.

Notice $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. Also, if $\mathfrak{a}$ is an intersection of prime ideals, then $\sqrt{\mathfrak{a}} = \mathfrak{a}$.

We call $\sqrt{\langle 0 \rangle}$ the **nilradical**, and sometimes denote it by $\mathrm{nil}(R)$. We call an element $x \in R$ **nilpotent** if x belongs to $\sqrt{\langle 0 \rangle}$, that is, if $x^n = 0$ for some $n \geq 1$.

We call R **reduced** if $\sqrt{\langle 0 \rangle} = \langle 0 \rangle$, that is, if R has no nonzero nilpotents.

Exercise **(3.14)**. — Find the nilpotents in $\mathbb{Z}/\langle n \rangle$. In particular, take $n = 12$.

Exercise **(3.15)**. — Let $\varphi\colon R \to R'$ be a ring map, $\mathfrak{b} \subset R'$ a subset. Prove

$$\varphi^{-1}\sqrt{\mathfrak{b}} = \sqrt{\varphi^{-1}\mathfrak{b}}.$$

Exercise **(3.16)**. — Let R be a ring, $\mathfrak{a} \subset \sqrt{\langle 0 \rangle}$ an ideal, and $P := R[Y]$ the polynomial ring in one variable. Let $u \in R$ be a unit, and $x \in R$ a nilpotent.

(1) Prove (a) that $u + x$ is a unit in R and (b) that $u + xY$ is a unit in P.
(2) Suppose $w \in R$ maps to a unit of $R/\mathfrak{a}$. Prove that w is a unit in R.

Theorem **(3.17)** (Scheinnullstellensatz). — *Let R be a ring, $\mathfrak{a}$ an ideal. Then*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$$

where $\mathfrak{p}$ runs through all the prime ideals containing $\mathfrak{a}$. (By convention, the empty intersection is equal to R.)

Proof: Take $x \notin \sqrt{\mathfrak{a}}$. Set $S := \{1, x, x^2, \ldots\}$. Then S is multiplicative, and $\mathfrak{a} \cap S = \emptyset$. By **(3.9)**, there is a $\mathfrak{p} \supset \mathfrak{a}$, but $x \notin \mathfrak{p}$. So $x \notin \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. Thus $\sqrt{\mathfrak{a}} \supset \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.

Conversely, take $x \in \sqrt{\mathfrak{a}}$. Say $x^n \in \mathfrak{a} \subset \mathfrak{p}$. Then $x \in \mathfrak{p}$. Thus $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. □

Proposition **(3.18)**. — *Let R be a ring, $\mathfrak{a}$ an ideal. Then $\sqrt{\mathfrak{a}}$ is an ideal.*

Proof: Take $x, y \in \sqrt{\mathfrak{a}}$; say $x^n \in \mathfrak{a}$ and $y^m \in \mathfrak{a}$. Then

$$(x + y)^{n+m-1} = \textstyle\sum_{i+j=m+n-1} \binom{n+m-1}{j} x^i y^j.$$

This sum belongs to $\mathfrak{a}$ as, in each summand, either x^i or y^j does, since, if $i \leq n-1$ and $j \leq m-1$, then $i + j \leq m + n - 2$. Thus $x + y \in \sqrt{\mathfrak{a}}$. So clearly $\sqrt{\mathfrak{a}}$ is an ideal.

Alternatively, given any collection of ideals $\mathfrak{a}_\lambda$, note that $\bigcap \mathfrak{a}_\lambda$ is also an ideal. So $\sqrt{\mathfrak{a}}$ is an ideal owing to **(3.17)**. □

Exercise **(3.19)**. — Let R be a ring, and $\mathfrak{a}$ an ideal. Assume $\sqrt{\mathfrak{a}}$ is finitely generated. Show there is an $n \geq 1$ such that $\left(\sqrt{\mathfrak{a}}\right)^n \subset \mathfrak{a}$.

Exercise **(3.20)**. — Let R be a ring, $\mathfrak{q}$ an ideal, $\mathfrak{p}$ a finitely generated prime. Prove that $\mathfrak{p} = \sqrt{\mathfrak{q}}$ if and only if there is $n \geq 1$ such that $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$.

Proposition **(3.21)**. — *Let R be a ring. Assume R is reduced with only one minimal prime $\mathfrak{q}$. Then R is a domain.*

Proof: Since R is reduced, $\langle 0 \rangle = \sqrt{\langle 0 \rangle}$ by **(3.13)**. Hence $\langle 0 \rangle$ is equal to the intersection of all the prime ideals $\mathfrak{p}$ by **(3.17)**. By **(3.11)**, every $\mathfrak{p}$ contains $\mathfrak{q}$. So $\langle 0 \rangle = \mathfrak{q}$. Thus R is a domain. □

EXERCISE **(3.22)**. — Let R be a ring. Assume R is reduced and has finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Prove $\varphi\colon R \to \prod(R/\mathfrak{p}_i)$ is injective, and for each i, there is some $(x_1, \ldots, x_n) \in \mathrm{Im}(\varphi)$ with $x_i \neq 0$ but $x_j = 0$ for $j \neq i$.

4. Modules

In Commutative Algebra, it has proven advantageous to expand the study of rings to include modules. Thus we obtain a richer theory, which is more flexible and more useful. We begin the expansion here by discussing residue modules, kernels, and images. In particular, we identify the universal property of the residue module, and use it to construct the Noether isomorphisms. We also construct free modules, direct sums, and direct products, and we describe their universal properties.

(4.1) (*Modules*). — Let R be a ring. Recall that an R**-module** M is an abelian group, written additively, with a **scalar multiplication**, $R \times M \to M$, written $(x, m) \mapsto xm$, that is

(1) **distributive**, $x(m + n) = xm + xn$ and $(x + y)m = xm + xn$,
(2) **associative**, $x(ym) = (xy)m$, and
(3) **unitary**, $1 \cdot m = m$.

For example, if R is a field, then an R-module is a vector space. Moreover, a $\mathbb{Z}$-module is just an abelian group; multiplication is repeated addition.

As in **(1.1)**, for any $x \in R$ and $m \in M$, we have $x \cdot 0 = 0$ and $0 \cdot m = 0$.

A **submodule** N of M is a subgroup that is **closed** under multiplication; that is, $xn \in N$ for all $x \in R$ and $n \in N$. For example, the ring R is itself an R-module, and the submodules are just the ideals. Given an ideal $\mathfrak{a}$, let $\mathfrak{a}N$ denote the smallest submodule containing all products an with $a \in \mathfrak{a}$ and $n \in N$. Similar to **(1.3)**, clearly $\mathfrak{a}N$ is equal to the set of finite sums $\sum a_i n_i$ with $a_i \in \mathfrak{a}$ and $n_i \in N$.

Given $m \in M$, we call the set of $x \in R$ with $xm = 0$ the **annihilator** of m, and denote it $\operatorname{Ann}(m)$. We call the set of $x \in R$ with $xm = 0$ for all $m \in M$ the **annihilator**of M, and denote it $\operatorname{Ann}(M)$. Clearly, $\operatorname{Ann}(m)$ and $\operatorname{Ann}(M)$ are ideals.

(4.2) (*Homomorphisms*). — Let R be a ring, M and N modules. Recall that a **homomorphism** is a map $\alpha\colon M \to N$ that is R**-linear**:

$$\alpha(xm + yn) = x(\alpha m) + y(\alpha n).$$

Associated to a homomorphism $\alpha\colon M \to N$ are its **kernel** and its **image**

$$\operatorname{Ker}(\alpha) := \alpha^{-1}(0) \subset M \quad \text{and} \quad \operatorname{Im}(\alpha) := \alpha(M) \subset N.$$

They are defined as subsets, but are obviously submodules.

A homomorphism α is called an **isomorphism** if it is bijective.

If so, then we write $\alpha\colon M \xrightarrow{\sim} N$. Then the set-theoretic inverse $\alpha^{-1}\colon N \to M$ is a homomorphism too. So *α is an isomorphism if and only if there is a set map $\beta\colon N \to M$ such that $\beta\alpha = 1_M$ and $\alpha\beta = 1_N$, and then $\beta = \alpha^{-1}$*. If there is an unspecified isomorphism between M and N, then we write $M = N$ when it is **canonical** (that is, it does not depend on any artificial choices), and we write $M \simeq N$ otherwise.

The set of homomorphisms α is denoted by $\operatorname{Hom}_R(M, N)$ or simply $\operatorname{Hom}(M, N)$. It is an R-module with addition and scalar multiplication defined by

$$(\alpha + \beta)m := \alpha m + \beta m \quad \text{and} \quad (x\alpha)m := x(\alpha m) = \alpha(xm).$$

Homomorphisms $\alpha\colon L \to M$ and $\beta\colon N \to P$ induce, via composition, a map

$$\mathrm{Hom}(\alpha, \beta)\colon \mathrm{Hom}(M, N) \to \mathrm{Hom}(L, P),$$

which is obviously a homomorphism. When α is the identity map 1_M, we write $\mathrm{Hom}(M, \beta)$ for $\mathrm{Hom}(1_M, \beta)$; similarly, we write $\mathrm{Hom}(\alpha, N)$ for $\mathrm{Hom}(\alpha, 1_N)$.

Exercise **(4.3)**. — Let R be a ring, M a module. Consider the set map

$$\theta\colon \mathrm{Hom}(R, M) \to M \quad \text{defined by} \quad \theta(\rho) := \rho(1).$$

Show that θ is an isomorphism, and describe its inverse.

(4.4) (*Endomorphisms*). — Let R be a ring, M a module. An **endomorphism** of M is a homomorphism $\alpha\colon M \to M$. The module of endomorphisms $\mathrm{Hom}(M, M)$ is also denoted $\mathrm{End}_R(M)$. It is a ring, usually noncommutative, with multiplication given by composition. Further, $\mathrm{End}_R(M)$ is a subring of $\mathrm{End}_{\mathbb{Z}}(M)$.

Given $x \in R$, let $\mu_x\colon M \to M$ denote the map of **multiplication** by x, defined by $\mu_x(m) := xm$. It is an endomorphism. Further, $x \mapsto \mu_x$ is a ring map

$$\mu_R\colon R \to \mathrm{End}_R(M) \subset \mathrm{End}_{\mathbb{Z}}(M).$$

(Thus we may view μ_R as representing R as a ring of operators on the abelian group M.) Note that $\mathrm{Ker}(\mu_R) = \mathrm{Ann}(M)$.

Conversely, given an abelian group N and a ring map

$$\nu\colon R \to \mathrm{End}_{\mathbb{Z}}(N),$$

we obtain a module structure on N by setting $xn := (\nu x)(n)$. Then $\mu_R = \nu$.

We call M **faithful** if $\mu_R\colon R \to \mathrm{End}_R(M)$ is injective, or $\mathrm{Ann}(M) = 0$. For example, R is a faithful R-module, as $x \cdot 1 = 0$ implies $x = 0$.

(4.5) (*Algebras*). — Fix two rings R and R'.

Suppose R' is an R-algebra with structure map φ. Let M' be an R'-module. Then M' is also an R-module by **restriction of scalars**: $xm := \varphi(x)m$. In other words, the R-module structure on M' corresponds to the composition

$$R \xrightarrow{\varphi} R' \xrightarrow{\mu_{R'}} \mathrm{End}_{\mathbb{Z}}(M').$$

In particular, R' it is an R-module; further, for all $x \in R$ and $y, z \in R'$,

$$(xy)z = x(yz).$$

Indeed, R' is an R'-module, so an R-module by restriction of scalars; further, $(xy)z = x(yz)$ since $(\varphi(x)y)z = \varphi(x)(yz)$ by associativity in R'.

Conversely, suppose R' is an R-module such that $(xy)z = x(yz)$. Then R' has an R-algebra structure that is compatible with the given R-module structure. Indeed, define $\varphi\colon R \to R'$ by $\varphi(x) := x \cdot 1$. Then $\varphi(x)z = xz$ as $(x \cdot 1)z = x(1 \cdot z)$. So the composition $\mu_{R'}\varphi\colon R \to R' \to \mathrm{End}_{\mathbb{Z}}(R')$ is equal to μ_R. Hence φ is a ring map, because μ_R is one and $\mu_{R'}$ is injective by **(4.4)**. Thus R' is an R-algebra, and restriction of scalars recovers its given R-module structure.

Suppose that $R' = R/\mathfrak{a}$ for some ideal $\mathfrak{a}$. Then an R-module M has a compatible R'-module structure if and only if $\mathfrak{a}M = 0$; if so, then the R'-structure is unique. Indeed, the ring map $\mu_R\colon R \to \mathrm{End}_{\mathbb{Z}}(M)$ factors through R' if and only if $\mu_R(\mathfrak{a}) = 0$ by **(1.4)**, so if and only if $\mathfrak{a}M = 0$; as $\mathrm{End}_{\mathbb{Z}}(M)$ may be noncommutative, we must apply **(1.4)** to $\mu_R(R)$, which is commutative.

Again suppose R' is an arbitrary R-algebra with structure map φ. A **subalgebra** R'' of R' is a subring such that φ maps into R''. The subalgebra **generated** by

$x_1, \dots, x_n \in R'$ is the smallest R-subalgebra that contains them. We denote it by $R[x_1, \dots, x_n]$. It clearly contains all polynomial combinations $f(x_1, \dots, x_n)$ with coefficients in R. In fact, the set R'' of these polynomial combinations is itself clearly an R-subalgebra; hence, $R'' = R[x_1, \dots, x_n]$.

We say R' is a **finitely generated R-algebra** or is **algebra finite over** R if there exist $x_1, \dots, x_n \in R'$ such that $R' = R[x_1, \dots, x_n]$.

(4.6) (*Residue modules*). — Let R be a ring, M a module, $M' \subset M$ a submodule. Form the set of cosets

$$M/M' := \{m + M' \mid m \in M\}.$$

Recall that M/M' inherits a module structure, and is called the **residue module** or **quotient of M modulo M'**. Form the **quotient map**

$$\kappa\colon M \to M/M' \quad \text{by} \quad \kappa(m) := m + M'.$$

Clearly κ is surjective, κ is linear, and κ has kernel M'.

Let $\alpha\colon M \to N$ be linear. Note that $\operatorname{Ker}(\alpha) \supset M'$ *if and only if* $\alpha(M') = 0$.

Recall that, *if* $\operatorname{Ker}(\alpha) \supset M'$*, then there exists a homomorphism* $\beta\colon M/M' \to N$ such that $\beta\kappa = \alpha$; that is, the following diagram is commutative:

$$\begin{array}{ccc} M & \xrightarrow{\kappa} & M/M' \\ & \searrow^{\alpha} & \downarrow{\scriptstyle \beta} \\ & & N \end{array}$$

Conversely, *if* β *exists, then* $\operatorname{Ker}(\alpha) \supset M'$*, or* $\alpha(M') = 0$*, as* $\kappa(M') = 0$.

Further, *if* β *exists, then* β *is unique* as κ is surjective.

Finally, since κ is surjective, *if* β *exists, then* β *is surjective if and only if* α *is so. In addition, then* β *is injective if and only if* $M' = \operatorname{Ker}(\alpha)$*. Hence* β *is an isomorphism if and only if* α *is surjective and* $M' = \operatorname{Ker}(\alpha)$*. In particular, always*

$$M/\operatorname{Ker}(\alpha) \xrightarrow{\sim} \operatorname{Im}(\alpha). \tag{4.6.1}$$

In practice, it is usually more convenient to view M/M' not as a set of cosets, but simply another module M'' that comes equipped with a surjective homomorphism $\alpha\colon M \to M''$ whose kernel is the given submodule M'.

Finally, as we have seen, M/M' has the following UMP: $\kappa(M') = 0$, *and given* $\alpha\colon M \to N$ *such that* $\alpha(M') = 0$*, there is a unique homomorphism* $\beta\colon M/M' \to N$ *such that* $\beta\kappa = \alpha$. Formally, the UMP determines M/M' up to unique isomorphism.

(4.7) (*Cyclic modules*). — Let R be a ring. A module M is said to be **cyclic** if there exists $m \in M$ such that $M = Rm$. If so, form $\alpha\colon R \to M$ by $x \mapsto xm$; then α induces an isomorphism $R/\operatorname{Ann}(m) \xrightarrow{\sim} M$ as $\operatorname{Ker}(\alpha) = \operatorname{Ann}(m)$; see **(4.6.1)**. Note that $\operatorname{Ann}(m) = \operatorname{Ann}(M)$. Conversely, given any ideal $\mathfrak{a}$, the R-module $R/\mathfrak{a}$ is cyclic, generated by the coset of 1, and $\operatorname{Ann}(R/\mathfrak{a}) = \mathfrak{a}$.

(4.8) (*Noether Isomorphisms*). — Let R be a ring, N a module, and L and M submodules.

First, assume $L \subset M \subset N$. Form the following composition of quotient maps:

$$\alpha\colon N \to N/L \to (N/L)/(M/L).$$

Clearly α is surjective, and $\operatorname{Ker}(\alpha) = M$. Hence owing to **(4.6)**, α *factors through*

the isomorphism β in this commutative diagram:

$$\begin{array}{ccc} N & \longrightarrow & N/M \\ \big\downarrow & & \beta\big\downarrow\simeq \\ N/L & \to & (N/L)/(M/L) \end{array} \tag{4.8.1}$$

Second, let $L + M$ denote the set of all sums $\ell + m$ with $\ell \in L$ and $m \in M$. Clearly $L + M$ is a submodule of N. It is called the **sum** of L and M.

Form the composition α' of the inclusion map $L \to L+M$ and the quotient map $L+M \to (L+M)/M$. Clearly α' is surjective and $\operatorname{Ker}(\alpha') = L \cap M$. Hence owing to **(4.6)**, α' *factors through the isomorphism* β' in this commutative diagram:

$$\begin{array}{ccc} L & \longrightarrow & L/(L\cap M) \\ \big\downarrow & & \beta'\big\downarrow\simeq \\ L+M & \to & (L+M)/M \end{array} \tag{4.8.2}$$

The isomorphisms of **(4.6.1)** and **(4.8.1)** and **(4.8.2)** are called **Noether's First, Second, and Third Isomorphisms.**

(4.9) (*Cokernels, coimages*). — Let R be a ring, $\alpha\colon M \to N$ a linear map. Associated to α are its **cokernel** and its **coimage**,

$$\operatorname{Coker}(\alpha) := N/\operatorname{Im}(\alpha) \quad \text{and} \quad \operatorname{Coim}(\alpha) := M/\operatorname{Ker}(\alpha);$$

they are quotient modules, and their quotient maps are both denoted by κ.

Note **(4.6)** yields the UMP of the cokernel: $\kappa\alpha = 0$, *and given a map* $\beta\colon N \to P$ *with* $\beta\alpha = 0$, *there is a unique map* $\gamma\colon \operatorname{Coker}(\alpha) \to P$ *with* $\gamma\kappa = \beta$ as shown below

$$\begin{array}{ccccc} M & \xrightarrow{\alpha} & N & \xrightarrow{\kappa} & \operatorname{Coker}(\alpha) \\ & \searrow & \big\downarrow\beta & \swarrow_{\gamma} & \\ & & P & & \end{array}$$

Further, **(4.6.1)** becomes $\operatorname{Coim}(\alpha) \xrightarrow{\sim} \operatorname{Im}(\alpha)$.

(4.10) (*Free modules*). — Let R be a ring, Λ a set, M a module. Given elements $m_\lambda \in M$ for $\lambda \in \Lambda$, by the submodule they **generate**, we mean the smallest submodule that contains them all. Clearly, any submodule that contains them all contains any (finite) linear combination $\sum x_\lambda m_\lambda$ with $x_\lambda \in R$. On the other hand, consider the set N of all such linear combinations; clearly, N is a submodule containing the m_λ. Thus N is the submodule generated by the m_λ.

The m_λ are said to be **free** or **linearly independent** if, whenever $\sum x_\lambda m_\lambda = 0$, also $x_\lambda = 0$ for all λ. Finally, the m_λ are said to form a **free basis** of M if they are free and generate M; if so, then we say M is **free** on the m_λ.

We say M is **finitely generated** if it has a finite set of generators.

We say M is **free** if it has a free basis. If so, then by (10.5) below, any two free bases have the same number ℓ of elements, and we say M is **free of rank** ℓ.

For example, form the set of **restricted vectors**

$$R^{\oplus\Lambda} := \{(x_\lambda) \mid x_\lambda \in R \text{ with } x_\lambda = 0 \text{ for almost all } \lambda\}.$$

It is a module under componentwise addition and scalar multiplication. It has a **standard basis**, nbbwhich consists of the vectors e_μ whose λth component is the

value of the **Kronecker delta function**; that is,

$$e_\mu := (\delta_{\mu\lambda}) \quad \text{where} \quad \delta_{\mu\lambda} := \begin{cases} 1, & \text{if } \lambda = \mu; \\ 0, & \text{if } \lambda \neq \mu. \end{cases}$$

Clearly the standard basis is free. If Λ has a finite number ℓ of elements, then $R^{\oplus\Lambda}$ is often written R^ℓ and called the **direct sum of ℓ copies** of R.

The free module $R^{\oplus\Lambda}$ has the following UMP: *given a module M and elements $m_\lambda \in M$ for $\lambda \in \Lambda$, there is a unique homomorphism*

$$\alpha\colon R^{\oplus\Lambda} \to M \text{ with } \alpha(e_\lambda) = m_\lambda \text{ for each } \lambda \in \Lambda;$$

namely, $\alpha\big((x_\lambda)\big) = \alpha\big(\sum x_\lambda e_\lambda\big) = \sum x_\lambda m_\lambda$. Note the following obvious statements:

(1) *α is surjective if and only if the m_λ generate M.*
(2) *α is injective if and only if the m_λ are linearly independent.*
(3) *α is an isomorphism if and only if the m_λ form a free basis.*

Thus *M is free of rank ℓ if and only if $M \simeq R^\ell$.*

Example **(4.11)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Q}$. Then any two x, y in M are not free; indeed, if $x = a/b$ and $y = -c/d$, then $bcx + ady = 0$. So M is not free. Also M is not finitely generated. Indeed, given any $m_1/n_1, \dots, m_r/n_r \in M$, let d be a common multiple of $n_1, \dots, n_r$. Then $(1/d)\mathbb{Z}$ contains every linear combination $x_1(m_1/n_1) + \cdots + x_\ell(m_\ell/n_\ell)$, but $(1/d)\mathbb{Z} \neq M$.

Exercise **(4.12)**. — Let R be a domain, and $x \in R$ nonzero. Let M be the submodule of $\mathrm{Frac}(R)$ generated by 1, x^{-1}, $x^{-2}, \dots$. Suppose that M is finitely generated. Prove that $x^{-1} \in R$, and conclude that $M = R$.

(4.13) (*Direct Products, Direct Sums*). — Let R be a ring, Λ a set, M_λ a module for $\lambda \in \Lambda$. The **direct product** of the M_λ is the set of arbitrary vectors:

$$\prod M_\lambda := \{(m_\lambda) \mid m_\lambda \in M_\lambda\}.$$

Clearly, $\prod M_\lambda$ is a module under componentwise addition and scalar multiplication.

The **direct sum** of the M_λ is the subset of **restricted vectors**:

$$\bigoplus M_\lambda := \{(m_\lambda) \mid m_\lambda = 0 \text{ for almost all } \lambda\} \subset \prod M_\lambda.$$

Clearly, $\bigoplus M_\lambda$ is a submodule of $\prod M_\lambda$. Clearly, $\bigoplus M_\lambda = \prod M_\lambda$ if Λ is finite. If $\Lambda = \{\lambda_1, \dots, \lambda_n\}$, then $\bigoplus M_\lambda$ is also denoted by $M_{\lambda_1} \oplus \cdots \oplus M_{\lambda_n}$.

The direct product comes equipped with projections

$$\pi_\kappa\colon \prod M_\lambda \to M_\kappa \quad \text{given by} \quad \pi_\kappa\big((m_\lambda)\big) := m_\kappa.$$

It is easy to see that $\prod M_\lambda$ has this UMP: *given homomorphisms $\alpha_\kappa\colon N \to M_\kappa$, there is a unique homomorphism $\alpha\colon N \to \prod M_\lambda$ satisfying $\pi_\kappa\alpha = \alpha_\kappa$* for all $\kappa \in \Lambda$; namely, $\alpha(n) = \big(\alpha_\lambda(n)\big)$. Often, α is denoted (α_λ). In other words, the π_λ induce a bijection of sets,

$$\mathrm{Hom}\big(N, \textstyle\prod M_\lambda\big) \xrightarrow{\sim} \prod \mathrm{Hom}(N, M_\lambda). \tag{4.13.1}$$

Clearly, this bijection is an isomorphism of modules.

Similarly, the direct sum comes equipped with injections

$$\iota_\kappa\colon M_\kappa \to \bigoplus M_\lambda \quad \text{given by} \quad \iota_\kappa(m) := (m_\lambda) \text{ where } m_\lambda := \begin{cases} m, & \text{if } \lambda = \kappa; \\ 0, & \text{if } \lambda \neq \kappa. \end{cases}$$

It is easy to see that it has this UMP: *given homomorphisms $\beta_\kappa\colon M_\kappa \to N$, there is*

a unique homomorphism $\beta\colon \bigoplus M_\lambda \to N$ *satisfying* $\beta\iota_\kappa = \beta_\kappa$ for all $\kappa \in \Lambda$; namely, $\beta\big((m_\lambda)\big) = \sum \beta_\lambda(m_\lambda)$. Often, β is denoted $\sum \beta_\lambda$; often, (β_λ). In other words, the ι_κ induce this bijection of sets:

$$\operatorname{Hom}\big(\bigoplus M_\lambda,\, N\big) \xrightarrow{\sim} \prod \operatorname{Hom}(M_\lambda,\, N). \tag{4.13.2}$$

Clearly, this bijection is an isomorphism of modules.

For example, if $M_\lambda = R$ for all λ, then $\bigoplus M_\lambda = R^{\oplus\Lambda}$ by construction. Further, if $N_\lambda := N$ for all λ, then $\operatorname{Hom}(R^{\oplus\Lambda},\, N) = \prod N_\lambda$ by **(4.13.2)** and **(4.3)**.

Exercise **(4.14)**. — Let Λ be an infinite set, R_λ a ring for $\lambda \in \Lambda$. Endow $\prod R_\lambda$ and $\bigoplus R_\lambda$ with componentwise addition and multiplication. Show that $\prod R_\lambda$ has a multiplicative identity (so is a ring), but that $\bigoplus R_\lambda$ does not (so is not a ring).

Exercise **(4.15)**. — Let R be a ring, L, M, and N modules. Consider a diagram

$$L \underset{\rho}{\overset{\alpha}{\rightleftarrows}} M \underset{\sigma}{\overset{\beta}{\rightleftarrows}} N$$

where α, β, ρ, and σ are homomorphisms. Prove that

$$M = L \oplus N \quad \text{and} \quad \alpha = \iota_L,\ \beta = \pi_N,\ \sigma = \iota_N,\ \rho = \pi_L$$

if and only if the following relations hold:

$$\beta\alpha = 0,\ \beta\sigma = 1,\ \rho\sigma = 0,\ \rho\alpha = 1,\ \text{and } \alpha\rho + \sigma\beta = 1.$$

Exercise **(4.16)**. — Let R be a ring, N a module, Λ a set, M_λ a module for $\lambda \in \Lambda$. Show that the injections $\iota_\kappa\colon M_\kappa \to \bigoplus M_\lambda$ induce an injection

$$\bigoplus \operatorname{Hom}(N,\, M_\lambda) \hookrightarrow \operatorname{Hom}(N,\, \bigoplus M_\lambda),$$

and that it is an isomorphism if N is finitely generated.

Exercise **(4.17)**. — Let R be a ring, $\mathfrak{a}$ an ideal, Λ a set, M_λ a module for $\lambda \in \Lambda$. Show $\mathfrak{a}\big(\bigoplus M_\lambda\big) = \bigoplus \mathfrak{a}M_\lambda$. Show $\mathfrak{a}(\prod M_\lambda) = \prod \mathfrak{a}M_\lambda$ if $\mathfrak{a}$ is finitely generated.

5. Exact Sequences

In the study of modules, the exact sequence plays a central role. We relate it to the kernel and image, the direct sum and direct product. We introduce diagram chasing, and prove the Snake Lemma, which is a fundamental result in homological algebra. We define projective modules, and characterize them in four ways. Finally, we prove Schanuel's Lemma, which relates two arbitrary presentations of a module.

DEFINITION **(5.1)**. — A (finite or infinite) sequence of module homomorphisms

$$\cdots \to M_{i-1} \xrightarrow{\alpha_{i-1}} M_i \xrightarrow{\alpha_i} M_{i+1} \to \cdots$$

is said to be **exact at** M_i if $\mathrm{Ker}(\alpha_i) = \mathrm{Im}(\alpha_{i-1})$. The sequence is said to be **exact** if it is exact at every M_i, except an initial source or final target.

PROPOSITION **(5.2)**. — *For $\lambda \in \Lambda$, let $M'_\lambda \to M_\lambda \to M''_\lambda$ be a sequence of module homomorphisms. If every sequence is exact, then so are the two induced sequences*

$$\bigoplus M'_\lambda \to \bigoplus M_\lambda \to \bigoplus M''_\lambda \quad \textit{and} \quad \prod M'_\lambda \to \prod M_\lambda \to \prod M''_\lambda.$$

Conversely, if either induced sequence is exact then so is every original one.

PROOF: The assertions are immediate from **(5.1)** and **(4.13)**. □

EXAMPLE **(5.3)**. — (1) A sequence $0 \to L \xrightarrow{\alpha} M$ is exact if and only if α is injective. If so, then we often identify L with its image $\alpha(L)$.

Dually — that is, in the analogous situation with all arrows reversed — a sequence $M \xrightarrow{\beta} N \to 0$ is exact if and only if β is surjective.

(2) A sequence $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is exact if and only if $L = \mathrm{Ker}(\beta)$, where '=' means "canonically isomorphic." Dually, a sequence $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is exact if and only if $N = \mathrm{Coker}(\alpha)$ owing to (1) and **(4.6.1)**.

(5.4) (*Short exact sequences*). — A sequence $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is exact if and only if α is injective and $N = \mathrm{Coker}(\alpha)$, or dually, if and only if β is surjective and $L = \mathrm{Ker}(\beta)$. If so, then the sequence is called **short exact**, and often we regard L as a submodule of M, and N as the quotient M/L.

For example, the following sequence is clearly short exact:

$$0 \to L \xrightarrow{\iota_L} L \oplus N \xrightarrow{\pi_N} N \to 0.$$

Often, we identify L with $\iota_L L$ and N with $\iota_N N$.

EXERCISE **(5.5)**. — Let M' and M'' be modules, $N \subset M'$ a submodule. Set $M := M' \oplus M''$. Using **(5.3)**(1) and **(5.4)** and **(5.2)**, prove $M/N = M'/N \oplus M''$.

EXERCISE **(5.6)**. — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Prove that, if M' and M'' are finitely generated, then so is M.

LEMMA **(5.7)**. — *Let $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ be a short exact sequence, and $N \subset M$ a submodule. Set $N' := \alpha^{-1}(N)$ and $N'' := \beta(N)$. Then the induced sequence $0 \to N' \to N \to N'' \to 0$ is short exact.*

PROOF: It is simple and straightforward to verify the asserted exactness. □

DEFINITION **(5.8)**. — We say that a short exact sequence

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0 \tag{5.8.1}$$

splitsif there is an isomorphism $\varphi\colon M \xrightarrow{\sim} M' \oplus M''$ with $\varphi\alpha = \iota_{M'}$ and $\beta = \pi_{M''}\varphi$.

We call a homomorphism $\rho\colon M \to M'$ a **retraction** of α if $\rho\alpha = 1_{M'}$.

Dually, we call a homomorphism $\sigma\colon M'' \to M$ a **section** of β if $\beta\sigma = 1_{M''}$.

PROPOSITION **(5.9)**. — *Let $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ be a short exact sequence of modules. Then the following conditions are equivalent:*

(1) *The sequence splits.*
(2) *There exists a retraction $\rho\colon M \to M'$ of α.*
(3) *There exists a section $\sigma\colon M'' \to M$ of β.*

PROOF: Assume (1). Then there exists $\varphi\colon M \xrightarrow{\sim} M' \oplus M''$ such that $\varphi\alpha = \iota_{M'}$ and $\beta = \pi_{M''}\varphi$. Set $\rho := \pi_{M'}\varphi$ and $\sigma := \varphi^{-1}\iota_{M''}$. Then clearly (2) and (3) hold.

Assume (2). Set $\sigma' := 1_M - \alpha\rho$. Then $\sigma'\alpha = \alpha - \alpha\rho\alpha = 0$. So there exists $\sigma\colon M'' \to M$ with $\sigma\beta = \sigma'$ by **(5.3)**(2) and the UMP of **(4.9)**. So $1_M = \alpha\rho + \sigma\beta$. Since $\beta\sigma\beta = \beta$ and β is surjective, $\beta\sigma = 1_{M''}$. Hence $\alpha\rho\sigma = 0$. Since α is injective, $\rho\sigma = 0$. Thus **(4.15)** yields (1) and also (3).

Assume (3). Then similarly (1) and (2) hold. □

EXERCISE **(5.10)**. — Let M', M'' be modules, and set $M := M' \oplus M''$. Let N be a submodule of M containing M', and set $N'' := N \cap M''$. Prove $N = M' \oplus N''$.

EXERCISE **(5.11)**. — Criticize the following misstatement of **(5.9)**: given a short exact sequence $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$, there is an isomorphism $M \simeq M' \oplus M''$ if and only if there is a section $\sigma\colon M'' \to M$ of β.

LEMMA **(5.12)** (Snake). — *Consider this commutative diagram with exact rows:*

$$\begin{array}{ccccccc} M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \to & 0 \\ {\scriptstyle\gamma'}\downarrow & & {\scriptstyle\gamma}\downarrow & & {\scriptstyle\gamma''}\downarrow & & \\ 0 & \to & N' & \xrightarrow{\alpha'} & N & \xrightarrow{\beta'} & N'' \end{array}$$

It yields the following exact sequence:

$$\operatorname{Ker}(\gamma') \xrightarrow{\varphi} \operatorname{Ker}(\gamma) \xrightarrow{\psi} \operatorname{Ker}(\gamma'') \xrightarrow{\partial} \operatorname{Coker}(\gamma') \xrightarrow{\varphi'} \operatorname{Coker}(\gamma) \xrightarrow{\psi'} \operatorname{Coker}(\gamma''). \tag{5.12.1}$$

Moreover, if α is injective, then so is φ; dually, if β' is surjective, then so is ψ'.

PROOF: Clearly α yields a unique compatible homomorphism $\operatorname{Ker}(\gamma') \to \operatorname{Ker}(\gamma)$ because $\gamma\alpha\big(\operatorname{Ker}(\gamma')\big) = 0$. By the UMP discussed in **(4.9)**, α' yields a unique compatible homomorphism φ' because M' goes to 0 in $\operatorname{Coker}(\gamma)$. Similarly, β and β' induce corresponding homomorphisms ψ and ψ'. Thus all the homomorphisms in **(5.12.1)** are defined except for ∂.

To define ∂, **chase** an $m'' \in \operatorname{Ker}(\gamma'')$ through the diagram. Since β is surjective, there is $m \in M$ such that $\beta(m) = m''$. By commutativity, $\gamma''\beta(m) = \beta'\gamma(m)$. So $\beta'\gamma(m) = 0$. By exactness of the bottom row, there is a unique $n' \in N'$ such that $\alpha'(n') = \gamma(m)$. Define $\partial(m'')$ to be the image of n' in $\operatorname{Coker}(\gamma')$.

To see ∂ is well defined, choose another $m_1 \in M$ with $\beta(m_1) = m''$. Let $n'_1 \in N'$ be the unique element with $\alpha'(n'_1) = \gamma(m_1)$ as above. Since $\beta(m - m_1) = 0$, there is an $m' \in M'$ with $\alpha(m') = m - m_1$. But $\alpha'\gamma' = \gamma\alpha$. So $\alpha'\gamma'(m') = \alpha'(n' - n'_1)$. Hence $\gamma'(m') = n' - n'_1$ since α' is injective. So n' and n'_1 have the same image in $\operatorname{Coker}(\gamma')$. Thus ∂ is well defined.

Let's show that **(5.12.1)** is exact at $\mathrm{Ker}(\gamma'')$. Take $m'' \in \mathrm{Ker}(\gamma'')$. As in the construction of ∂, take $m \in M$ such that $\beta(m) = m''$ and take $n' \in N'$ such that $\alpha'(n') = \gamma(m)$. Suppose $m'' \in \mathrm{Ker}(\partial)$. Then the image of n' in $\mathrm{Coker}(\gamma')$ is equal to 0; so there is $m' \in M'$ such that $\gamma'(m') = n'$. Clearly $\gamma\alpha(m') = \alpha'\gamma'(m')$. So $\gamma\alpha(m') = \alpha'(n') = \gamma(m)$. Hence $m - \alpha(m') \in \mathrm{Ker}(\gamma)$. Since $\beta\big(m - \alpha(m')\big) = m''$, clearly $m'' = \psi(m - \alpha(m'))$; so $m'' \in \mathrm{Im}(\psi)$. Hence $\mathrm{Ker}(\partial) \subset \mathrm{Im}(\psi)$.

Conversely, suppose $m'' \in \mathrm{Im}(\psi)$. We may assume $m \in \mathrm{Ker}(\gamma)$. So $\gamma(m) = 0$ and $\alpha'(n') = 0$. Since α' is injective, $n' = 0$. Thus $\partial(m'') = 0$, and so $\mathrm{Im}(\psi) \subset \mathrm{Ker}(\partial)$. Thus $\mathrm{Ker}(\partial)$ is equal to $\mathrm{Im}(\psi)$; that is, **(5.12.1)** is exact at $\mathrm{Ker}(\gamma'')$.

The other verifications of exactness are similar or easier.

The last two assertions are clearly true. □

Exercise **(5.13)**. — Referring to **(4.8)**, give an alternative proof that β is an isomorphism by applying the Snake Lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & N/M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle\kappa} & & \downarrow{\scriptstyle\beta} & & \\ 0 & \to & M/L & \to & N/L & \xrightarrow{\lambda} & (N/L)/(M/L) & \to & 0 \end{array}$$

Exercise **(5.14)** (*Five Lemma*). — Consider this commutative diagram:

$$\begin{array}{ccccccccc} M_4 & \xrightarrow{\alpha_4} & M_3 & \xrightarrow{\alpha_3} & M_2 & \xrightarrow{\alpha_2} & M_1 & \xrightarrow{\alpha_1} & M_0 \\ \downarrow{\scriptstyle\gamma_4} & & \downarrow{\scriptstyle\gamma_3} & & \downarrow{\scriptstyle\gamma_2} & & \downarrow{\scriptstyle\gamma_1} & & \downarrow{\scriptstyle\gamma_0} \\ N_4 & \xrightarrow{\beta_4} & N_3 & \xrightarrow{\beta_3} & N_2 & \xrightarrow{\beta_2} & N_1 & \xrightarrow{\beta_1} & N_0 \end{array}$$

Assume it has exact rows. Via a chase, prove these two statements:

(1) If γ_3 and γ_1 are surjective and if γ_0 is injective, then γ_2 is surjective.
(2) If γ_3 and γ_1 are injective and if γ_4 is surjective, then γ_2 is injective.

Exercise **(5.15)** (*Nine Lemma*). — Consider this commutative diagram:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L' & \longrightarrow & L & \longrightarrow & L'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M' & \to & M & \to & M'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & N' & \to & N & \to & N'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} \qquad \textbf{(5.15.1)}$$

Assume all the columns are exact and the middle row is exact. Applying the Snake Lemma, prove that the first row is exact if and only if the third is.

Exercise **(5.16)**. — Consider this commutative diagram with exact rows:

$$\begin{array}{ccccc} M' & \xrightarrow{\beta} & M & \xrightarrow{\gamma} & M'' \\ \downarrow{\scriptstyle\alpha'} & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha''} \\ N' & \xrightarrow{\beta'} & N & \xrightarrow{\gamma'} & N'' \end{array}$$

Assume α' and γ are surjective. Given $n \in N$ and $m'' \in M''$ with $\alpha''(m'') = \gamma'(n)$, show that there is $m \in M$ such that $\alpha(m) = n$ and $\gamma(m) = m''$.

THEOREM **(5.17)** (Left exactness of Hom). — (1) *Let $M' \to M \to M'' \to 0$ be a sequence of module homomorphisms. Then it is exact if and only if, for all modules N, the following induced sequence is exact:*

$$0 \to \mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N). \tag{5.17.1}$$

(2) *Let $0 \to N' \to N \to N''$ be a sequence of module homomorphisms. Then it is exact if and only if, for all modules M, the following induced sequence is exact:*

$$0 \to \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'').$$

PROOF: By **(5.3)**(2), the exactness of $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ means simply that $M'' = \mathrm{Coker}(\alpha)$. On the other hand, the exactness of **(5.17.1)** means that a $\varphi \in \mathrm{Hom}(M, N)$ maps to 0, or equivalently $\varphi\alpha = 0$, if and only if there is a unique $\gamma\colon M'' \to N$ such that $\gamma\beta = \varphi$. So **(5.17.1)** is exact if and only if M'' has the UMP of $\mathrm{Coker}(\alpha)$, discussed in **(4.9)**; that is, $M'' = \mathrm{Coker}(\alpha)$. Thus (1) holds.

The proof of (2) is similar. □

DEFINITION **(5.18)**. — A (free) **presentation** of a module M is an exact sequence

$$G \to F \to M \to 0$$

with G and F free. If G and F are free of finite rank, then the presentation is called **finite**. If M has a finite presentation, then M is said to be **finitely presented**.

PROPOSITION **(5.19)**. — *Given a module M and a set of generators $\{m_\lambda\}_{\lambda\in\Lambda}$, there is an exact sequence $0 \to K \to R^{\oplus\Lambda} \xrightarrow{\alpha} M \to 0$ with $\alpha(e_\lambda) = m_\lambda$, where $\{e_\lambda\}$ is the standard basis; further, there is a presentation $R^{\oplus\Sigma} \to R^{\oplus\Lambda} \xrightarrow{\alpha} M \to 0$.*

PROOF: By **(4.10)**(1), there is a surjection $\alpha\colon R^{\oplus\Lambda} \twoheadrightarrow M$ with $\alpha(e_\lambda) = m_\lambda$. Set $K := \mathrm{Ker}(\alpha)$. Then $0 \to K \to R^{\oplus\Lambda} \to M \to 0$ is exact by **(5.4)**. Take a set of generators $\{k_\sigma\}_{\sigma\in\Sigma}$ of K, and repeat the process to obtain a surjection $R^{\oplus\Sigma} \twoheadrightarrow K$. Then $R^{\oplus\Sigma} \to R^{\oplus\Lambda} \to M \to 0$ is a presentation. □

DEFINITION **(5.20)**. — A module P is called **projective** if, given any surjective homomorphism $\beta\colon M \twoheadrightarrow N$, every homomorphism $\alpha\colon P \to N$ **lifts** to a homomorphism $\gamma\colon P \to M$; that is, $\alpha = \beta\gamma$.

EXERCISE **(5.21)**. — Show that a free module $R^{\oplus\Lambda}$ is projective.

THEOREM **(5.22)**. — *The following conditions on a module P are equivalent:*

(1) *The module P is projective.*
(2) *Every short exact sequence $0 \to K \to M \to P \to 0$ splits.*
(3) *There is a module K such that $K \oplus P$ is free.*
(4) *Every exact sequence $N' \to N \to N''$ induces an exact sequence*

$$\mathrm{Hom}(P, N') \to \mathrm{Hom}(P, N) \to \mathrm{Hom}(P, N''). \tag{5.22.1}$$

(5) *Every surjective homomorphism $\beta\colon M \twoheadrightarrow N$ induces a surjection*

$$\mathrm{Hom}(P, \beta)\colon \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, N).$$

PROOF: Assume (1). In (2), the surjection $M \twoheadrightarrow P$ and the identity $P \to P$ yield a section $P \to M$. So the sequence splits by **(5.9)**. Thus (2) holds.

Assume (2). By **(5.19)**, there is an exact sequence $0 \to K \to R^{\oplus\Lambda} \to P \to 0$. Then (2) implies $K \oplus P \simeq R^{\oplus\Lambda}$. Thus (3) holds.

Assume (3); say $K \oplus P \simeq R^{\oplus\Lambda}$. For each $\lambda \in \Lambda$, take a copy $N'_\lambda \to N_\lambda \to N'_\lambda$ of the exact sequence $N' \to N \to N''$ of (4). Then the induced sequence

$$\prod N'_\lambda \to \prod N_\lambda \to \prod N''_\lambda.$$

is exact by **(5.2)**. But by the end of **(4.13)**, that sequence is equal to this one:

$$\operatorname{Hom}(R^{\oplus\Lambda}, N') \to \operatorname{Hom}(R^{\oplus\Lambda}, N) \to \operatorname{Hom}(R^{\oplus\Lambda}, N'').$$

But $K \oplus P \simeq R^{\oplus\Lambda}$. So owing to **(4.13.2)**, the latter sequence is also equal to

$$\operatorname{Hom}(K, N') \oplus \operatorname{Hom}(P, N') \to \operatorname{Hom}(K, N) \oplus \operatorname{Hom}(P, N) \to \operatorname{Hom}(K, N'') \oplus \operatorname{Hom}(P, N'').$$

Hence **(5.22.1)** is exact by **(5.2)**. Thus (4) holds.

Assume (4). Then every exact sequence $M \xrightarrow{\beta} N \to 0$ induces an exact sequence

$$\operatorname{Hom}(P, M) \to \operatorname{Hom}(P, N) \to 0.$$

In other words, (5) holds.

Assume (5). By definition, $\operatorname{Hom}(P, \beta)(\gamma) = \beta\gamma$. Therefore, (1) holds. □

LEMMA **(5.23)** (Schanuel). — *Given two short exact sequences*

$$0 \to L \xrightarrow{i} P \xrightarrow{\alpha} M \to 0 \quad \textit{and} \quad 0 \to L' \xrightarrow{i'} P' \xrightarrow{\alpha'} M \to 0$$

with P and P' projective, there is an isomorphism of exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & L \oplus P' & \xrightarrow{i\oplus 1_{P'}} & P \oplus P' & \xrightarrow{(\alpha\ 0)} & M & \to & 0 \\ & & \cong\downarrow{\scriptstyle\beta} & & \cong\downarrow{\scriptstyle\gamma} & & =\downarrow{\scriptstyle 1_M} & & \\ 0 & \to & P \oplus L' & \xrightarrow{1_P\oplus i'} & P \oplus P' & \xrightarrow{(0\ \alpha')} & M & \to & 0 \end{array}$$

PROOF: First, let's construct an intermediate isomorphism of exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & L \oplus P' & \xrightarrow{i\oplus 1_{P'}} & P \oplus P' & \xrightarrow{(\alpha\ 0)} & M & \to & 0 \\ & & \cong\uparrow{\scriptstyle\lambda} & & \cong\uparrow{\scriptstyle\theta} & & =\uparrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & K & \longrightarrow & P \oplus P' & \xrightarrow{(\alpha\ \alpha')} & M & \to & 0 \end{array}$$

Take $K := \operatorname{Ker}(\alpha\,\alpha')$. To form θ, recall that P' is projective and α is surjective. So there is a map $\pi\colon P' \to P$ such that $\alpha' = \alpha\pi$. Take $\theta := \left(\begin{smallmatrix} 1 & \pi \\ 0 & 1 \end{smallmatrix}\right)$.

Then θ has $\left(\begin{smallmatrix} 1 & -\pi \\ 0 & 1 \end{smallmatrix}\right)$ as inverse. Further, the right-hand square is commutative:

$$(\alpha\ 0)\theta = (\alpha\ 0)\left(\begin{smallmatrix} 1 & \pi \\ 0 & 1 \end{smallmatrix}\right) = (\alpha\ \alpha\pi) = (\alpha\ \alpha').$$

So θ induces the desired isomorphism $\lambda\colon K \xrightarrow{\sim} L \oplus P'$.

Symmetrically, form an automorphism θ' of $P \oplus P'$, which induces an isomorphism $\lambda'\colon K \xrightarrow{\sim} P \oplus L'$. Finally, take $\gamma := \theta'\theta^{-1}$ and $\beta := \lambda'\lambda^{-1}$. □

PROPOSITION **(5.24)**. — *Let R be a ring, M a finitely presented module. Then in any exact sequence $0 \to L \to R^n \to M \to 0$, necessarily L is finitely generated.*

PROOF: By hypothesis, there is a finite presentation $R^l \to R^m \to M \to 0$. Let L' be the image of R^l in R^m. Then $L' \oplus R^n \simeq L \oplus R^m$ by Schanuel's Lemma **(5.23)**. Hence L is a quotient of $R^l \oplus R^n$. Thus L is finitely generated. □

EXERCISE **(5.25)**. — Let R be a ring, $P := R[X_1, X_2, \dots]$ the polynomial ring. Set $M := P/\langle X_1, X_2, \dots \rangle$. Is M finitely generated? Finitely presented? Explain.

EXERCISE **(5.26)**. — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Assume M' and M'' are finitely presented. Show that M is too.

6. Direct Limits

Category theory provides the right abstract setting for certain common concepts, constructions, and proofs. Here we treat adjoints and direct limits. We elaborate on two key special cases of direct limits: coproducts (direct sums) and coequalizers (cokernels). Then we construct arbitrary direct limits of sets and of modules. Further, we prove direct limits are preserved by left adjoints; whence, direct limits commute with each other other, and in particular, with coproducts and coequalizers.

Although this section is the most abstract of the entire book, all the material here is elementary, and none of it is very deep. In fact, many statements are just concise restatements in more expressive language; they can be understood through a simple translation of terms. Experience shows that it pays to learn this more abstract language, but that doing so requires determined, yet modest effort.

(6.1) (*Categories*). — A **category** $\mathcal{C}$ is a collection of elements, called **objects**. Each pair of objects A, B is equipped with a set $\mathrm{Hom}_{\mathcal{C}}(A,B)$ of elements, called **maps** or **morphisms**. We write $\alpha\colon A \to B$ or $A \xrightarrow{\alpha} B$ to mean $\alpha \in \mathrm{Hom}_{\mathcal{C}}(A,B)$.

Further, given objects A, B, C, there is a **composition law**

$$\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \to \mathrm{Hom}_{\mathcal{C}}(A,C), \quad \text{written} \quad (\alpha,\beta) \mapsto \beta\alpha,$$

and there is a distinguished map $1_B \in \mathrm{Hom}_{\mathcal{C}}(B,B)$, called the **identity** such that

(1) composition is **associative**, or $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ for $\gamma\colon C \to D$, and
(2) 1_B is **unitary**, or $1_B\alpha = \alpha$ and $\beta 1_B = \beta$.

We say α is an **isomorphism** with **inverse** $\beta\colon B \to A$ if $\alpha\beta = 1_B$ and $\beta\alpha = 1_A$.

For example, four common categories are those of sets ((Sets)), of rings ((Rings)), of R-modules ((R-mod)), and of R-algebras ((R-alg)); the corresponding maps are the set maps, and the ring, R-module, and R-algebra homomorphisms.

Given categories $\mathcal{C}$ and $\mathcal{C}'$, their **product** $\mathcal{C} \times \mathcal{C}'$ is the category whose objects are the pairs (A, A') with A an object of $\mathcal{C}$ and A' an object of $\mathcal{C}'$ and whose maps are the pairs (α, α') of maps α in $\mathcal{C}$ and α' in $\mathcal{C}'$.

(6.2) (*Functors*). — A map of categories is known as a functor. Namely, given categories $\mathcal{C}$ and $\mathcal{C}'$, a (**covariant**) **functor** $F\colon \mathcal{C} \to \mathcal{C}'$ is a rule that assigns to each object A of $\mathcal{C}$ an object $F(A)$ of $\mathcal{C}'$ and to each map $\alpha\colon A \to B$ of $\mathcal{C}$ a map $F(\alpha)\colon F(A) \to F(B)$ of $\mathcal{C}'$ preserving composition and identity; that is,

(1) $F(\beta\alpha) = F(\beta)F(\alpha)$ for maps $\alpha\colon A \to B$ and $\beta\colon B \to C$ of $\mathcal{C}$, and
(2) $F(1_A) = 1_{F(A)}$ for any object A of $\mathcal{C}$.

We also denote a functor F by $F(\bullet)$, by $A \mapsto F(A)$, or by $A \mapsto F_A$.

Note that a functor F preserves isomorphisms. Indeed, if $\alpha\beta = 1_B$ and $\beta\alpha = 1_A$, then $F(\alpha)F(\beta) = 1_{F(B)}$ and $F(\beta)F(\alpha) = F(1_A)$.

For example, let R be a ring, M a module. Then clearly $\mathrm{Hom}_R(M, \bullet)$ is a functor from ((R-mod)) to ((R-mod)). A second example is the **forgetful functor** from ((R-mod)) to ((Sets)); it sends a module to its underlying set and a homomorphism to its underlying set map.

A map of functors is known as a natural transformation. Namely, given two functors $F, F'\colon \mathcal{C} \rightrightarrows \mathcal{C}'$, a **natural transformation** $\theta\colon F \to F'$ is a collection of maps $\theta(A)\colon F(A) \to F'(A)$, one for each object A of $\mathcal{C}$, such that $\theta(B)F(\alpha) = F'(\alpha)\theta(A)$

for every map $\alpha\colon A \to B$ of $\mathcal{C}$; that is, the following diagram is commutative:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(\alpha)} & F(B) \\ {\scriptstyle\theta(A)}\downarrow & & \downarrow{\scriptstyle\theta(B)} \\ F'(A) & \xrightarrow{F'(\alpha)} & F'(B) \end{array}$$

For example, the identity maps $1_{F(A)}$ trivially form a natural transformation 1_F from any functor F to itself. We call F and F' **isomorphic** if there are natural transformations $\theta\colon F \to F'$ and $\theta'\colon F' \to F$ with $\theta'\theta = 1_F$ and $\theta\theta' = 1_{F'}$.

A **contravariant** functor G from $\mathcal{C}$ to $\mathcal{C}'$ is a rule similar to F, but G reverses the direction of maps; that is, $G(\alpha)$ carries $G(B)$ to $G(A)$, and G satisfies the analogues of (1) and (2). For example, fix a module N; then $\mathrm{Hom}(\bullet, N)$ is a contravariant functor from $((R\text{-mod}))$ to $((R\text{-mod}))$.

Exercise **(6.3)**. — (1) Show that the condition **(6.2)**(1) is equivalent to the commutativity of the corresponding diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(C)\big) \end{array}$$

(2) Given $\gamma\colon C \to D$, show **(6.2)**(1) yields the commutativity of this diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,D) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(D)\big) \end{array}$$

(6.4) (*Adjoints*). — Let $\mathcal{C}$ and $\mathcal{C}'$ be categories, $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ functors. We call (F, F') an **adjoint pair**, F the **left adjoint** of F', and F' the **right adjoint** of F if, for each object $A \in \mathcal{C}$ and object $A' \in \mathcal{C}'$, there is a natural bijection

$$\mathrm{Hom}_{\mathcal{C}'}(F(A),\, A') \;\simeq\; \mathrm{Hom}_{\mathcal{C}}(A,\, F'(A')). \qquad \textbf{(6.4.1)}$$

Here **natural** means that maps $B \to A$ and $A' \to B'$ induce a commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}'}(F(A),\, A') & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\, F'(A')) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}'}(F(B),\, B') & \simeq & \mathrm{Hom}_{\mathcal{C}}(B,\, F'(B')) \end{array}$$

Naturality serves to determine an adjoint up to canonical isomorphism. Indeed, let F and G be two left adjoints of F'. Given $A \in \mathcal{C}$, define $\theta(A)\colon G(A) \to F(A)$ to be the image of $1_{F(A)}$ under the adjoint bijections

$$\mathrm{Hom}_{\mathcal{C}'}(F(A),\, F(A)) \;\simeq\; \mathrm{Hom}_{\mathcal{C}}(A,\, F'F(A)) \;\simeq\; \mathrm{Hom}_{\mathcal{C}'}(G(A),\, F(A)).$$

To see that $\theta(A)$ is natural in A, take a map $\alpha\colon A \to B$. It induces the following

diagram, which is commutative owing to the naturality of the adjoint bijections:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathcal{C}'}(F(A),\,F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\,F'F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}'}(G(A),\,F(A)) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_{\mathcal{C}'}(F(A),\,F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\,F'F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}'}(G(A),\,F(B)) \\
\uparrow & & \uparrow & & \uparrow \\
\mathrm{Hom}_{\mathcal{C}'}(F(B),\,F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(B,\,F'F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}'}(G(B),\,F(B))
\end{array}$$

Chase after $1_{F(A)}$ and $1_{F(B)}$. Both map to $F(\alpha) \in \mathrm{Hom}_{\mathcal{C}'}(F(A),\,F(B))$. So both map to the same image in $\mathrm{Hom}_{\mathcal{C}'}(G(A),\,F(B))$. But clockwise, $1_{F(A)}$ maps to $F(\alpha)\theta(A)$; counterclockwise, $1_{F(B)}$ maps to $\theta(B)G(\alpha)$. So $\theta(B)G(\alpha) = F(\alpha)\theta(A)$. Thus the $\theta(A)$ form a natural transformation $\theta\colon G \to F$.

Similarly, there is a natural transformation $\theta'\colon F \to G$. It remains to show $\theta'\theta = 1_G$ and $\theta\theta' = 1_F$. However, by naturality, this diagram is commutative:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathcal{C}'}(F(A),\,F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\,F'F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(G(A),\,F(A)) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_{\mathcal{C}'}(F(A),\,G(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\,F'G(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(G(A),\,G(A))
\end{array}$$

Chase after $1_{F(A)}$. Clockwise, its image is $\theta'(A)\theta(A)$ in the lower right corner. Counterclockwise, its image is $1_{G(A)}$, owing to the definition of θ'. Thus $\theta'\theta = 1_G$. Similarly, $\theta\theta' = 1_F$, as required.

For example, the "free module" functor is the left adjoint of the forgetful functor from $((R\text{-mod}))$ to $((\mathrm{Sets}))$, since by **(4.10)**,

$$\mathrm{Hom}_{((R\text{-mod}))}(R^{\oplus\Lambda},\,M) = \mathrm{Hom}_{((\mathrm{Sets}))}(\Lambda,\,M).$$

Similarly, the "polynomial ring" functor is the left adjoint of the forgetful functor from $((R\text{-alg}))$ to $((\mathrm{Sets}))$, since by **(1.2)**,

$$\mathrm{Hom}_{((R\text{-alg}))}\big(R[X_1,\ldots,X_n],\,R'\big) = \mathrm{Hom}_{((\mathrm{Sets}))}\big(\{X_1,\ldots,X_n\},\,R'\big).$$

Exercise **(6.5)**. — Let $\mathcal{C}$ and $\mathcal{C}'$ be categories, $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ an adjoint pair. Let $\varphi_{A,A'}\colon \mathrm{Hom}_{\mathcal{C}'}(FA,\,A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(A,\,F'A')$ denote the natural bijection, and set $\eta_A := \varphi_{A,FA}(1_{FA})$. Do the following:

(1) Prove η_A is natural in A; that is, given $g\colon A \to B$, the induced square

$$\begin{array}{ccc}
A & \xrightarrow{\eta_A} & F'FA \\
{\scriptstyle g}\downarrow & & \downarrow{\scriptstyle F'Fg} \\
B & \xrightarrow{\eta_B} & F'FB
\end{array}$$

is commutative. We call the natural transformation $A \mapsto \eta_A$ the **unit** of $(F,\,F')$.

(2) Given $f'\colon FA \to A'$, prove $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

(3) Prove the natural map $\eta_A\colon A \to F'FA$ is **universal** from A to F'; that is, given $f\colon A \to F'A'$, there is a unique map $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$.

(4) Conversely, instead of assuming $(F,\,F')$ is an adjoint pair, assume given a natural transformation $\eta\colon 1_{\mathcal{C}} \to F'F$ satisfying (1) and (3). Prove the equation in (2) defines a natural bijection making $(F,\,F')$ an adjoint pair, whose unit is η.

(5) Identify the units in the two examples in **(6.4)**: the "free module" functor and the "polynomial ring" functor.

(Dually, we can define a **counit** $\varepsilon\colon FF' \to 1_{\mathcal{C}'}$, and prove similar statements.)

(6.6) (*Direct limits*). — Let Λ, $\mathcal{C}$ be categories. Assume Λ is **small**; that is, its objects form a set. Given a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$, its **direct limit** or **colimit**, denoted $\varinjlim M_\lambda$ or $\varinjlim_{\lambda\in\Lambda} M_\lambda$, is defined as the universal example of an object P of $\mathcal{C}$ equipped with maps $\beta_\mu\colon M_\mu \to P$, called **insertions**, that are compatible with the **transition maps** $\alpha_\mu^\kappa\colon M_\kappa \to M_\mu$, which are the images of the maps of Λ. In other words, there is a unique map β such that all these diagrams commute:

$$\begin{array}{ccccc} M_\kappa & \xrightarrow{\alpha_\mu^\kappa} & M_\mu & \xrightarrow{\alpha_\mu} & \varinjlim M_\lambda \\ \downarrow{\scriptstyle \beta_\kappa} & & \downarrow{\scriptstyle \beta_\mu} & & \downarrow{\scriptstyle \beta} \\ P & \xrightarrow{1_P} & P & \xrightarrow{1_P} & P \end{array}$$

To indicated this context, the functor $\lambda \mapsto M_\lambda$ is often called a **direct system.**

As usual, universality implies that, once equipped with its insertions α_μ, the limit $\varinjlim M_\lambda$ is determined up to unique isomorphism, assuming it exists. In practice, there is usually a canonical choice for $\varinjlim M_\lambda$, given by a construction. In any case, let us use $\varinjlim M_\lambda$ to denote a particular choice.

We say that $\mathcal{C}$ **has direct limits indexed by** Λ if, for every functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$, the direct limit $\varinjlim M_\lambda$ exists. We say that $\mathcal{C}$ **has direct limits** if it has direct limits indexed by every small category Λ. We say that a functor $F\colon \mathcal{C} \to \mathcal{C}'$ **preserves direct limits** if, given any direct limit $\varinjlim M_\lambda$ in $\mathcal{C}$, the direct limit $\varinjlim F(M_\lambda)$ exists, and is equal to $F(\varinjlim M_\lambda)$; more precisely, the maps $F(\alpha_\mu)\colon F(M_\mu) \to F(\varinjlim M_\lambda)$ induce a canonical map

$$\phi\colon \varinjlim F(M_\lambda) \to F(\varinjlim M_\lambda),$$

and ϕ is an isomorphism. Sometimes, we construct $\varinjlim F(M_\lambda)$ by showing that $F(\varinjlim M_\lambda)$ has the requisite UMP.

Assume $\mathcal{C}$ has direct limits indexed by Λ. Then, given a natural transformation from $\lambda \mapsto M_\lambda$ to $\lambda \mapsto N_\lambda$, universality yields unique commutative diagrams

$$\begin{array}{ccc} M_\mu & \longrightarrow & \varinjlim M_\lambda \\ \downarrow & & \downarrow \\ N_\mu & \longrightarrow & \varinjlim N_\lambda \end{array}$$

To put it another way, form the **functor category** $\mathcal{C}^\Lambda$: its objects are the functors $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$, and its maps are the natural transformations (they form a set as Λ is one). Then taking direct limits yields a functor $\varinjlim$ from $\mathcal{C}^\Lambda$ to $\mathcal{C}$.

In fact, it is just a restatement of the definitions that the "direct limit" functor $\varinjlim$ is the left adjoint of the **diagonal functor**

$$\Delta\colon \mathcal{C} \to \mathcal{C}^\Lambda.$$

By definition, Δ sends each object M to the **constant functor** ΔM, which has the same value M at every $\lambda \in \Lambda$ and has the same value 1_M at every map of Λ; further, Δ carries a map $\gamma\colon M \to N$ to the natural transformation $\Delta\gamma\colon \Delta M \to \Delta N$, which has the same value γ at every $\lambda \in \Lambda$.

(6.7) (*Coproducts*). — Let $\mathcal{C}$ be a category, Λ a set, and M_λ an object of $\mathcal{C}$ for each $\lambda \in \Lambda$. The **coproduct** $\coprod_{\lambda\in\Lambda} M_\lambda$, or simply $\coprod M_\lambda$, is defined as the universal example of an object P equipped with a map $\beta_\mu\colon M_\mu \to P$ for each $\mu \in \Lambda$. The

maps $\iota_\mu\colon M_\mu \to \coprod M_\lambda$ are called the **inclusions**. Thus, given an example P, there exists a unique map $\beta\colon \coprod M_\lambda \to P$ with $\beta\iota_\mu = \beta_\mu$ for all $\mu \in \Lambda$.

For instance, if $\mathcal{C} = ((R\text{-mod}))$, then the coproduct $\coprod M_\lambda$ is just the direct sum $\bigoplus M_\lambda$. If $\mathcal{C} = ((\text{Sets}))$, then the coproduct $\coprod M_\lambda$ is the disjoint union $\bigsqcup M_\lambda$.

Note that the coproduct is a special case of the direct limit. Indeed, regard Λ as a **discrete** category: its objects are the $\lambda \in \Lambda$, and it has just the required maps, namely, the 1_λ. Then $\varinjlim M_\lambda = \coprod M_\lambda$ with the insertions equal to the inclusions.

(6.8) (*Coequalizers*). — Let $\alpha, \alpha'\colon M \to N$ be two maps in a category $\mathcal{C}$. Their **coequalizer** is defined as the universal example of an object P equipped with a map $\eta\colon N \to P$ such that $\eta\alpha = \eta\alpha'$.

For instance, if $\mathcal{C} = ((R\text{-mod}))$, then the coequalizer is $\operatorname{Coker}(\alpha - \alpha')$. In particular, the coequalizer of α and 0 is just $\operatorname{Coker}(\alpha)$.

Suppose $\mathcal{C} = ((\text{Sets}))$. Take the smallest equivalence relation $\sim$ on N with $\alpha(m) \sim \alpha'(m)$ for all $m \in M$; explicitly, $n \sim n'$ if there are elements $m_1, \dots, m_r$ with $\alpha(m_1) = n$, with $\alpha'(m_r) = n'$, and with $\alpha(m_i) = \alpha'(m_{i+1})$ for $1 \le i < r$. Clearly, the coequalizer is the quotient $N/\!\sim$ equipped with the quotient map.

Note that the coequalizer is a special case of the direct limit. Indeed, let Λ be the category consisting of two objects κ, μ and two nontrivial maps $\varphi, \varphi'\colon \kappa \to \mu$. Define $\lambda \mapsto M_\lambda$ in the obvious way: set $M_\kappa := M$ and $M_\mu := N$; send φ to α and φ' to α'. Then the coequalizer is $\varinjlim M_\lambda$.

Exercise **(6.9)**. — Let $\alpha\colon L \to M$ and $\beta\colon L \to N$ be two maps. Their **pushout** is defined as the universal example of an object P equipped with a pair of maps $\gamma\colon M \to P$ and $\delta\colon N \to P$ such that $\gamma\alpha = \delta\beta$. Express the pushout as a direct limit. Show that, in $((\text{Sets}))$, the pushout is the disjoint union $M \sqcup N$ modulo the smallest equivalence relation $\sim$ with $m \sim n$ if there is $\ell \in L$ with $\alpha(\ell) = m$ and $\beta(\ell) = n$. Show that, in $((R\text{-mod}))$, the pushout is equal to the direct sum $M \oplus N$ modulo the image of L under the map $(\alpha, -\beta)$.

Lemma **(6.10)**. — *A category $\mathcal{C}$ has direct limits if and only if $\mathcal{C}$ has coproducts and coequalizers. If a category $\mathcal{C}$ has direct limits, then a functor $F\colon \mathcal{C} \to \mathcal{C}'$ preserves them if and only if F preserves coproducts and coequalizers.*

Proof: If $\mathcal{C}$ has direct limits, then $\mathcal{C}$ has coproducts and coequalizers because they are special cases by **(6.7)** and **(6.8)**. By the same token, if $F\colon \mathcal{C} \to \mathcal{C}'$ preserves direct limits, then F preserves coproducts and coequalizers.

Conversely, assume that $\mathcal{C}$ has coproducts and coequalizers. Let Λ be a small category, and $\lambda \mapsto M_\lambda$ a functor from Λ to $\mathcal{C}$. Let Σ be the set of transition maps $\alpha_\mu^\lambda\colon M_\lambda \to M_\mu$. For each $\sigma := \alpha_\mu^\lambda \in \Sigma$, set $M_\sigma := M_\lambda$. Set $M := \coprod_{\sigma\in\Sigma} M_\sigma$ and $N := \coprod_{\lambda\in\Lambda} M_\lambda$. For each σ, there are two maps $M_\sigma := M_\lambda \to N$: the inclusion ι_λ and the composition $\iota_\mu\alpha_\mu^\lambda$. Correspondingly, there are two maps $\alpha, \alpha'\colon M \to N$. Let C be their coequalizer, and $\eta\colon N \to C$ the insertion.

Given maps $\beta_\lambda\colon M_\lambda \to P$ with $\beta_\mu\alpha_\mu^\lambda = \beta_\lambda$, there is a unique map $\beta\colon N \to P$ with $\beta\iota_\lambda = \beta_\lambda$ by the UMP of the coproduct. Clearly $\beta\alpha = \beta\alpha'$; so β factors uniquely through C by the UMP of the coequalizer. Thus $C = \varinjlim M_\Lambda$, as desired.

Finally, if $F\colon \mathcal{C} \to \mathcal{C}'$ preserves coproducts and coequalizers, then F preserves arbitrary direct limits as F preserves the above construction. □

Theorem **(6.11)**. — *The categories* $((R\text{-mod}))$ *and* $((\text{Sets}))$ *have direct limits.*

PROOF: The assertion follows from **(6.10)** because ((*R*-mod)) and ((Sets)) have coproducts by **(6.7)** and have coequalizers by **(6.8)**. □

THEOREM **(6.12)**. — *Every left adjoint $F\colon \mathcal{C} \to \mathcal{C}'$ preserves direct limits.*

PROOF: Let Λ be a small category, $\lambda \mapsto M_\lambda$ a functor from Λ to $\mathcal{C}$ such that $\varinjlim M_\lambda$ exists. Given an object P' of $\mathcal{C}'$, consider all possible commutative diagrams

$$\begin{array}{ccccc} F(M_\kappa) & \xrightarrow{F(\alpha_\mu^\kappa)} & F(M_\mu) & \xrightarrow{F(\alpha_\mu)} & F(\varinjlim M_\lambda) \\ \downarrow{\scriptstyle \beta'_\kappa} & & \downarrow{\scriptstyle \beta'_\mu} & & \downarrow{\scriptstyle \beta'} \\ P' & \xrightarrow{1} & P' & \xrightarrow{1} & P' \end{array} \tag{6.12.1}$$

where α_μ^κ is any transition map and α_μ is the corresponding insertion. Given the β'_κ, we must show there is a unique β'.

Say F is the left adjoint of $F'\colon \mathcal{C}' \to \mathcal{C}$. Then giving **(6.12.1)** is equivalent to giving this corresponding commutative diagram:

$$\begin{array}{ccccc} M_\kappa & \xrightarrow{\alpha_\mu^\kappa} & M_\mu & \xrightarrow{\alpha_\mu} & \varinjlim M_\lambda \\ \downarrow{\scriptstyle \beta_\kappa} & & \downarrow{\scriptstyle \beta_\mu} & & \downarrow{\scriptstyle \beta} \\ F'(P') & \xrightarrow{1} & F'(P') & \xrightarrow{1} & F'(P') \end{array}$$

However, given the β_κ, there is a unique β by the UMP of $\varinjlim M_\lambda$. □

PROPOSITION **(6.13)**. — *Let $\mathcal{C}$ be a category, Λ and Σ small categories. Assume $\mathcal{C}$ has direct limits indexed by Σ. Then the functor category $\mathcal{C}^\Lambda$ does too.*

PROOF: Let $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$ be a functor from Σ to $\mathcal{C}^\Lambda$. Then a map $\sigma \to \tau$ in Σ yields a natural transformation from $\lambda \to M_{\sigma\lambda}$ to $\lambda \mapsto M_{\tau\lambda}$. So a map $\lambda \mapsto \mu$ in Λ yields a commutative square

$$\begin{array}{ccc} M_{\sigma\lambda} & \to & M_{\sigma\mu} \\ \downarrow & & \downarrow \\ M_{\tau\lambda} & \to & M_{\tau\mu} \end{array} \tag{6.13.1}$$

in a manner compatible with composition in Σ. Hence, with λ fixed, the rule $\sigma \mapsto M_{\sigma\lambda}$ is a functor from Σ to $\mathcal{C}$.

By hypothesis, $\varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda}$ exists. So $\lambda \mapsto \varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda}$ is a functor from Λ to $\mathcal{C}$. Further, as $\tau \in \Sigma$ varies, there are compatible natural transformations from the $\lambda \mapsto M_{\tau\lambda}$ to $\lambda \mapsto \varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda}$. Finally, the latter is the direct limit of the functor $\tau \mapsto (\lambda \mapsto M_{\tau\lambda})$ from Σ to $\mathcal{C}^\Lambda$, because, given any functor $\lambda \mapsto P_\lambda$ from Λ to $\mathcal{C}$ equipped with, for $\tau \in \Sigma$, compatible natural transformations from the $\lambda \mapsto M_{\tau\lambda}$ to $\lambda \mapsto P_\lambda$, there are, for $\lambda \in \Lambda$, compatible unique maps $\varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda} \to P_\lambda$. □

THEOREM **(6.14)** (Direct limits commute). — *Let $\mathcal{C}$ be a category with direct limits indexed by small categories Σ and Λ. Let $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$ be a functor from Σ to $\mathcal{C}^\Lambda$. Then*

$$\varinjlim_{\sigma\in\Sigma} \varinjlim_{\lambda\in\Lambda} M_{\sigma,\lambda} = \varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma} M_{\sigma,\lambda}.$$

PROOF: By **(6.6)**, the functor $\varinjlim_{\lambda\in\Lambda}\colon \mathcal{C}^\Lambda \to \mathcal{C}$ is a left adjoint. By **(6.13)**, the category $\mathcal{C}^\Lambda$ has direct limits indexed by Σ. So **(6.12)** yields the assertion. □

COROLLARY **(6.15)**. — *Let Λ be a small category, R a ring, and $\mathcal{C}$ either* ((Sets)) *or* ((R-mod)). *Then functor* $\varinjlim\colon \mathcal{C}^{\Lambda} \to \mathcal{C}$ *preserves coproducts and coequalizers.*

PROOF: By **(6.7)** and **(6.8)**, both coproducts and coequalizers are special cases of direct limits, and $\mathcal{C}$ has them. So **(6.14)** yields the assertion. □

EXERCISE **(6.16)**. — Let $\mathcal{C}$ be a category, Σ and Λ small categories.

(1) Prove $\mathcal{C}^{\Sigma\times\Lambda} = (\mathcal{C}^{\Lambda})^{\Sigma}$ with $(\sigma,\lambda) \mapsto M_{\sigma,\lambda}$ corresponding to $\sigma \mapsto (\lambda \mapsto M_{\sigma,\lambda})$.

(2) Assume $\mathcal{C}$ has direct limits indexed by Σ and by Λ. Prove that $\mathcal{C}$ has direct limits indexed by $\Sigma \times \Lambda$ and that $\varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma} = \varinjlim_{(\sigma,\lambda)\in\Sigma\times\Lambda}$.

EXERCISE **(6.17)**. — Let $\lambda \mapsto M_\lambda$ and $\lambda \mapsto N_\lambda$ be two functors from a small category Λ to ((R-mod)), and $\{\theta_\lambda\colon M_\lambda \to N_\lambda\}$ a natural transformation. Show

$$\varinjlim \operatorname{Coker}(\theta_\lambda) = \operatorname{Coker}(\varinjlim M_\lambda \to \varinjlim N_\lambda).$$

Show that the analogous statement for kernels can be false by constructing a counterexample using the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \to & \mathbb{Z}/\langle 2\rangle & \to & 0 \\
\downarrow{\scriptstyle \mu_2} & & \downarrow{\scriptstyle \mu_2} & & \downarrow{\scriptstyle \mu_2} & & \\
\mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \to & \mathbb{Z}/\langle 2\rangle & \to & 0
\end{array}$$

7. Filtered Direct Limits

Filtered direct limits are direct limits indexed by a filtered category, which is a more traditional sort of index set. We give an alternative construction of these limits for modules. We conclude that forming them preserves exact sequences, and so commutes with forming the module of homomorphisms out of a fixed finitely presented source. We end by proving that every module is a filtered direct limit of finitely presented modules.

(7.1) (*Filtered categories*). — We call a small category Λ **filtered** if

(1) given objects κ and λ, for some μ there are maps $\kappa \to \mu$ and $\lambda \to \mu$,
(2) given two maps $\sigma, \tau\colon \eta \rightrightarrows \kappa$ with the same source and the same target, for some μ there is a map $\varphi\colon \kappa \to \mu$ such that $\varphi\sigma = \varphi\tau$.

Given a category $\mathcal{C}$, we say a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$ is **filtered** if Λ is filtered. If so, then we say the direct limit $\varinjlim M_\lambda$ is **filtered** if it exists.

For example, let Λ be a partially ordered set. Suppose Λ is **directed**; that is, given $\kappa, \lambda \in \Lambda$, there is a μ with $\kappa \leq \mu$ and $\lambda \leq \mu$. Regard Λ as a category whose objects are its elements and whose sets $\mathrm{Hom}(\kappa, \lambda)$ consist of a single element if $\kappa \leq \lambda$, and are empty if not; morphisms can be composed as the ordering is transitive. Clearly, the category Λ is filtered.

Exercise **(7.2)**. — Let R be a ring, M a module, Λ a set, M_λ a submodule for each $\lambda \in \Lambda$. Assume $\bigcup M_\lambda = M$. Assume, given λ, $\mu \in \Lambda$, there is $\nu \in \Lambda$ such that M_λ, $M_\mu \subset M_\nu$. Order Λ by inclusion: $\lambda \leq \mu$ if $M_\lambda \subset M_\mu$. Prove that $M = \varinjlim M_\lambda$.

Exercise **(7.3)**. — Show that every module M is the filtered direct limit of its finitely generated submodules.

Exercise **(7.4)**. — Show that every direct sum of modules is the filtered direct limit of its finite direct subsums.

Example **(7.5)**. — Let Λ be the set of all positive integers, and for each $n \in \Lambda$, set $M_n := \{r/n \mid r \in \mathbb{Z}\} \subset \mathbb{Q}$. Then $\bigcup M_n = \mathbb{Q}$ and M_m, $M_n \subset M_{mn}$. Then **(7.2)** yields $\mathbb{Q} = \varinjlim M_n$ where Λ is ordered by inclusion of the M_n.

However, $M_m \subset M_n$ if and only if $1/m = s/n$ for some s, if and only if $m \mid n$. Thus we may view Λ as ordered by divisibility of the $n \in \Lambda$.

For each $n \in \Lambda$, set $R_n := \mathbb{Z}$, and define $\beta_n\colon R_n \to M_n$ by $\beta_n(r) := r/n$. Clearly, β_n is a $\mathbb{Z}$-module isomorphism. And if $n = ms$, then this diagram is commutative:

$$\begin{array}{ccc} R_m & \xrightarrow{\mu_s} & R_n \\ {\scriptstyle \beta_m}\downarrow{\scriptstyle \simeq} & & {\scriptstyle \beta_n}\downarrow{\scriptstyle \simeq} \\ M_m & \xrightarrow{\iota_n^m} & M_n \end{array} \tag{7.5.1}$$

where ι_n^m is the inclusion. Hence $\mathbb{Q} = \varinjlim R_n$ where the transition maps are the multiplication maps μ_s.

Exercise **(7.6)**. — Keep the setup of **(7.5)**. For each $n \in \Lambda$, set $N_n := \mathbb{Z}/\langle n \rangle$; if $n = ms$, define $\alpha_n^m\colon N_m \to N_n$ by $\alpha_n^m(x) := xs \pmod n$. Show $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$.

PROPOSITION **(7.7)**. — *Let Λ be a filtered category, R a ring, and $\mathcal{C}$ either* ((Sets)) *or* ((R-mod)) *or* ((R-alg)). *Let $\lambda \mapsto M_\lambda$ be a functor from Λ to $\mathcal{C}$. Define a relation $\sim$ on the disjoint union $\bigsqcup M_\lambda$ as follows: $m_1 \sim m_2$ for $m_i \in M_{\lambda_i}$ if there are transition maps $\alpha_\mu^{\lambda_i}\colon M_{\lambda_i} \to M_\mu$ such that $\alpha_\mu^{\lambda_1} m_1 = \alpha_\mu^{\lambda_2} m_2$. Then $\sim$ is an equivalence relation. Set $M := \bigl(\bigsqcup M_\lambda\bigr)/\!\sim$. Then $M = \varinjlim M_\lambda$, and for each μ, the canonical map $\alpha_\mu\colon M_\mu \to M$ is equal to the insertion map $M_\mu \to \varinjlim M_\lambda$.*

PROOF: Clearly $\sim$ is reflexive and symmetric. Let's show it is transitive. Given $m_i \in M_{\lambda_i}$ for $i = 1, 2, 3$ with $m_1 \sim m_2$ and $m_2 \sim m_3$, there are $\alpha_\mu^{\lambda_i}$ for $i = 1, 2$ and $\alpha_\nu^{\lambda_i}$ for $i = 2, 3$ with $\alpha_\mu^{\lambda_1} m_1 = \alpha_\mu^{\lambda_2} m_2$ and $\alpha_\nu^{\lambda_2} m_2 = \alpha_\nu^{\lambda_3} m_3$. Then **(7.1)**(1) yields α_ρ^μ and α_ρ^ν. Possibly, $\alpha_\rho^\mu \alpha_\mu^{\lambda_2} \neq \alpha_\rho^\nu \alpha_\nu^{\lambda_2}$, but in any case, **(7.1)**(2) yields α_σ^ρ with $\alpha_\sigma^\rho(\alpha_\rho^\mu \alpha_\mu^{\lambda_2}) = \alpha_\sigma^\rho(\alpha_\rho^\nu \alpha_\nu^{\lambda_2})$. Hence, $(\alpha_\sigma^\rho \alpha_\rho^\mu)\alpha_\mu^{\lambda_1} m_1 = (\alpha_\sigma^\rho \alpha_\rho^\nu)\alpha_\nu^{\lambda_3} m_3$. Thus $m_1 \sim m_3$.

If $\mathcal{C} = (($$R$-mod$))$, define addition in M as follows. Given $m_i \in M_{\lambda_i}$ for $i = 1, 2$, there are $\alpha_\mu^{\lambda_i}$ by **(7.1)**(1). Set

$$\alpha_{\lambda_1} m_1 + \alpha_{\lambda_2} m_2 := \alpha_\mu(\alpha_\mu^{\lambda_1} m_1 + \alpha_\mu^{\lambda_2} m_2).$$

We must check that this addition is well defined.

First, consider μ. Suppose there are $\alpha_\nu^{\lambda_i}$ too. Then **(7.1)**(1) yields α_ρ^μ and α_ρ^ν. Possibly, $\alpha_\rho^\mu \alpha_\mu^{\lambda_i} \neq \alpha_\rho^\nu \alpha_\nu^{\lambda_i}$, but **(7.1)**(2) yields α_σ^ρ with $\alpha_\sigma^\rho(\alpha_\rho^\mu \alpha_\mu^{\lambda_1}) = \alpha_\sigma^\rho(\alpha_\rho^\nu \alpha_\nu^{\lambda_1})$ and then α_τ^σ with $\alpha_\tau^\sigma(\alpha_\sigma^\rho \alpha_\rho^\mu \alpha_\mu^{\lambda_2}) = \alpha_\tau^\sigma(\alpha_\sigma^\rho \alpha_\rho^\nu \alpha_\nu^{\lambda_2})$. Therefore,

$$(\alpha_\tau^\sigma \alpha_\sigma^\rho \alpha_\rho^\mu)(\alpha_\mu^{\lambda_1} m_1 + \alpha_\mu^{\lambda_2} m_2) = (\alpha_\tau^\sigma \alpha_\sigma^\rho \alpha_\rho^\nu)(\alpha_\nu^{\lambda_1} m_1 + \alpha_\nu^{\lambda_2} m_2).$$

Thus both μ and ν yield the same value for $\alpha_{\lambda_1} m_1 + \alpha_{\lambda_2} m_2$.

Second, suppose $m_1 \sim m_1' \in M_{\lambda_1'}$. Then a similar, but easier, argument yields $\alpha_{\lambda_1} m_1 + \alpha_{\lambda_2} m_2 = \alpha_{\lambda_1'} m_1' + \alpha_{\lambda_2} m_2$. Thus addition is well defined on M.

Define scalar multiplication on M similarly. Then clearly M is an R-module.

If $\mathcal{C} = (($$R$-alg$))$, then we can see similarly that M is canonically an R-algebra.

Finally, let $\beta_\lambda\colon M_\lambda \to N$ be maps with $\beta_\lambda \alpha_\lambda^\kappa = \beta_\kappa$ for all α_λ^κ. The β_λ induce a map $\bigsqcup M_\lambda \to N$. Suppose $m_1 \sim m_2$ for $m_i \in M_{\lambda_i}$; that is, $\alpha_\mu^{\lambda_1} m_1 = \alpha_\mu^{\lambda_2} m_2$ for some $\alpha_\mu^{\lambda_i}$. Then $\beta_{\lambda_1} m_1 = \beta_{\lambda_2} m_2$ as $\beta_\mu \alpha_\mu^{\lambda_i} = \beta_{\lambda_i}$. So there is a unique map $\beta\colon M \to N$ with $\beta\alpha_\lambda = \beta_\lambda$ for all λ. Further, if $\mathcal{C} = (($$R$-mod$))$ or $\mathcal{C} = (($$R$-alg$))$, then clearly β is a homomorphism. The proof is now complete. □

COROLLARY **(7.8)**. — *Preserve the conditions of* **(7.7)**.

(1) *Given $m \in \varinjlim M_\lambda$, for some λ, there is $m_\lambda \in M_\lambda$ such that $m = \alpha_\lambda m_\lambda$.*

(2) *Given $m_i \in M_{\lambda_i}$ for $i = 1, 2$ such that $\alpha_{\lambda_1} m_1 = \alpha_{\lambda_2} m_2$, there are $\alpha_\mu^{\lambda_i}$ such that $\alpha_\mu^{\lambda_1} m_1 = \alpha_\mu^{\lambda_2} m_2$.*

(3) *Suppose $\mathcal{C} = (($$R$−mod$))$ or $\mathcal{C} = (($$R$−alg$))$. Then given $m_\lambda \in M_\lambda$ such that $\alpha_\lambda m_\lambda = 0$, there is α_μ^λ such that $\alpha_\mu^\lambda m_\lambda = 0$.*

PROOF: The assertions follow immediately from **(7.7)**. □

EXERCISE **(7.9)**. — Let R be a filtered direct limit of rings R_λ. Show $R = 0$ if and only if $R_\lambda = 0$ for some λ. Show R is a domain if R_λ is a domain for every λ.

THEOREM **(7.10)** (Exactness of filtered direct limits). — *Let R be a ring, Λ a filtered category. Let $\mathcal{C}$ be the category of 3-term exact sequences of R-modules: its*

objects are the 3*-term exact sequences, and its maps are the commutative diagrams*

$$\begin{array}{ccccc} L & \longrightarrow & M & \longrightarrow & N \\ \downarrow & & \downarrow & & \downarrow \\ L' & \to & M' & \to & N' \end{array}$$

Then, for any functor $\lambda \mapsto (L_\lambda \xrightarrow{\beta_\lambda} M_\lambda \xrightarrow{\gamma_\lambda} N_\lambda)$ *from* Λ *to* $\mathcal{C}$*, the induced sequence* $\varinjlim L_\lambda \xrightarrow{\beta} \varinjlim M_\lambda \xrightarrow{\gamma} \varinjlim N_\lambda$ *is exact.*

Proof: Abusing notation, in all three cases, denote by α_λ^κ the transition maps and by α_λ the insertions. Then given $\ell \in \varinjlim L_\lambda$, there is $\ell_\lambda \in L_\lambda$ with $\alpha_\lambda \ell_\lambda = \ell$ by **(7.8)**(1). By hypothesis, $\gamma_\lambda \beta_\lambda \ell_\lambda = 0$; so $\gamma\beta\ell = 0$. Thus $\mathrm{Im}(\beta) \subset \mathrm{Ker}(\gamma)$.

For the opposite inclusion, take $m \in \varinjlim M_\lambda$ with $\gamma m = 0$. By **(7.8)**(1), there is $m_\lambda \in M_\lambda$ with $\alpha_\lambda m_\lambda = m$. Now, $\alpha_\lambda \gamma_\lambda m_\lambda = 0$ by commutativity. So by **(7.8)**(3), there is α_μ^λ with $\alpha_\mu^\lambda \gamma_\lambda m_\lambda = 0$. So $\gamma_\mu \alpha_\mu^\lambda m_\lambda = 0$ by commutativity. Hence there is $\ell_\mu \in L_\mu$ with $\beta_\mu \ell_\mu = \alpha_\mu^\lambda m_\lambda$ by exactness. Apply α_μ to get

$$\beta\alpha_\mu\ell_\mu = \alpha_\mu\beta_\mu\ell_\mu = \alpha_\mu\alpha_\mu^\lambda m_\lambda = m.$$

Thus $\mathrm{Ker}(\gamma) \subset \mathrm{Im}(\beta)$. So $\mathrm{Ker}(\gamma) = \mathrm{Im}(\beta)$ as asserted. □

Exercise **(7.11)**. — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, and $N \subset M$ a submodule. For each λ, let $\alpha_\lambda \colon M_\lambda \to M$ be the insertion, and set $N_\lambda := \alpha_\lambda^{-1} N \subset M_\lambda$. Prove that $N = \varinjlim N_\lambda$.

Proposition **(7.12)**. — *Let* Λ *a filtered category,* R *a ring,* $\lambda \mapsto M_\lambda$ *a functor from* Λ *to* $((R\text{-mod}))$*, and* N *an* R*-module. Consider the canonical homomorphism*

$$\theta(N) \colon \varinjlim \mathrm{Hom}(N, M_\lambda) \to \mathrm{Hom}(N, \varinjlim M_\lambda),$$

which is induced by the insertions $M_\lambda \to \varinjlim M_\lambda$*. Then* $\theta(N)$ *is injective if* N *is finitely generated; further,* $\theta(N)$ *is bijective if* N *is finitely presented.*

Proof: If $N := R$, then $\theta(N)$ is bijective by **(4.3)**. Assume N is finitely generated, and take a presentation $R^{\oplus\Sigma} \to R^n \to N \to 0$ with Σ finite if N is finitely presented. It induces the following commutative diagram:

$$\begin{array}{ccccccc} 0 \to & \varinjlim \mathrm{Hom}(N, M_\lambda) & \to & \varinjlim \mathrm{Hom}(R^n, M_\lambda) & \to & \varinjlim \mathrm{Hom}(R^{\oplus\Sigma}, M_\lambda) \\ & {\scriptstyle\theta(N)}\downarrow & & {\scriptstyle\theta(R^n)}\downarrow\simeq & & {\scriptstyle\theta(R^{\oplus\Sigma})}\downarrow \\ 0 \to & \mathrm{Hom}(N, \varinjlim M_\lambda) & \to & \mathrm{Hom}(R^n, \varinjlim M_\lambda) & \to & \mathrm{Hom}(R^{\oplus\Sigma}, \varinjlim M_\lambda) \end{array}$$

The rows are exact owing to **(5.17)**, the left exactness of Hom, and to **(7.10)**, the exactness of filtered direct limits. Now, Hom preserves finite direct sums by **(4.13)**, and direct limit does so by **(6.15)** and **(6.7)**; hence, $\theta(R^n)$ is bijective, and $\theta(R^{\oplus\Sigma})$ is bijective if Σ is finite. A diagram chase yields the assertion. □

Exercise **(7.13)**. — Let Λ and Λ' be small categories, $C \colon \Lambda' \to \Lambda$ a functor. Assume Λ' is filtered. Assume C is **cofinal**; that is,

(1) given $\lambda \in \Lambda$, there is a map $\lambda \to C\lambda'$ for some $\lambda' \in \Lambda'$, and
(2) given $\psi, \varphi \colon \lambda \rightrightarrows C\lambda'$, there is $\chi \colon \lambda' \to \lambda_1'$ with $(C\chi)\psi = (C\chi)\varphi$.

Let $\lambda \mapsto M_\lambda$ be a functor from Λ to $\mathcal{C}$ whose direct limit exists. Show that

$$\varinjlim_{\lambda' \in \Lambda'} M_{C\lambda'} = \varinjlim_{\lambda \in \Lambda} M_\lambda;$$

more precisely, show that the right side has the UMP characterizing the left.

EXERCISE **(7.14)**. — Show that every R-module M is the filtered direct limit over a directed set of finitely presented modules.

8. Tensor Products

Given two modules, their tensor product is the target of the universal bilinear map. We construct the product, and establish various properties: bifunctoriality, commutativity, associativity, cancellation, and most importantly, adjoint associativity; the latter relates the product to the module of homomorphisms. With one factor fixed, the product becomes a linear functor. We prove Watt's Theorem; it characterizes "tensor-product" functors as those linear functors that commute with direct sums and cokernels. Lastly, we discuss the tensor product of algebras.

(8.1) (*Bilinear maps*). — Let R a ring, and M, N, P modules. We call a map

$$\alpha\colon M \times N \to P$$

bilinear if it is linear in each variable; that is, given $m \in M$ and $n \in N$, the maps

$$m' \mapsto \alpha(m', n) \quad \text{and} \quad n' \mapsto \alpha(m, n')$$

are R-linear. Denote the set of all these maps by $\mathrm{Bil}_R(M, N; P)$. It is clearly an R-module, with sum and scalar multiplication performed valuewise.

(8.2) (*Tensor product*). — Let R be a ring, and M, N modules. Their **tensor product**, denoted $M \otimes_R N$ or simply $M \otimes N$, is constructed as the quotient of the free module $R^{\oplus(M\times N)}$ modulo the submodule generated by the following elements, where (m, n) stands for the standard basis element $e_{(m,n)}$:

$$\begin{gathered}(m + m',\, n) - (m,\, n) - (m',\, n) \quad \text{and} \quad (m,\, n + n') - (m, n) - (m, n'),\\ (xm,\, n) - x(m, n) \quad \text{and} \quad (m,\, xn) - x(m, n)\end{gathered} \tag{8.2.1}$$

for all $m, m' \in M$ and $n, n' \in N$ and $x \in R$.

Note that $M \otimes N$ is the target of the canonical map with source $M \times N$

$$\beta\colon M \times N \to M \otimes N,$$

which sends each (m, n) to its residue class $m \otimes n$. By construction, β is bilinear.

Theorem **(8.3)** (UMP of tensor product). — *Let R be a ring, M, N modules. Then $\beta\colon M \times N \to M \otimes N$ is the universal example of a bilinear map with source $M \times N$; in fact, β induces, not simply a bijection, but a module isomorphism,*

$$\theta\colon \mathrm{Hom}_R(M \otimes_R N, P) \xrightarrow{\sim} \mathrm{Bil}_R(M, N; P). \tag{8.3.1}$$

Proof: Note that, if we follow any bilinear map with any linear map, then the result is bilinear; hence, θ is well defined. Clearly, θ is a module homomorphism. Further, θ is injective since $M \otimes_R N$ is generated by the image of β. Finally, given any bilinear map $\alpha\colon M\times N \to P$, by **(4.10)** it extends to a map $\alpha'\colon R^{\oplus(M\times N)} \to P$, and α' carries all the elements in **(8.2.1)** to 0; hence, α' factors through β. Thus θ is also surjective, so an isomorphism, as asserted. □

(8.4) (*Bifunctoriality*). — Let R be a ring, $\alpha\colon M \to M'$ and $\alpha'\colon N \to N'$ module homomorphisms. Then there is a canonical commutative diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{\alpha\times\alpha'} & M' \times N' \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\beta'} \\ M \otimes N & \xrightarrow{\alpha\otimes\alpha'} & M' \otimes N' \end{array}$$

Indeed, $\beta' \circ (\alpha \times \alpha')$ is clearly bilinear; so the UMP **(8.3)** yields $\alpha \otimes \alpha'$. Thus $\bullet \otimes N$ and $M \otimes \bullet$ are commuting **linear** functors, that is, linear on maps (see **(9.2)**).

PROPOSITION **(8.5)**. — *Let R be a ring, M and N modules.*

(1) *Then the switch map $M \times N \to N \times M$ induces an isomorphism*

$$M \otimes_R N = N \otimes_R M. \qquad \textbf{((commutative law))}$$

(2) *Then multiplication of R on M induces an isomorphism*

$$R \otimes_R M = M. \qquad \textbf{((unitary law))}$$

PROOF: The switch map induces an isomorphism $R^{\oplus(M\times N)} \xrightarrow{\sim} R^{\oplus(N\times M)}$, and it preserves the elements of **(8.2.1)**. Thus (1) holds.

Define $\beta\colon R \times M \to M$ by $\beta(x, m) := xm$. Clearly β is bilinear. Let's check β has the requisite UMP. Given a bilinear map $\alpha\colon R \times M \to P$, define $\gamma\colon M \to P$ by $\gamma(m) := \alpha(1, m)$. Then γ is linear as α is bilinear. Also, $\alpha = \gamma\beta$ as

$$\alpha(x, m) = x\alpha(1, m) = \alpha(1, xm) = \gamma(xm) = \gamma\beta(x, m).$$

Further, γ is unique as β is surjective. Thus the UMP holds, so (2) does too. □

EXERCISE **(8.6)**. — Let R be a domain, $\mathfrak{a}$ a nonzero ideal. Set $K := \mathrm{Frac}(R)$. Show that $\mathfrak{a} \otimes_R K = K$.

(8.7) (*Bimodules*). — Let R and R' be rings. An abelian group N is an (R, R')-**bimodule** if it is both an R-module and an R'-module and if $x(x'n) = x'(xn)$ for all $x \in R$, all $x' \in R'$, and all $n \in N$. At times, we think of N as a left R-module, with multiplication xn, and as a right R'-module, with multiplication nx'. Then the compatibility condition becomes the associative law: $x(nx') = (xn)x'$. A (R, R')-**homomorphism** of bimodules is a map that is both R-linear and R'-linear.

Let M be an R-module, and let N be an (R, R')-bimodule. Then $M \otimes_R N$ is an (R, R')-bimodule with R-structure as usual and with R'-structure defined by $x'(m \otimes n) := m \otimes (x'n)$ for all $x' \in R'$, all $m \in M$, and all $n \in N$. The latter multiplication is well defined and the two multiplications commute because of bifunctoriality **(8.4)** with $\alpha := \mu_x$ and $\alpha' := \mu_{x'}$.

For instance, suppose R' is an R-algebra. Then R' is an (R, R')-bimodule. So $M \otimes_R R'$ is an R'-module. It is said to be obtained by **extension of scalars**.

EXERCISE **(8.8)**. — Let R be a ring, R' an R-algebra, M, N two R'-modules. Show there is a canonical R-linear map $\tau\colon M \otimes_R N \to M \otimes_{R'} N$.

Let $K \subset M \otimes_R N$ denote the R-submodule generated by all the differences $(x'm) \otimes n - m \otimes (x'n)$ for $x' \in R'$ and $m \in M$ and $n \in N$. Show $K = \mathrm{Ker}(\tau)$. Show τ is surjective, and is an isomorphism if R' is a quotient of R.

THEOREM **(8.9)**. — *Let R and R' be rings, M an R-module, P an R'-module, N an (R, R')-bimodule, . Then there are two canonical (R, R')-isomorphisms:*

$$M \otimes_R (N \otimes_{R'} P) = (M \otimes_R N) \otimes_{R'} P, \qquad \textbf{((associative law))}$$

$$\mathrm{Hom}_{R'}(M \otimes_R N,\, P) = \mathrm{Hom}_R\big(M,\, \mathrm{Hom}_{R'}(N, P)\big). \qquad \textbf{((adjoint associativity))}$$

PROOF: Note that $M \otimes_R (N \otimes_{R'} P)$ and $(M \otimes_R N) \otimes_{R'} P$ are (R, R')-bimodules. For each (R, R')-bimodule Q, call a map $\tau\colon M \times N \times P \to Q$ **trilinear** if it is R-bilinear in $M \times N$ and R'-bilinear in $N \times P$. Denote the set of all these τ by $\mathrm{Tril}(M, N, P;\ Q)$. It is, clearly, an (R, R')-bimodule.

A trilinear map τ yields an R-bilinear map $M \times (N \otimes_{R'} P) \to Q$, whence a map $M \otimes_R (N \otimes_{R'} P) \to Q$, which is both R-linear and R'-linear, and *vice versa*. Thus

$$\mathrm{Tril}_{(R,R')}(M,N,P;\,Q) = \mathrm{Hom}\big(M \otimes_R (N \otimes_{R'} P),\, Q\big).$$

Similarly, there is a canonical isomorphism of (R,R')-bimodules

$$\mathrm{Tril}_{(R,R')}(M,N,P;\,Q) = \mathrm{Hom}\big((M \otimes_R N) \otimes_{R'} P,\, Q\big).$$

Hence both $M \otimes_R (N \otimes_{R'} P)$ and $(M \otimes_R N) \otimes_{R'} P$ are universal examples of a target of a trilinear map with source $M \times N \times P$. Thus they are equal, as asserted.

To establish the isomorphism of adjoint associativity, define a map

$$\alpha\colon \mathrm{Hom}_{R'}(M \otimes_R N, P) \to \mathrm{Hom}_R\big(M,\, \mathrm{Hom}_{R'}(N,P)\big) \quad \text{by}$$
$$\big(\alpha(\gamma)(m)\big)(n) := \gamma(m \otimes n).$$

Let's check α is well defined. First, $\alpha(\gamma)(m)$ is R'-linear, because given $x' \in R'$,

$$\gamma(m \otimes (x'n)) = \gamma(x'(m \otimes n)) = x'\gamma(m \otimes n)$$

since γ is R'-linear. Further, $\alpha(\gamma)$ is R-linear, because given $x \in R$,

$$(xm) \otimes n = m \otimes (xn) \quad \text{and so} \quad \big(\alpha(\gamma)(xm)\big)(n) = \big(\alpha(\gamma)(m)\big)(xn).$$

Thus $\alpha(\gamma) \in \mathrm{Hom}_R\big(M,\, \mathrm{Hom}_{R'}(N,P)\big)$. Clearly, α is an (R,R')-homomorphism.

To obtain an inverse to α, given $\eta \in \mathrm{Hom}_R\big(M,\, \mathrm{Hom}_{R'}(N,P)\big)$, define a map $\zeta\colon M \times N \to P$ by $\zeta(m,n) := (\eta(m))(n)$. Clearly, ζ is $\mathbb{Z}$-bilinear, so ζ induces a $\mathbb{Z}$-linear map $\delta\colon M \otimes_{\mathbb{Z}} N \to P$. Given $x \in R$, clearly $(\eta(xm))(n) = (\eta(m))(xn)$; so $\delta((xm) \otimes n) = \delta(m \otimes (xn))$. Hence, δ induces a $\mathbb{Z}$-linear map $\beta(\eta)\colon M \otimes_R N \to P$ owing to **(8.8)** with $\mathbb{Z}$ for R and with R for R'. Clearly, $\beta(\eta)$ is R'-linear as $\eta(m)$ is so. Finally, it is easy to verify that $\alpha(\beta(\eta)) = \eta$ and $\beta(\alpha(\gamma)) = \gamma$, as desired. □

Corollary **(8.10)**. — *Let R and R' be rings, M an R-module, P an R'-module. If R' is an R-algebra, then there are two canonical (R,R')-isomorphisms:*

$$(M \otimes_R R') \otimes_{R'} P = M \otimes_R P, \qquad \textbf{((cancellation law))}$$
$$\mathrm{Hom}_{R'}(M \otimes_R R', P) = \mathrm{Hom}_R(M,P). \qquad \textbf{((left adjoint))}$$

Instead, if R is an R'-algebra, then there is another canonical (R,R')-isomorphism:

$$\mathrm{Hom}_{R'}(M,P) = \mathrm{Hom}_R(M,\, \mathrm{Hom}_{R'}(R,P)). \qquad \textbf{((right adjoint))}$$

In other words, $\bullet \otimes_R R'$ is the left adjoint of restriction of scalars from R' to R, and $\mathrm{Hom}_{R'}(R,\bullet)$ is the right adjoint of restriction of scalars from R to R'.

Proof: The cancellation law results from the associative and unitary laws; the adjoint isomorphisms, from adjoint associativity, **(4.3)** and the unitary law. □

Corollary **(8.11)**. — *Let R, R' be rings, N a bimodule. Then the functor $\bullet \otimes_R N$ preserves direct limits, or equivalently, direct sums and cokernels.*

Proof: By adjoint associativity, $\bullet \otimes_R N$ is the left adjoint of $\mathrm{Hom}_{R'}(N,\bullet)$. Thus the assertion results from **(6.12)** and from **(6.7)** and **(6.8)**. □

Example **(8.12)**. — Tensor product does not preserve kernels, nor even injections. Indeed, consider the injection $\mu_2\colon \mathbb{Z} \to \mathbb{Z}$. Tensor it with $N := \mathbb{Z}/\langle 2\rangle$, obtaining $\mu_2\colon N \to N$. This map is zero, but not injective as $N \neq 0$.

EXERCISE **(8.13)**. — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module.
(1) Use **(8.11)** to show that $(R/\mathfrak{a}) \otimes M = M/\mathfrak{a}M$.
(2) Use (1) to show that $(R/\mathfrak{a}) \otimes (R/\mathfrak{b}) = R/(\mathfrak{a}+\mathfrak{b})$.

EXERCISE **(8.14)**. — Let k be a field, M and N nonzero vector spaces. Prove that $M \otimes N \neq 0$.

THEOREM **(8.15)** (Watts). — *Let $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a linear functor. Then there is a natural transformation $\theta(\bullet)\colon \bullet \otimes F(R) \to F(\bullet)$ with $\theta(R) = 1$, and $\theta(\bullet)$ is an isomorphism if and only if F preserves direct sums and cokernels.*

PROOF: As F is a linear functor, there is, by definition, a natural R-linear map $\theta(M)\colon \mathrm{Hom}(R, M) \to \mathrm{Hom}(F(R), F(M))$. But $\mathrm{Hom}(R, M) = M$ by **(4.3)**. Set $N := F(R)$. Then, with $P := F(M)$, adjoint associativity yields the desired map

$$\theta(M) \in \mathrm{Hom}\big(M, \mathrm{Hom}(N, F(M))\big) = \mathrm{Hom}(M \otimes N, F(M)).$$

Explicitly, $\theta(M)(m \otimes n) = F(\rho)(n)$ where $\rho\colon R \to M$ is defined by $\rho(1) = m$. Alternatively, this formula can be used to construct $\theta(M)$, as $(m, n) \mapsto F(\rho)(n)$ is clearly bilinear. Either way, it is not hard to see that $\theta(M)$ is natural in M.

If $\theta(\bullet)$ is an isomorphism, then F preserves direct sums and cokernels by **(8.11)**.

To prove the converse, take a presentation $R^{\oplus\Lambda} \xrightarrow{\beta} R^{\oplus\Sigma} \xrightarrow{\alpha} M \to 0$; one exists by **(5.19)**. Applying θ, we get this commutative diagram:

$$\begin{array}{ccccccc} R^{\oplus\Lambda} \otimes N & \longrightarrow & R^{\oplus\Sigma} \otimes N & \longrightarrow & M \otimes N & \longrightarrow & 0 \\ \downarrow{\scriptstyle \theta(R^{\oplus\Lambda})} & & \downarrow{\scriptstyle \theta(R^{\oplus\Sigma})} & & \downarrow{\scriptstyle \theta(M)} & & \\ F(R^{\oplus\Lambda}) & \longrightarrow & F(R^{\oplus\Sigma}) & \longrightarrow & F(M) & \longrightarrow & 0 \end{array} \qquad \textbf{(8.15.1)}$$

By construction, $\theta(R) = 1_N$. If F preserves direct sums, then $\theta(R^{\oplus\Lambda}) = 1_{N^{\oplus\Lambda}}$ and $\theta(R^{\oplus\Sigma}) = 1_{N^{\oplus\Sigma}}$; in fact, given any natural transformation $\theta\colon T \to U$ of linear functors, let's show that, if T and U preserve direct sums, then so does θ.

Given a collection of modules M_λ, each inclusion $\iota_\lambda\colon M_\lambda \to \bigoplus M_\lambda$ yields, because of naturality, the following commutative diagram:

$$\begin{array}{ccc} T(M_\lambda) & \xrightarrow{T(\iota_\lambda)} & \bigoplus T(M_\lambda) \\ \downarrow{\scriptstyle \theta(M_\lambda)} & & \downarrow{\scriptstyle \theta(\bigoplus M_\lambda)} \\ U(M_\lambda) & \xrightarrow{U(\iota_\lambda)} & \bigoplus U(M_\lambda) \end{array}$$

Hence $\theta(\bigoplus M_\lambda)T(\iota_\lambda) = \bigoplus \theta(M_\lambda)T(\iota_\lambda)$. But the UMP of direct sum says that, given any N, a map $\bigoplus T(M_\lambda) \to N$ is determined by its compositions with the inclusions $T(\iota_\lambda)$. Thus $\theta(\bigoplus M_\lambda) = \bigoplus \theta(M_\lambda)$, as desired.

Suppose F preserves cokernels. Since $\bullet \otimes N$ does too, the rows of **(8.15.1)** are exact by **(5.3)**. Therefore, $\theta(M)$ is an isomorphism. □

EXERCISE **(8.16)**. — Let $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a linear functor. Show that F always preserves finite direct sums. Show that $\theta(M)\colon M \otimes F(R) \to F(M)$ is surjective if F preserves surjections and M is finitely generated, and that $\theta(M)$ is an isomorphism if F preserves cokernels and M is finitely presented.

LEMMA **(8.17)** (Equational Criterion for Vanishing). — *Let R be a ring, M and N modules, and $\{n_\lambda\}_{\lambda\in\Lambda}$ a set of generators of N. Then any element of $M \otimes N$ can be written as a finite sum $\sum m_\lambda \otimes n_\lambda$ with $m_\lambda \in M$. Further, $\sum m_\lambda \otimes n_\lambda = 0$*

if and only if there are $m_\sigma \in M$ and $x_{\lambda\sigma} \in R$ for $\sigma \in \Sigma$ for some Σ such that

$$\textstyle\sum_\sigma x_{\lambda\sigma} m_\sigma = m_\lambda \text{ for all } \lambda \text{ and } \sum_\lambda x_{\lambda\sigma} n_\lambda = 0 \text{ for all } \sigma.$$

PROOF: By **(8.2)**, $M \otimes N$ is generated by elements of the form $m \otimes n$ with $m \in M$ and $n \in N$, and if $n = \sum x_\lambda n_\lambda$ with $x_\lambda \in R$, then $m \otimes n = \sum (x_\lambda m) \otimes n_\lambda$. Thus any element of $M \otimes N$ has the asserted form $\sum m_\lambda \otimes n_\lambda$.

Assume the m_σ and the $x_{\lambda\sigma}$ exist. Then

$$\textstyle\sum m_\lambda \otimes n_\lambda = \sum_\lambda \big(\sum_\sigma x_{\lambda\sigma} m_\sigma\big) \otimes n_\lambda = \sum_\sigma \big(m_\sigma \otimes \sum_\lambda x_{\lambda\sigma} n_\lambda\big) = 0.$$

Conversely, by **(5.19)**, there is a presentation $R^{\oplus\Sigma} \xrightarrow{\beta} R^{\oplus\Lambda} \xrightarrow{\alpha} N \to 0$ with $\alpha(e_\lambda) = n_\lambda$ for all λ where $\{e_\lambda\}$ is the standard basis of $R^{\oplus\Lambda}$. Then by **(8.11)** the following sequence is exact:

$$M \otimes R^{\oplus\Sigma} \xrightarrow{1\otimes\beta} M \otimes R^{\oplus\Lambda} \xrightarrow{1\otimes\alpha} M \otimes N \to 0.$$

Further, $(1 \otimes \alpha)\big(\sum m_\lambda \otimes e_\lambda\big) = 0$. So the exactness implies there is an element $s \in M \otimes R^{\oplus\Sigma}$ such that $(1 \otimes \beta)(s) = \sum m_\lambda \otimes e_\lambda$. Let $\{e_\sigma\}$ be the standard basis of $R^{\oplus\Sigma}$, and write $s = \sum m_\sigma \otimes e_\sigma$ with $m_\sigma \in M$. Write $\beta(e_\sigma) = \sum_\lambda x_{\lambda\sigma} e_\lambda$. Then clearly $0 = \alpha\beta(e_\sigma) = \sum_\lambda x_{\lambda\sigma} n_\lambda$, and

$$\textstyle 0 = \sum_\lambda m_\lambda \otimes e_\lambda - \sum_\sigma m_\sigma \otimes \big(\sum_\lambda x_{\lambda\sigma} e_\lambda\big) = \sum_\lambda \big(m_\lambda - \sum_\sigma x_{\lambda\sigma} m_\sigma\big) \otimes e_\lambda.$$

Since the e_λ are independent, $m_\lambda = \sum_\sigma x_{\lambda\sigma} m_\sigma$, as asserted. □

(8.18) (*Algebras*). — Let R be a ring, S and T algebras with structure maps $\sigma\colon R \to S$ and $\tau\colon R \to T$. Set $U := S \otimes_R T$; it is an R-module. Now, define $S \times T \times S \times T \to U$ by $(s, t, s', t') \mapsto ss' \otimes tt'$. This map is clearly linear in each factor. So it induces a bilinear map

$$\mu\colon U \times U \to U \quad \text{with} \quad \mu(s \otimes t,\, s' \otimes t') = (ss' \otimes tt').$$

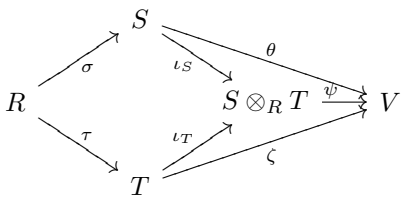
It is easy to check that U is a ring with μ as product. In fact, U is an R-algebra with structure map ω given by $\omega(r) := \sigma(r) \otimes 1 = 1 \otimes \tau(r)$, called the **tensor product** of S and T over R.

Define $\iota_S\colon S \to S \otimes_R T$ by $\iota_S(s) := s \otimes 1$. Clearly ι_S is an R-algebra homomorphism. Define $\iota_T\colon T \to S \otimes T$ similarly. Given an R-algebra V, define a map

$$\gamma\colon \operatorname{Hom}_{((R\text{-alg}))}(S \otimes_R T,\, V) \to \operatorname{Hom}_{((R\text{-alg}))}(S,\, V) \times \operatorname{Hom}_{((R\text{-alg}))}(T,\, V).$$

by $\gamma(\psi) := (\psi\iota_S,\, \psi\iota_T)$. Conversely, given R-algebra homomorphisms $\theta\colon S \to V$ and $\zeta\colon T \to V$, define $\eta\colon S \times T \to V$ by $\eta(s, t) := \theta(s) \cdot \zeta(t)$. Then η is clearly bilinear, so it defines a linear map $\psi\colon S \otimes_R T \to V$. It is easy to see that the map $(\theta, \zeta) \mapsto \psi$ is an inverse to γ. Thus γ is bijective.

In other words, $S \otimes_R T$ is the **coproduct** of S and T in $((R\text{-alg}))$:



EXAMPLE **(8.19)**. — Let R be a ring, S an algebra, and $X_1, \dots, X_n$ variables. Then there is a canonical S-algebra isomorphism

$$S \otimes_R R[X_1, \dots, X_n] = S[X_1, \dots, X_n].$$

Indeed, given an S-algebra homomorphism $S \to T$ and elements $x_1, \dots, x_n$ of T, there is an R-algebra homomorphism $R[X_1, \dots, X_n] \to T$ by **(1.2)**. So by **(8.18)**, there is a unique S-algebra homomorphism $S \otimes_R R[X_1, \dots, X_n] \to T$. Thus both $S \otimes_R R[X_1, \dots, X_n] \to T$ and $S[X_1, \dots X_n]$ possess the same UMP.

In particular, for variables $Y_1, \dots, Y_m$, we obtain

$$R[X_1, \dots, X_n] \otimes_R R[Y_1, \dots, Y_m] = R[X_1, \dots, X_n, Y_1, \dots, Y_m].$$

EXERCISE **(8.20)**. — Let X be a variable, ω a complex cubic root of 1, and $\sqrt[3]{2}$ the real cube root of 2. Set $k := \mathbb{Q}(\omega)$ and $K := k[\sqrt[3]{2}]$. Show $K = k[X]/\langle X^3 - 2\rangle$ and then $K \otimes_k K = K \times K \times K$.

9. Flatness

A module is called flat if tensor product with it is an exact functor. First, we study exact functors in general. Then we prove various properties of flat modules. Notably, we prove Lazard's Theorem, which characterizes the flat modules as the filtered direct limits of free modules of finite rank. Lazard's Theorem yields the Ideal Criterion for Flatness, which characterizes the flat modules as those whose tensor product with any finitely generated ideal is equal to the ordinary product.

LEMMA **(9.1)**. — *Let R be a ring, $\alpha\colon M \to N$ a homomorphism of modules. Then there is a diagram with two short exact sequences involving N'*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \xrightarrow{\alpha} & N & \longrightarrow & P & \longrightarrow & 0 \\ & & & & & \searrow^{\alpha'} \quad \nearrow_{\alpha''} & & & & & \\ & & & & & 0 \longrightarrow N' \longrightarrow 0 & & & & & \end{array} \tag{9.1.1}$$

if and only if $M' = \operatorname{Ker}(\alpha)$ and $N' = \operatorname{Im}(\alpha)$ and $P = \operatorname{Coker}(\alpha)$.

PROOF: The equations yield the diagram since $\operatorname{Coim}(\alpha) \xrightarrow{\sim} \operatorname{Im}(\alpha)$ by **(4.9)**.

Conversely, given the diagram, note that $\operatorname{Ker}(\alpha) = \operatorname{Ker}(\alpha')$ since α'' is injective. So $M' = \operatorname{Ker}(\alpha)$. So $N' = \operatorname{Coim}(\alpha)$ since α' is surjective. Hence $N' = \operatorname{Im}(\alpha)$. Therefore, $P = \operatorname{Coker}(\alpha)$. Thus the equations hold. □

(9.2) (*Exact Functors*). — Let R be a ring, R' an algebra, F a functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Assume F is **R-linear**; that is, the associated map

$$\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{R'}(FM, FN)$$

is R-linear. Then, if a map $\alpha\colon M \to N$ is 0, so is $F\alpha\colon FM \to FN$. But $M = 0$ if and only if $1_M = 0$. Further, $F(1_M) = 1_{FM}$. Thus if $M = 0$, then $FM = 0$.

We call F **exact** if it preserves exact sequences. For example, $\operatorname{Hom}(P, \bullet)$ is exact if and only if P is projective by **(5.22)**.

We call F **left exact** if it preserves kernels. When F is contravariant, we call F **left exact** if it takes cokernels to kernels. For example, $\operatorname{Hom}(N, \bullet)$ and $\operatorname{Hom}(\bullet, N)$ are left exact covariant and contravariant functors.

We call F **right exact** if it preserves cokernels. For example, $M \otimes \bullet$ is right exact.

PROPOSITION **(9.3)**. — *Let R be a ring, R' an algebra, F an R-linear functor. Then the following conditions are equivalent:*

(1) *F preserves exact sequences; that is, F is exact.*
(2) *F preserves short exact sequences.*
(3) *F preserves kernels and surjections.*
(4) *F preserves cokernels and injections.*
(5) *F preserves kernels and images.*

PROOF: Trivially, (1) implies (2). In view of **(5.3)**, clearly (1) yields (3) and (4).

Assume (3). Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Since F preserves kernels, $0 \to FM' \to FM \to FM''$ is exact; since F preserves surjections, $FM \to FM'' \to 0$ is also exact. Thus (2) holds. Similarly, (4) implies (2).

Assume (2). Given $\alpha\colon M \to N$, form the diagram **(9.1.1)**. Applying F to it and

using (2), we obtain a similar diagram for $F(\alpha)$. Hence **(9.1)** yields (5).

Finally, assume (5). Let $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ be exact; that is, $\mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$. Now, (5) yields $\mathrm{Ker}(F(\beta)) = F(\mathrm{Ker}(\beta))$ and $\mathrm{Im}(F(\alpha)) = F(\mathrm{Im}(\alpha))$. Therefore, $\mathrm{Ker}(F(\beta)) = \mathrm{Im}(F(\alpha))$. Thus (1) holds. □

(9.4) (*Flatness*). — An R-module M is said to be **flat** over R or R-**flat** if the functor $M \otimes_R \bullet$ preserves injections. It is equivalent by **(9.3)** that $M \otimes_R \bullet$ be exact since it is right exact.

Lemma **(9.5)**. — *A direct sum $\bigoplus M_\lambda$ is flat if and only if each summand is flat.*

Proof: Let $\beta\colon N' \to N$ be an injective map. Then **(8.11)** yields

$$\big(\bigoplus M_\lambda\big) \otimes \beta = \bigoplus (M_\lambda \otimes \beta);$$

see the end of the proof of **(8.15)**, taking $T(M) := M \otimes N'$ and $U(M) := M \otimes N$. Now, the map on the right is injective if and only if each summand $M_\lambda \otimes \beta$ is injective by **(5.2)**. The assertion follows. □

Proposition **(9.6)**. — *A free module is flat; in fact, a projective module is flat.*

Proof: The unitary law implies that R is flat over R. Hence a free module is flat by **(9.5)**. Finally, a projective module is a direct summand of a free module by **(5.22)**, and therefore flat by **(9.5)**. □

Exercise **(9.7)**. — Let R be a ring, R' a flat algebra, and P a flat R'-module. Show that P is a flat R-module.

Exercise **(9.8)**. — Let R be a ring, M a flat module, and R' an algebra. Show that $M \otimes_R R'$ is a flat R'-module.

Exercise **(9.9)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume that $R/\mathfrak{a}$ is R-flat. Show that $\mathfrak{a} = \mathfrak{a}^2$.

Proposition **(9.10)**. — *Let R be a ring, $0 \to M' \to M \to M'' \to 0$ an exact sequence of modules. Assume M'' is flat.*

(1) *Then $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact for any module N.*

(2) *Then M is flat if and only if M' is flat.*

Proof: By **(5.19)**, there is an exact sequence $0 \to K \to R^{\oplus\Lambda} \to N \to 0$. Tensor it with the given sequence to obtain the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & M' \otimes K & \longrightarrow & M \otimes K & \longrightarrow & M'' \otimes K & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \alpha} & & \\
0 & \to & M' \otimes R^{\oplus\Lambda} & \xrightarrow{\beta} & M \otimes R^{\oplus\Lambda} & \to & M'' \otimes R^{\oplus\Lambda} & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & M' \otimes N & \xrightarrow{\gamma} & M \otimes N & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Here α and β are injective by Definition **(9.4)**, as M'' and $R^{\oplus\Lambda}$ are flat by hypothesis

and by **(9.6)**. So the rows and columns are exact, as tensor product is right exact. Finally, the Snake Lemma, **(5.12)**, implies γ is injective. Thus (1) holds.

To prove (2), take an injection $\beta\colon N' \to N$, and form this commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M'\otimes N' & \longrightarrow & M\otimes N' & \longrightarrow & M''\otimes N' & \longrightarrow & 0 \\ & & {\scriptstyle\alpha'}\downarrow & & {\scriptstyle\alpha}\downarrow & & {\scriptstyle\alpha''}\downarrow & & \\ 0 & \longrightarrow & M'\otimes N & \longrightarrow & M\otimes N & \longrightarrow & M''\otimes N & \longrightarrow & 0 \end{array}$$

Its rows are exact by (1).

Assume M is flat. Then α is injective. Hence α' is too. Thus M' is flat.

Conversely, assume M' is flat. Then α' is injective. But α'' is injective as M'' is flat. Hence α is injective by the Snake lemma. Thus M is flat. Thus (2) holds. □

Proposition **(9.11)**. — *A filtered direct limit of flat modules $\varinjlim M_\lambda$ is flat.*

Proof: Let $\beta\colon N' \to N$ be injective. Then $M_\lambda \otimes \beta$ is injective for each λ since M_λ is flat. So $\varinjlim(M_\lambda \otimes \beta)$ is injective by the exactness of filtered direct limits, **(7.10)**. So $(\varinjlim M_\lambda)\otimes\beta$ is injective by **(8.11)**. Thus $\varinjlim M_\lambda$ is flat. □

Proposition **(9.12)**. — *Let R and R' be rings, M an R-module, N an (R,R')-bimodule, and P an R'-module. Then there is a canonical homomorphism*

$$\theta\colon \operatorname{Hom}_R(M,\,N)\otimes_{R'} P \to \operatorname{Hom}_R(M,\,N\otimes_{R'} P). \qquad \textbf{(9.12.1)}$$

Assume P is flat. If M is finitely generated, then θ is injective; if M is finitely presented, then θ is an isomorphism.

Proof: The map θ exists by Watts's Theorem, **(8.15)**, with R' for R, applied to $\operatorname{Hom}_R(M, N\otimes_{R'}\bullet)$. Explicitly, $\theta(\varphi\otimes p)(m) = \varphi(m)\otimes p$. Alternatively, this formula can be used to construct θ, as $(\varphi, n)\mapsto\psi$, where $\psi(m) := \varphi(m)\otimes p$, is clearly bilinear.

Clearly, θ is bijective if $M = R$. So θ is bijective if $M = R^n$ for any n, as $\operatorname{Hom}_R(\bullet, Q)$ preserves finite direct sums for any Q by **(4.13)**.

Assume that M is finitely generated. Then from **(5.19)**, we obtain a presentation $R^{\oplus\Lambda}\to R^n\to M\to 0$, with Λ finite if P is finitely presented. Since θ is natural, it yields this commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Hom}_R(M,N)\otimes_{R'} P & \longrightarrow & \operatorname{Hom}_R(R^n,N)\otimes_{R'} P & \longrightarrow & \operatorname{Hom}_R(R^{\oplus\Lambda},N)\otimes_{R'} P \\ & & {\scriptstyle\theta}\downarrow & & {\scriptstyle\simeq}\downarrow & & \downarrow \\ 0 & \longrightarrow & \operatorname{Hom}_R(M,N\otimes_{R'} P) & \longrightarrow & \operatorname{Hom}_R(R^n,N\otimes_{R'} P) & \longrightarrow & \operatorname{Hom}_R(R^{\oplus\Lambda},\,N\otimes_{R'} P) \end{array}$$

Its rows are exact owing to the left exactness of Hom and to the flatness of P. The right-hand vertical map is bijective if Λ is finite. The assertion follows. □

Exercise **(9.13)**. — Let R be a ring, R' an algebra, M and N modules. Show that there is a canonical map

$$\sigma\colon \operatorname{Hom}_R(M,\,N)\otimes_R R' \to \operatorname{Hom}_{R'}(M\otimes_R R',\,N\otimes_R R').$$

Assume R' is flat over R. Show that if M is finitely generated, then σ is injective, and that if M is finitely presented, then σ is an isomorphism.

Definition **(9.14)**. — Let R be a ring, M a module. Let Λ_M be the category whose objects are the pairs (R^m,α) where $\alpha\colon R^m\to M$ is a homomorphism, and whose maps $(R^m,\alpha)\to(R^n,\beta)$ are the homomorphisms $\varphi\colon R^m\to R^n$ with $\beta\varphi=\alpha$.

PROPOSITION **(9.15)**. — *Let R be a ring, M a module, and $(R^m, \alpha) \mapsto R^m$ the forgetful functor from Λ_M to $((R\text{-mod}))$. Then $M = \varinjlim_{(R^m,\alpha)\in\Lambda_M} R^m$.*

PROOF: By the UMP, the $\alpha\colon R^m \to M$ induce a map $\zeta\colon \varinjlim R^m \to M$. Let's show ζ is bijective. First, ζ is surjective, because each $x \in M$ is in the image of (R, α_x) where $\alpha_x(r) := rx$.

For injectivity, let $y \in \mathrm{Ker}(\zeta)$. By construction, $\bigoplus_{(R^m,\alpha)} R^m \to \varinjlim R^m$ is surjective; see the proof of **(6.10)**. So y is in the image of some finite sum $\bigoplus_{(R^{m_i},\,\alpha_i)} R^{m_i}$. Set $m := \sum m_i$. Then $\bigoplus R^{m_i} = R^m$. Set $\alpha := \sum \alpha_i$. Then y is the image of some $y' \in R^m$ under the insertion $\iota_m\colon R^m \to \varinjlim R^m$. But $y \in \mathrm{Ker}(\zeta)$. So $\alpha(y') = 0$.

Let $\theta, \varphi\colon R \rightrightarrows R^m$ be the homomorphisms with $\theta(1) := y'$ and $\varphi(1) := 0$. They yield maps in Λ_M. So, by definition of direct limit, they have the same compositions with the insertion ι_m. Hence $y = \iota_m(y') = 0$. Thus ζ is injective, so bijective. □

THEOREM **(9.16)** (Lazard). — *Let R be a ring, M a module. Then the following conditions are equivalent:*

(1) *M is flat.*
(2) *Given a finitely presented module P, this version of* **(9.12.1)** *is surjective:*
$$\mathrm{Hom}_R(P, R) \otimes_R M \to \mathrm{Hom}_R(P, M).$$
(3) *Given a finitely presented module P and a map $\beta\colon P \to M$, there exists a factorization $\beta\colon P \xrightarrow{\gamma} R^n \xrightarrow{\alpha} M$;*
(4) *Given an $\alpha\colon R^m \to M$ and a $k \in \mathrm{Ker}(\alpha)$, there exists a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi(k) = 0$.*
(5) *Given an $\alpha\colon R^m \to M$ and $k_1, \dots, k_r \in \mathrm{Ker}(\alpha)$ there exists a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi(k_i) = 0$ for $i = 1, \dots, r$.*
(6) *Given $R^r \xrightarrow{\rho} R^m \xrightarrow{\alpha} M$ such that $\alpha\rho = 0$, there exists a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi\rho = 0$.*
(7) *Λ_M is filtered.*
(8) *M is a filtered direct limit of free modules of finite rank.*

PROOF: Assume (1). Then **(9.12)** yields (2).

Assume (2). Consider (3). There are $\gamma_1, \dots, \gamma_n \in \mathrm{Hom}(P, R)$ and $x_1, \dots, x_n \in M$ such that $\beta(p) = \sum \gamma_i(p)x_i$. Let $\gamma\colon P \to R^n$ be $(\gamma_1, \dots, \gamma_n)$, and let $\alpha\colon R^n \to M$ be given by $\alpha(r_1, \dots, r_n) = \sum r_i x_i$. Then $\beta = \alpha\gamma$, as (3) requires.

Assume (3), and consider (4). Set $P := R^m/Rk$, and let $\kappa\colon R^m \to P$ denote the quotient map. Then P is finitely presented, and there is $\beta\colon P \to M$ such that $\beta\kappa = \alpha$. By (3), there is a factorization $\beta\colon P \xrightarrow{\gamma} R^n \to M$. Set $\varphi := \gamma\kappa$. Then $\beta\colon R^m \xrightarrow{\varphi} R^n \to M$ is a factorization of β and $\varphi(k) = 0$.

Assume (4), and consider (5). Set $m_0 := m$ and $\alpha_0 = \alpha$. Inductively, (4) yields
$$\alpha_{i-1}\colon R^{m_{i-1}} \xrightarrow{\varphi_i} R^{m_i} \xrightarrow{\alpha_i} M \quad \text{for} \quad i = 1, \dots, r$$
such that $\varphi_i \cdots \varphi_1(k_i) = 0$. Set $\varphi := \varphi_r \cdots \varphi_1$ and $n := m_r$. Then (5) holds.

Assume (5), and consider (6). Let $e_1, \dots, e_r$ be the standard basis of R^r, and set $k_i := \rho(e_i)$. Then $\alpha(k_i) = 0$. So (5) yields a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi(k_i) = 0$. Then $\varphi\rho = 0$, as required by (6).

Assume (6). Given (R^{m_1}, α_1) and (R^{m_2}, α_2) in Λ_M, set $m := m_1 + m_2$ and $\alpha := \alpha_1 + \alpha_2$. Then the inclusions $R^{m_i} \to R^m$ induce maps in Λ_M. Thus the first

condition of **(7.1)** is satisfied.

Given $\sigma, \tau\colon (R^r, \omega) \rightrightarrows (R^m, \alpha)$ in Λ_M, set $\rho := \sigma - \tau$. Then $\alpha\rho = 0$. So (6) yields a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ with $\varphi\rho = 0$. Then φ is a map of Λ_M, and $\varphi\sigma = \varphi\tau$. Hence the second condition of **(7.1)** is satisfied. Thus (7) holds.

If (7) holds, then (8) does too, since $M = \varinjlim_{(R^m,\alpha)\in\Lambda_M} R^m$ by **(9.15)**.

Assume (8). Say $M = \varinjlim M_\lambda$ with the M_λ free. Each M_λ is flat by **(9.4)**, and a filtered direct limit of flat modules is flat by **(9.11)**. Thus M is flat □

Exercise **(9.17)** (*Equational Criterion for Flatness*). — Prove that the Condition **(9.16)**(4) can be reformulated as follows: For every relation $\sum_i x_i y_i = 0$ with $x_i \in R$ and $y_i \in M$, there are $x_{ij} \in R$ and $y'_j \in M$ such that

$$\textstyle\sum_j x_{ij} y'_j = y_i \text{ for all } i \text{ and } \sum_i x_{ij} x_i = 0 \text{ for all } j. \qquad \textbf{(9.17.1)}$$

Lemma **(9.18)** (Ideal Criterion for Flatness). — *A module N is flat if and only if $\mathfrak{a} \otimes N \xrightarrow{\sim} \mathfrak{a}N$ for every finitely generated ideal $\mathfrak{a}$.*

Proof: In any case, **(8.5)**(2) implies $R\otimes N \xrightarrow{\sim} N$ with $a\otimes x \mapsto ax$. If N is flat, then the inclusion $\mathfrak{a} \hookrightarrow R$ yields an injection $\mathfrak{a}\otimes N \hookrightarrow R\otimes N$, and so $\mathfrak{a}\otimes N \xrightarrow{\sim} \mathfrak{a}N$.

To prove the converse, let's check the criterion **(9.17)**. Given $\sum_{i=1}^n x_i y_i = 0$ with $x_i \in R$ and $y_i \in N$, set $\mathfrak{a} := \langle x_1, \dots, x_n\rangle$. If $\mathfrak{a} \otimes N \xrightarrow{\sim} \mathfrak{a}N$, then $\sum_i x_i \otimes y_i = 0$; so the Equational Criterion for Vanishing **(8.17)** yields **(9.17.1)**. Thus N is flat. □

Example **(9.19)**. — Let R be a domain, and set $K := \mathrm{Frac}(R)$. Then K is flat, but K is not projective unless $R = K$. Indeed, **(8.6)** says $\mathfrak{a} \otimes_R K = K$, with $a \otimes x = ax$, for any ideal $\mathfrak{a}$ of R. So K is flat by **(9.18)**.

Suppose K is projective. Then $K \hookrightarrow R^\Lambda$ for some Λ by **(5.22)**. So there is a nonzero map $\alpha\colon K \to R$. So there is an $x \in K$ with $\alpha(x) \neq 0$. Set $a := \alpha(x)$. Take any nonzero $b \in R$. Then $ab \cdot \alpha(x/ab) = \alpha(x) = a$. Since R is a domain, $b \cdot \alpha(x/ab) = 1$. Hence $b \in R^\times$. Thus R is a field. So **(2.3)** yields $R = K$.

Exercise **(9.20)**. — Let R be a domain, M a module. Prove that, if M is flat, then M is **torsion free**; that is, $\mu_x\colon M \to M$ is injective for all nonzero $x \in R$. Prove that, conversely, if R is a PID and M is torsion free, then M is flat.

10. Cayley–Hamilton Theorem

The Cayley–Hamilton Theorem says that a matrix satisfies its own characteristic polynomial. We prove an equivalent form, known as the "Determinant Trick." Using the Trick, we obtain various results, including the uniqueness of the rank of a finitely generated free module. We also obtain Nakayama's Lemma, and use it to study finitely generated modules further. Then we turn to the important notions of integrality and module finiteness for an algebra. Using the Trick, we relate these notions to each other, and study their properties. We end with a discussion of integral extensions and normal rings.

(10.1) (*Cayley–Hamilton Theorem*). — Let R be a ring, and $\mathbf{M} := (a_{ij})$ an $n \times n$ matrix with $a_{ij} \in R$. Let $\mathbf{I}_n$ be the $n \times n$ identity matrix, and T a variable. The **characteristic polynomial** of $\mathbf{M}$ is the following polynomial:

$$p_{\mathbf{M}}(T) := T^n + a_1 T^{n-1} + \cdots + a_n := \det(T\mathbf{I}_n - \mathbf{M}).$$

Let $\mathfrak{a}$ be an ideal. If $a_{ij} \in \mathfrak{a}$ for all i, j, then clearly $a_k \in \mathfrak{a}^k$ for all k.

The **Cayley–Hamilton Theorem** asserts that, in the ring of matrices,

$$p_{\mathbf{M}}(\mathbf{M}) = 0.$$

It is a special case of **(10.2)** below; indeed, take $M := R^n$, take $m_1, \dots, m_n$ to be the standard basis, and take φ to be the endomorphism defined by $\mathbf{M}$.

Conversely, given the setup of **(10.2)**, form the surjection $\alpha\colon R^n \twoheadrightarrow M$ taking the ith standard basis element to m_i, and form the map $\Phi\colon R^n \to R^n$ associated to the matrix $\mathbf{M}$. Then $\varphi\alpha = \alpha\Phi$. Hence, given any polynomial $p(T)$, we have $p(\varphi)\alpha = \alpha p(\Phi)$. Hence, if $p(\Phi) = 0$, then $p(\varphi) = 0$ as α is surjective. Thus *the Cayley–Hamilton Theorem and the Determinant Trick* **(10.2)** *are equivalent.*

Theorem **(10.2)** (Determinant Trick). — *Let M be an R-module generated by $m_1, \dots, m_n$, and $\varphi\colon M \to M$ an endomorphism. Say $\varphi(m_i) =: \sum_{j=1}^n a_{ij} m_j$ with $a_{ij} \in R$, and form the matrix $\mathbf{M} := (a_{ij})$. Then $p_{\mathbf{M}}(\varphi) = 0$ in $\operatorname{End}(M)$.*

Proof: Let δ_{ij} be the Kronecker delta function, $\mu_{a_{ij}}$ the multiplication map. Let $\mathbf{\Delta}$ stand for the matrix $(\delta_{ij}\varphi - \mu_{a_{ij}})$ with entries in $\operatorname{End}(M)$, and $\mathbf{X}$ for the column vector (m_j). Then clearly $\mathbf{\Delta X} = 0$. Multiply on the left by the **matrix of cofactors** $\mathbf{\Gamma}$ of $\mathbf{\Delta}$: the (i,j)th entry of $\mathbf{\Gamma}$ is $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the jth row and the ith column of $\mathbf{\Delta}$. Then $\mathbf{\Gamma\Delta X} = 0$. Now, $\mathbf{\Gamma\Delta} = \det(\mathbf{\Delta})\mathbf{I}_n$. Hence $\det(\mathbf{\Delta})m_j = 0$ for all j. Thus $p_{\mathbf{M}}(\varphi) = 0$. □

Proposition **(10.3)**. — *Let M be a finitely generated module, $\mathfrak{a}$ an ideal. Then $M = \mathfrak{a}M$ if and only if there exists $a \in \mathfrak{a}$ such that $(1 + a)M = 0$.*

Proof: Assume $M = \mathfrak{a}M$. Say $m_1, \dots, m_n$ generate M, and $m_i = \sum_{j=1}^n a_{ij} m_j$ with $a_{ij} \in \mathfrak{a}$. Set $\mathbf{M} := (a_{ij})$. Say $p_{\mathbf{M}}(T) = T^n + a_1 T^{n-1} + \cdots + a_n$. Set $a := a_1 + \cdots + a_n \in \mathfrak{a}$. Then $(1 + a)M = 0$ by **(10.2)** with $\varphi := 1_M$.

Conversely, if there exists $a \in \mathfrak{a}$ such that $(1 + a)M = 0$, then $m = -am$ for all $m \in M$. So $M \subset \mathfrak{a}M \subset M$. Thus $M = \mathfrak{a}M$. □

Corollary **(10.4)**. — *Let R be a ring, M a finitely generated module, and φ an endomorphism of M. If φ is surjective, then φ is an isomorphism.*

PROOF: Let $P := R[X]$ be the polynomial ring in one variable. By the UMP of P, there is an R-algebra homomorphism $\mu\colon P \to \mathrm{End}(M)$ with $\mu(X) = \varphi$. So M is an P-module such that $p(X)M = p(\varphi)M$ for any $p(X) \in P$ by **(4.4)**. Set $\mathfrak{a} := \langle X \rangle$. Since φ is surjective, $M = \mathfrak{a}M$. By **(10.3)**, there is $a \in \mathfrak{a}$ with $(1+a)M = 0$. Say $a = Xr$ for some polynomial r. Then $1_M + \varphi r(\varphi) = 0$. Thus φ is invertible. □

COROLLARY **(10.5)**. — *Let R be a ring, m and n positive integers.*

(1) *Then any n generators $v_1, \dots, v_n$ of the free module R^n form a free basis.*

(2) *If $R^m \simeq R^n$, then $m = n$.*

PROOF: Form the surjection $\alpha\colon R^n \twoheadrightarrow R^n$ taking the ith standard basis element to v_i. Then φ is an isomorphism by **(10.4)**. So the v_i form a free basis by **(4.10)**(3).

To prove (2), say $m \le n$. Then R^n has m generators. Add to them $n - m$ zeros. The result is a free basis by (1), so can contain no zeros. Thus $n - m = 0$. □

EXERCISE **(10.6)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a}$ is finitely generated and satisfies $\mathfrak{a} = \mathfrak{a}^2$. Prove there is a unique idempotent e such that $\langle e \rangle = \mathfrak{a}$.

PROPOSITION **(10.7)**. — *Let R be a ring, $\mathfrak{a}$ an ideal. Then these conditions are equivalent:*

(1) *$R/\mathfrak{a}$ is projective over R.*

(2) *$R/\mathfrak{a}$ is flat over R, and $\mathfrak{a}$ is finitely generated.*

(3) *$\mathfrak{a}$ is generated by an idempotent.*

PROOF: Suppose (1) holds. Then $R/\mathfrak{a}$ is flat by **(9.6)**. Further, the sequence $0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$ splits by **(5.22)**, and so $\mathfrak{a}$ is principal. Thus (2) holds.

Suppose (2) holds. Then $\mathfrak{a} = \mathfrak{a}^2$ by **(9.9)**. Thus (3) holds by **(10.6)**.

Suppose (3) holds. Then $R = \mathfrak{a} \times R/\mathfrak{a}$ by **(1.11)**. So (1) holds by **(5.22)**. □

LEMMA **(10.8)** (Nakayama). — *Let R be a ring, $\mathfrak{m} \subset \mathrm{rad}(R)$ an ideal, M a finitely generated module. Assume $M = \mathfrak{m}M$. Then $M = 0$.*

PROOF: By **(10.3)**, there is $a \in \mathfrak{m}$ with $(1+a)M = 0$. By **(3.2)**, $1 + a$ is a unit. Thus $M = (1+a)^{-1}(1+a)M = 0$.

Alternatively, suppose $M \neq 0$. Say $m_1, \dots, m_n$ generate M with n minimal. Then $m_1 = a_1 m_1 + \cdots + a_n m_n$ with $a_i \in \mathfrak{m}$. By **(3.2)**, we may set $x_i := (1 - a_1)^{-1} a_i$. Then $m_1 = x_2 m_2 + \cdots + x_n m_n$, contradicting minimality of n. Thus $M = 0$. □

PROPOSITION **(10.9)**. — *Let R be a ring, $\mathfrak{m} \subset \mathrm{rad}(R)$ an ideal, $N \subset M$ modules.*

(1) *If M/N is finitely generated and if $N + \mathfrak{m}M = M$, then $N = M$.*

(2) *Assume M is finitely generated. Then elements $m_1, \dots, m_n$ generate M if and only if their images $m_1', \dots, m_n'$ generate $M' := M/\mathfrak{m}M$.*

PROOF: In (1), the second hypothesis holds if and only if $\mathfrak{m}(M/N) = M/N$. Hence (1) holds by **(10.8)** applied with M/N for M.

In (2), let N be the submodule generated by $m_1, \dots, m_n$. Since M is finitely generated, so is M/N. Hence $N = M$ if the m_i' generate $M/\mathfrak{m}M$ by (1). The converse is obvious. □

EXERCISE **(10.10)**. — Let A be a local ring, $\mathfrak{m}$ the maximal ideal, M a finitely generated A-module, and $m_1, \dots, m_n \in M$. Set $k := A/\mathfrak{m}$ and $M' := M/\mathfrak{m}M$, and write m_i' for the image of m_i in M'. Prove that $m_1', \dots, m_n' \in M'$ form a basis of the k-vector space M' if and only if $m_1, \dots, m_n$ form a **minimal generating**

set of M (that is, no proper subset generates M), and prove that every minimal generating set of M has the same number of elements.

Exercise **(10.11)**. — Let A be a local ring, k its residue field, M and N finitely generated modules. (1) Show that $M = 0$ if and only if $M \otimes_A k = 0$. (2) Show that $M \otimes_A N \neq 0$ if $M \neq 0$ and $N \neq 0$.

Proposition **(10.12)**. — *Consider these conditions on an R-module P:*

(1) *P is free and of finite rank;*
(2) *P is projective and finitely generated;*
(3) *P is flat and finitely presented.*

Then (1) *implies* (2)*, and* (2) *implies* (3)*; all three are equivalent if R is local.*

Proof: A free module is always projective by **(5.21)**, and a projective module is always flat by **(9.6)**. Further, each of the three conditions requires P to be finitely generated; so assume it is. Thus (1) implies (2).

Let $p_1, \dots, p_n \in P$ generate, and let $0 \to L \to R^n \to P \to 0$ be the short exact sequence defined by sending the ith standard basis element to p_i. Set $F := R^n$.

Assume P is projective. Then the sequence splits by **(5.22)**. So **(5.9)** yields a surjection $\rho\colon F \to L$. Hence L is finitely generated. Thus (2) implies (3).

Assume P is flat and R is local. Denote the residue field of R by k. Then, by **(9.10)**(1), the sequence $0 \to L \otimes k \to F \otimes k \to P \otimes k \to 0$ is exact. Now, $F \otimes k = (R \otimes k)^n = k^n$ by **(8.11)** and the unitary law; so $\dim_k F \otimes k = n$. Finally, rechoose the p_i so that n is minimal. Then $\dim_k P \otimes k = n$, because the $p_i \otimes 1$ form a basis by **(10.10)**. Therefore, $\dim_k L \otimes k = 0$; so $L \otimes k = 0$.

Assume P is finitely presented. Then L is finitely generated by **(5.24)**. Hence $L = 0$ by **(10.11)**(1). So $F = P$. Thus (3) implies (1). □

Definition **(10.13)**. — Let R be a ring, R' an R-algebra. Then R' is said to be **module finite** over R if R' is a finitely generated R-module.

An element $x \in R'$ is said to be **integral over** R or **integrally dependent on** R if there exist a positive integer n and elements $a_i \in R$ such that

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0. \qquad \textbf{(10.13.1)}$$

Such an equation is called an **equation of integral dependence of degree** n.

If every $x \in R'$ is integral over R, then R' is said to be **integral over** R.

Exercise **(10.14)**. — Let G be a finite group acting on a domain R, and R' the ring of invariants. Show every $x \in R$ is integral over R', in fact, over the subring R'' generated by the elementary symmetric functions in the conjugates gx for $g \in G$.

Proposition **(10.15)**. — *Let R be a ring, R' an R-algebra, n a positive integer, and $x \in R'$. Then the following conditions are equivalent:*

(1) *x satisfies an equation of integral dependence of degree n;*
(2) *$R[x]$ is generated as an R-module by $1, x, \dots, x^{n-1}$;*
(3) *x lies in a subalgebra R'' generated as an R-module by n elements;*
(4) *there is a faithful $R[x]$-module M generated over R by n elements.*

Proof: Assume (1) holds. Say $p(X)$ is a monic polynomial of degree n with $p(x) = 0$. For any m, let $M_m \subset R[x]$ be the R-submodule generated by $1, \dots, x^m$. For $m \geq n$, clearly $x^m - x^{m-n}p(x)$ is in M_{m-1}. But $p(x) = 0$. So also $x^m \in M_{m-1}$. So by induction, $M_m = M_{n-1}$. Hence $M_{n-1} = R[x]$. Thus (2) holds.

If (2) holds, then trivially (3) holds with $R'' := R[x]$.

If (3) holds, then (4) holds with $M := R''$, as $xM = 0$ implies $x = x \cdot 1 = 0$.

Assume (4) holds. In **(10.2)**, take $\varphi := \mu_x$. We obtain a monic polynomial p of degree n with $p(x)M = 0$. Since M is faithful, $p(x) = 0$. Thus (1) holds. □

Exercise **(10.16)**. — Let k be a field, $P := k[X]$ the polynomial ring in one variable, $f \in P$. Set $R := k[X^2] \subset P$. Using the free basis $1, X$ of P over R, find an explicit equation of integral dependence of degree 2 on R for f.

Corollary **(10.17)**. — *Let R be a ring, P the polynomial ring in one variable, and $\mathfrak{a}$ an ideal of P. Set $R' := P/\mathfrak{a}$, and let x be the image of X in R'. Let n be a positive integer. Then the following conditions are equivalent:*

(1) *$\mathfrak{a} = \langle p \rangle$ where p is a monic polynomial of degree n;*
(2) *$1, x, \dots, x^{n-1}$ form a free basis of R' over R;*
(3) *R' is a free R-module of rank n.*

Proof: Assume (1) holds. Then $p(x) = 0$ is an equation of integral dependence of degree n. So $1, x, \dots, x^{n-1}$ generate R' by (1)⇒(2) of **(10.15)**. Suppose

$$b_1 x^{n-1} + \cdots + b_n = 0$$

with the $b_i \in R$. Set $q(X) := b_1 X^{n-1} + \cdots + b_n$. Then $q(x) = 0$. So $q \in \mathfrak{a}$. Hence $q = fp$ for some $f \in P$. But p is monic of degree n. Hence $q = 0$. Thus (2) holds.

Trivially, (2) implies (3).

Finally, assume (3) holds. Then (3)⇒(1) of **(10.15)** yields a monic polynomial $p \in \mathfrak{a}$ of degree n. Form the induced homomorphism $\psi\colon P/\langle p \rangle \to R'$. It is obviously surjective. Since (1) implies (3), the quotient $P/\langle p \rangle$ is free of rank n. So ψ is an isomorphism by **(10.4)**. Hence $\langle p \rangle = \mathfrak{a}$. Thus (1) holds. □

Lemma **(10.18)**. — *Let R be a ring, R' a module-finite R-algebra, and M a finitely generated R'-module. Then M is a finitely generated R-module.*

Proof: Say elements x_i generate R' as a module over R, and say elements m_j generate M over R'. Then clearly the products $x_i m_j$ generate M over R. □

Theorem **(10.19)** (Tower Law for Integrality). — *Let R be a ring, R' an algebra, and R'' an R'-algebra. If $x \in R''$ is integral over R' and if R' is integral over R, then x is integral over R.*

Proof: Say $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in R'$. For $m = 1, \dots, n$, set $R_m := R[a_1, \dots, a_m] \subset R''$. Then R_m is module finite over R_{m-1} by (1)⇒(2) of **(10.15)**. So R_m is module finite over R by **(10.18)** and induction on m.

Moreover, x is integral over R_n. So $R_n[x]$ is module finite over R_n by (1)⇒(2) of **(10.15)**. Hence $R_n[x]$ is module finite over R by **(10.18)**. So x is integral over R by (3)⇒(1) of **(10.15)**, as desired. □

Theorem **(10.20)**. — *Let R be a ring, R' an R-algebra. Then the following conditions are equivalent:*

(1) *R' is finitely generated as an R-algebra and is integral over R;*
(2) *$R' = R[x_1, \dots, x_n]$ with all x_i integral over R;*
(3) *R' is module-finite over R.*

PROOF: Trivially, (1) implies (2).

Assume (2) holds. To prove (3), set $R'' := R[x_1] \subset R'$. Then R'' is module finite over R by (1)⇒(2) of **(10.15)**. We may assume R' is module finite over R'' by induction on n. So **(10.18)** yields (3).

If (3) holds, then R' is integral over R by (3)⇒(1) of **(10.15)**; so (1) holds. □

EXERCISE **(10.21)**. — Let $R_1, \dots, R_n$ be R-algebras, integral over R. Show that their product $\prod R_i$ is a integral over R.

DEFINITION **(10.22)**. — Let R be a ring, R' an algebra. The **integral closure** or **normalization** of R in R' is the subset $\overline{R}$ of elements that are integral over R. If $R \subset R'$ and $R = \overline{R}$, then R is said to be **integrally closed** in R'.

If R is a domain, then its integral closure $\overline{R}$ in its fraction field $\mathrm{Frac}(R)$ is called simply its **normalization**, and R is said to be **normal** if $R = \overline{R}$.

EXERCISE **(10.23)**. — For $1 \le i \le r$, let R_i be a ring, R_i' an extension of R_i, and $x_i \in R_i'$. Set $R := \prod R_i$, set $R' := \prod R_i'$, and set $x := (x_1, \dots, x_r)$. Prove

(1) x is integral over R if and only if x_i is integral over R_i for each i;

(2) R is integrally closed in R' if and only if each R_i is integrally closed in R_i'.

COROLLARY **(10.24)**. — *Let R be a ring, R' an R-algebra, $\overline{R}$ the integral closure of R in R'. Then $\overline{R}$ is an R-algebra, and is integrally closed in R'.*

PROOF: Take $a \in R$ and $x, y \in \overline{R}$. Then the ring $R[x, y]$ is integral over R by (2)⇒(1) of **(10.20)**. So ax and $x + y$ and xy are integral over R. Thus $\overline{R}$ is an R-algebra. Finally, $\overline{R}$ is integrally closed in R' owing to **(10.19)**. □

THEOREM **(10.25)** (Gauss). — *A UFD is normal.*

PROOF: Let R be the UFD. Given $x \in \mathrm{Frac}(R)$, say $x = r/s$ with $r, s \in R$ relatively prime. Suppose x satisfies **(10.13.1)**. Then

$$r^n = -(a_1 r^{n-1} + \cdots + a_n s^{n-1})s.$$

So any prime element dividing s also divides r. Hence s is a unit. Thus $x \in R$. □

EXAMPLE **(10.26)**. — (1) A polynomial ring in n variables over a field is a UFD, so normal by **(10.25)**.

(2) The ring $R := \mathbb{Z}[\sqrt{5}]$ is not a UFD, since

$$(1 + \sqrt{5})(1 - \sqrt{5}) = -4 = -2 \cdot 2,$$

and $1 + \sqrt{5}$, and $1 - \sqrt{5}$ and 2 are irreducible, but not associates. However, set $\tau := (1 + \sqrt{5})/2$, the "golden ratio." The ring $\mathbb{Z}[\tau]$ is known to be a PID; see [8, p. 292]. Hence, $\mathbb{Z}[\tau]$ is a UFD, so normal by **(10.25)**; hence, $\mathbb{Z}[\tau]$ contains the normalization $\overline{R}$ of R. On the other hand, $\tau^2 - \tau - 1 = 0$; hence, $\mathbb{Z}[\tau] \subset \overline{R}$. Thus $\mathbb{Z}[\tau] = \overline{R}$.

(3) Let $d \in \mathbb{Z}$ be square-free. In the field $K := \mathbb{Q}(\sqrt{d})$, form $R := \mathbb{Z} + \mathbb{Z}\delta$ where

$$\delta := \begin{cases} (1 + \sqrt{d})/2, & \text{if } d \equiv 1 \pmod 4; \\ \sqrt{d}, & \text{if not.} \end{cases}$$

Then R is the normalization $\overline{\mathbb{Z}}$ of $\mathbb{Z}$ in K; see [1, pp. 412–3].

(4) Let k be a field, $k[t]$ the polynomial ring in one variable. Set $R := k[t^2, t^3]$. Then $\mathrm{Frac}(R) = k(t)$. Further, t is integral over R as t satisfies $X^2 - t^2 = 0$; hence,

$k[t] \subset \overline{R}$. However, $k[t]$ is normal by (1); hence, $k[t] \supset \overline{R}$. Thus $k[t] = \overline{R}$.

Let $k[X, Y]$ be the polynomial ring in two variables, and $\varphi\colon k[X, Y] \to R$ the k-algebra homomorphism defined by $\varphi(X) := t^2$ and $\varphi(Y) := t^3$. Clearly φ is surjective. Set $\mathfrak{p} := \operatorname{Ker}\varphi$. Since R is a domain, but not a field, $\mathfrak{p}$ is prime by **(2.9)**, but not maximal by **(2.16)**. Clearly $\mathfrak{p} \supset \langle Y^2 - X^3\rangle$. Since $Y^2 - X^3$ is irreducible, **(2.23)** implies that $\mathfrak{p} = \langle Y^2 - X^3\rangle$. So $k[X, Y]/\langle Y^2 - X^3\rangle \xrightarrow{\sim} R$, which provides us with another description of R.

Exercise **(10.27)**. — Let k be a field, X and Y variables. Set

$$R := k[X, Y]/\langle Y^2 - X^2 - X^3\rangle,$$

and let $x, y \in R$ be the residues of X, Y. Prove that R is a domain, but not a field. Set $t := y/x \in \operatorname{Frac}(R)$. Prove that $k[t]$ is the integral closure of R in $\operatorname{Frac}(R)$.

11. Localization of Rings

Localization generalizes construction of the fraction field of a domain. We localize an arbitrary ring using as denominators the elements of any given multiplicative set. The result is the universal example of an algebra in which all these elements become units. When the multiplicative set is the complement of a prime ideal, we obtain a local ring. We relate the ideals in the original ring to those in the localized ring. We end by localizing algebras and then varying the set of denominators.

(11.1) (*Localization*). — Let R be a ring, and S a multiplicative set. Define a relation on $R \times S$ by $(x, s) \sim (y, t)$ if there is $u \in S$ such that $xtu = ysu$.

This relation is an equivalence relation. Indeed, it is reflexive as $1 \in S$ and is trivially symmetric. As to transitivity, let $(y, t) \sim (z, r)$. Say $yrv = ztv$ with $v \in S$. Then $xturv = ysurv = ztvsu$. Thus $(x, s) \sim (z, r)$.

Denote by $S^{-1}R$ the set of equivalence classes, and by x/s the class of (x, s).

Define $x/s \cdot y/t := xy/st$. This product is well defined. Indeed, say $y/t = z/r$. Then there is $v \in S$ such that $yrv = ztv$. So $xsyrv = xsztv$. Thus $xy/st = xz/sr$.

Define $x/s + y/t := (tx + sy)/(st)$. Then, similarly, this sum is well defined.

With these definitions, it is easy to check *$S^{-1}R$ is a ring* with $0/1$ for 0 and $1/1$ for 1. It is called the **localization at S or with respect to S**.

Let $\varphi_S \colon R \to S^{-1}R$ be the map given by $\varphi_S(x) := x/1$. Then φ_S is a ring map, and it carries elements of S to units in $S^{-1}R$ as $s/1 \cdot 1/s = 1$.

Exercise **(11.2)**. — Let R be a ring, S a multiplicative set. Prove $S^{-1}R = 0$ if and only if S contains a nilpotent element.

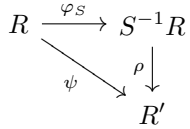
(11.3) (*Total quotient ring*). — Let R be a ring, S the set of all nonzerodivisors of R. Clearly S is a multiplicative set. The map $\varphi_S \colon R \to S^{-1}R$ is injective, because if $\varphi_S x = 0$, then $sx = 0$ for some $s \in S$, and so $x = 0$. We call $S^{-1}R$ the **total quotient ring** of R, and view R as a subring.

Let $T \subset S$ be a multiplicative subset. Clearly, $R \subset T^{-1}R \subset S^{-1}R$.

Suppose R is a domain. Then $S = R - \{0\}$; so the total quotient ring is just the fraction field $\operatorname{Frac}(R)$, and φ_S is just the natural inclusion of R into $\operatorname{Frac}(R)$. Further, $T^{-1}R$ is a domain by **(2.3)** as $T^{-1}R \subset S^{-1}R = \operatorname{Frac}(R)$.

Exercise **(11.4)**. — Find all intermediate rings $\mathbb{Z} \subset R \subset \mathbb{Q}$, and describe each R as a localization of $\mathbb{Z}$. As a starter, prove $\mathbb{Z}[2/3] = S^{-1}\mathbb{Z}$ where $S = \{3^i \mid i \geq 0\}$.

Theorem **(11.5)** (UMP). — *Let R be a ring, S a multiplicative set. Then $S^{-1}R$ is the universal example of an R-algebra in which all the elements of S become units. In fact, given a ring map $\psi \colon R \to R'$, then $\psi(S) \subset R'^{\times}$ if and only if there is a ring map $\rho \colon S^{-1}R \to R'$ with $\rho\varphi_S = \psi$; that is, this diagram commutes:*



Further, there is at most one ρ. Moreover, R' may be noncommutative.

PROOF: First, suppose that ρ exists. Let $s \in S$. Then $\psi(s) = \rho(s/1)$. Hence $\psi(s)\rho(1/s) = \rho(s/1 \cdot 1/s) = 1$. Thus $\psi(S) \subset R'^{\times}$.

Next, note that ρ is determined by ψ as follows:

$$\rho(x/s) = \rho(x/1)\rho(1/s) = \psi(x)\psi(s)^{-1}.$$

Conversely, suppose $\psi(S) \subset R'^{\times}$. Set $\rho(x/s) := \psi(s)^{-1}\psi(x)$. Let's check that ρ is well defined. Say $x/s = y/t$. Then there is $u \in S$ such that $xtu = ysu$. Hence

$$\psi(x)\psi(t)\psi(u) = \psi(y)\psi(s)\psi(u).$$

Since $\psi(u)$ is a unit, $\psi(x)\psi(t) = \psi(y)\psi(s)$. Now, $st = ts$, so

$$\psi(t)^{-1}\psi(s)^{-1} = \psi(s)^{-1}\psi(t)^{-1}.$$

Hence $\psi(x)\psi(s)^{-1} = \psi(y)\psi(t)^{-1}$. Thus ρ is well defined. Clearly, ρ is a ring map. Clearly, $\psi = \rho\varphi_S$. □

COROLLARY **(11.6)**. — *Let R be a ring, and S a multiplicative set. Then the canonical map $\varphi_S \colon R \to S^{-1}R$ is an isomorphism if and only if S consists of units.*

PROOF: If φ_S is an isomorphism, then S consists of units, because $\varphi_S(S)$ does so. Conversely, if S consists of units, then the identity map $R \to R$ has the UMP that characterizes φ_S; whence, φ_S is an isomorphism. □

EXERCISE **(11.7)**. — Let R' and R'' be rings. Consider $R := R' \times R''$ and set $S := \{\,(1,1),\,(1,0)\,\}$. Prove $R' = S^{-1}R$.

EXERCISE **(11.8)**. — Take R and S as in **(11.7)**. On $R \times S$, impose this relation:

$$(x,s) \sim (y,t) \quad \text{if} \quad xt = ys.$$

Prove that it is not an equivalence relation.

DEFINITION **(11.9)**. — Let R be a ring, $f \in R$. Set $S := \{f^n \mid n \geq 0\}$. We call the ring $S^{-1}R$ the **localization of R at f**, and set $R_f := S^{-1}R$ and $\varphi_f := \varphi_S$.

PROPOSITION **(11.10)**. — *Let R be a ring, $f \in R$, and X a variable. Then*

$$R_f = R[X]/\langle 1 - fX \rangle.$$

PROOF: Set $R' := R[X]/\langle 1 - fX\rangle$, and let $\varphi \colon R \to R'$ be the canonical map. Let's show that R' has the UMP characterizing localization **(11.5)**.

First, let $x \in R'$ be the residue of X. Then $1 - x\varphi(f) = 0$. So $\varphi(f)$ is a unit. So $\varphi(f^n)$ is a unit for $n \geq 0$.

Second, let $\psi \colon R \to R''$ be a homomorphism carrying f to a unit. Define $\theta \colon R[X] \to R''$ by $\theta|R = \psi$ and $\theta X = \psi(f)^{-1}$. Then $\theta(1 - fX) = 0$. So θ factors via a homomorphism $\rho \colon R' \to R''$, and $\psi = \rho\varphi$. Further, ρ is unique, since every element of R' is a polynomial in x and since $\rho x = \psi(f)^{-1}$ as $1 - (\rho x)(\rho\varphi f) = 0$. □

PROPOSITION **(11.11)**. — *Let R be a ring, S a multiplicative set, $\mathfrak{a}$ an ideal.*

(1) *Then $\mathfrak{a}S^{-1}R = \{a/s \in S^{-1}R \mid a \in \mathfrak{a} \text{ and } s \in S\}$.*
(2) *Then $\mathfrak{a} \cap S \neq \emptyset$ if and only if $\mathfrak{a}S^{-1}R = S^{-1}R$ if and only if $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = R$.*

PROOF: Let $a, b \in \mathfrak{a}$ and x/s, $y/t \in S^{-1}R$. Then $ax/s + by/t = (axt + bys)/st$; further, $axt + bys \in \mathfrak{a}$ and $st \in S$. So $\mathfrak{a}S^{-1}R \subset \{a/s \mid a \in \mathfrak{a} \text{ and } s \in S\}$. But the opposite inclusion is trivial. Thus (1) holds.

As to (2), if $\mathfrak{a} \cap S \ni s$, then $\mathfrak{a}S^{-1}R \ni s/s = 1$, so $\mathfrak{a}S^{-1}R = S^{-1}R$; whence, $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = R$. Conversely, suppose $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = R$. Then $\mathfrak{a}S^{-1}R \ni 1$. So (1) yields $a \in \mathfrak{a}$ and $s \in S$ such that $a/s = 1$. So there exists a $t \in S$ such that $at = st$. But $at \in \mathfrak{a}$ and $st \in S$. So $\mathfrak{a} \cap S \neq \emptyset$. Thus (2) holds. □

DEFINITION **(11.12)**. — Let R be a ring, S a multiplicative set, $\mathfrak{a}$ a subset of R. Then the **saturation** of $\mathfrak{a}$ with respect to S is the set denoted by $\mathfrak{a}^S$ and defined by

$$\mathfrak{a}^S := \{a \in R \mid \text{there is } s \in S \text{ with } as \in \mathfrak{a}\}.$$

If $\mathfrak{a} = \mathfrak{a}^S$, then we say $\mathfrak{a}$ is **saturated**.

PROPOSITION **(11.13)**. — *Let R be a ring, S a multiplicative set, $\mathfrak{a}$ an ideal.*
(1) *Then* $\mathrm{Ker}(\varphi_S) = \langle 0 \rangle^S$. (2) *Then* $\mathfrak{a} \subset \mathfrak{a}^S$. (3) *Then* $\mathfrak{a}^S$ *is an ideal.*

PROOF: Clearly, (1) holds, for $a/1 = 0$ if and only if there is $s \in S$ with $as = 0$. Clearly, (2) holds as $1 \in S$. Clearly, (3) holds, for if as, $bt \in \mathfrak{a}$, then $(a + b)st \in \mathfrak{a}$, and if $x \in R$, then $xas \in \mathfrak{a}$. □

EXERCISE **(11.14)**. — Let R be a ring, S a multiplicative set. Prove that

$$\mathrm{nil}(R)(S^{-1}R) = \mathrm{nil}(S^{-1}R).$$

PROPOSITION **(11.15)**. — *Let R be a ring, S a multiplicative set.*
(1) *Let $\mathfrak{b}$ be an ideal of $S^{-1}R$. Then*

$$\text{(a) } \varphi_S^{-1}\mathfrak{b} = (\varphi_S^{-1}\mathfrak{b})^S \quad \textit{and} \quad \text{(b) } \mathfrak{b} = (\varphi_S^{-1}\mathfrak{b})(S^{-1}R).$$

(2) *Let $\mathfrak{a}$ be an ideal of R. Then $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = \mathfrak{a}^S$.*
(3) *Let $\mathfrak{p}$ be a prime ideal of R, and assume $\mathfrak{p} \cap S = \emptyset$. Then*

$$\text{(a) } \mathfrak{p} = \mathfrak{p}^S \quad \text{and} \quad \text{(b) } \mathfrak{p}S^{-1}R \text{ is prime.}$$

PROOF: To prove (1)(a), take $a \in R$ and $s \in S$ with $as \in \varphi_S^{-1}\mathfrak{b}$. Then $as/1 \in \mathfrak{b}$; so $a/1 \in \mathfrak{b}$ because $1/s \in S^{-1}R$. Hence $a \in \varphi_S^{-1}\mathfrak{b}$. Therefore, $(\varphi_S^{-1}\mathfrak{b})^S \subset \varphi_S^{-1}\mathfrak{b}$. The opposite inclusion holds as $1 \in S$. Thus (1)(a) holds.

To prove (1)(b), take $a/s \in \mathfrak{b}$. Then $a/1 \in \mathfrak{b}$. So $a \in \varphi_S^{-1}\mathfrak{b}$. Hence $a/1 \cdot 1/s$ is in $(\varphi_S^{-1}\mathfrak{b})(S^{-1}R)$. Thus $\mathfrak{b} \subset (\varphi_S^{-1}\mathfrak{b})(S^{-1}R)$. Now, take $a \in \varphi_S^{-1}\mathfrak{b}$. Then $a/1 \in \mathfrak{b}$. So $\mathfrak{b} \supset (\varphi_S^{-1}\mathfrak{b})(S^{-1}R)$. Thus (1)(b) holds too.

To prove (2), take $a \in \mathfrak{a}^S$. Then there is $s \in S$ with $as \in \mathfrak{a}$. But $a/1 = as/1 \cdot 1/s$. So $a/1 \in \mathfrak{a}S^{-1}R$. Thus $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) \supset \mathfrak{a}^S$. Now, take $x \in \varphi_S^{-1}(\mathfrak{a}S^{-1}R)$. Then $x/1 = a/s$ with $a \in \mathfrak{a}$ and $s \in S$ by **(11.13)**(1). Hence there is $t \in S$ such that $xst = at \in \mathfrak{a}$. So $x \in \mathfrak{a}^S$. Thus $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) \subset \mathfrak{a}^S$. Thus (2) holds.

To prove (3), note $\mathfrak{p} \subset \mathfrak{p}^S$ as $1 \in S$. Conversely, if $sa \in \mathfrak{p}$ with $s \in S \subset R - \mathfrak{p}$, then $a \in \mathfrak{p}$ as $\mathfrak{p}$ is prime. Thus (a) holds.

As for (b), say $a/s \cdot b/t \in \mathfrak{p}S^{-1}R$. Then $ab \in \varphi_S^{-1}(\mathfrak{p}S^{-1}R)$, and the latter is equal to $\mathfrak{p}^S$ by (2), so to $\mathfrak{p}$ by (a). Hence $ab \in \mathfrak{p}$, so either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. So either $a/s \in \mathfrak{p}S^{-1}R$ or $b/t \in \mathfrak{p}S^{-1}R$. Thus $\mathfrak{p}S^{-1}R$ is prime. Thus (3) holds. □

COROLLARY **(11.16)**. — *Let R be a ring, S a multiplicative set.*

(1) *Then $\mathfrak{a} \mapsto \mathfrak{a}S^{-1}R$ is an inclusion-preserving bijection from the set of all ideals $\mathfrak{a}$ of R with $\mathfrak{a} = \mathfrak{a}^S$ to the set of all ideals $\mathfrak{b}$ of $S^{-1}R$. The inverse is $\mathfrak{b} \mapsto \varphi_S^{-1}\mathfrak{b}$.*

(2) *Then $\mathfrak{p} \mapsto \mathfrak{p}S^{-1}R$ is an inclusion-preserving bijection from the set of all primes of R with $\mathfrak{p} \cap S = \emptyset$ to the set of all primes $\mathfrak{q}$ of $S^{-1}R$. The inverse is $\mathfrak{q} \mapsto \varphi_S^{-1}\mathfrak{q}$.*

PROOF: In (1), the maps are inverses by **(11.15)**(1), (2); clearly, they preserve inclusions. Further, (1) implies (2) by **(11.15)**(3), by **(2.8)**, and by **(11.11)**(2). □

DEFINITION **(11.17)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal. Set $S := R - \mathfrak{p}$. We call the ring $S^{-1}R$ the **localization of R at $\mathfrak{p}$**, and set $R_\mathfrak{p} := S^{-1}R$ and $\varphi_\mathfrak{p} := \varphi_S$.

PROPOSITION **(11.18)**. — *Let R be a ring, $\mathfrak{p}$ a prime ideal. Then $R_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}R_\mathfrak{p}$.*

PROOF: Let $\mathfrak{b}$ be a proper ideal of $R_\mathfrak{p}$. Then $\varphi_\mathfrak{p}^{-1}\mathfrak{b} \subset \mathfrak{p}$ owing to **(11.11)**(2). Hence **(11.16)**(1) yields $\mathfrak{b} \subset \mathfrak{p}R_\mathfrak{p}$. Thus $\mathfrak{p}R_\mathfrak{p}$ is a maximal ideal, and the only one.

Alternatively, let $x/s \in R_\mathfrak{p}$. Suppose x/s is a unit. Then there is a y/t with $xy/st = 1$. So there is a $u \notin \mathfrak{p}$ with $xyu = stu$. But $stu \notin \mathfrak{p}$. Hence $x \notin \mathfrak{p}$.

Conversely, let $x \notin \mathfrak{p}$. Then $s/x \in R_\mathfrak{p}$. So x/s is a unit in $R_\mathfrak{p}$ if and only if $x \notin \mathfrak{p}$, so if and only if $x/s \notin \mathfrak{p}R_\mathfrak{p}$. Thus by **(11.11)**(1), the nonunits of $R_\mathfrak{p}$ form $\mathfrak{p}R_\mathfrak{p}$, which is an ideal. Hence **(3.4)** yields the assertion. □

(11.19) (*Algebras*). — Let R be a ring, S a multiplicative set, R' an R-algebra. It is easy to generalize **(11.1)** as follows. Define a relation on $R' \times S$ by $(x, s) \sim (y, t)$ if there is $u \in S$ with $xtu = ysu$. It is easy to check, as in **(11.1)**, that this relation is an equivalence relation.

Denote by $S^{-1}R'$ the set of equivalence classes, and by x/s the class of (x, s). Clearly, $S^{-1}R'$ is an $S^{-1}R$-algebra with addition and multiplication given by

$$x/s + y/t := (xt + ys)/(st) \quad \text{and} \quad x/s \cdot y/t := xy/st.$$

We call $S^{-1}R'$ the **localization of R' with respect to S**.

Let $\varphi'_S \colon R' \to S^{-1}R'$ be the map given by $\varphi'_S(x) := x/1$. Then φ'_S makes $S^{-1}R'$ into an R'-algebra, so also into an R-algebra, and φ'_S is an R-algebra map.

Note that elements of S become units in $S^{-1}R'$. Moreover, it is easy to check, as in **(11.5)**, that $S^{-1}R'$ has the following UMP: *φ'_S is an algebra map, and elements of S become units in $S^{-1}R'$; further, given an algebra map $\psi \colon R' \to R''$ such that elements of S become units in R'', there is a unique R-algebra map $\rho \colon S^{-1}R' \to R''$ such that $\rho\varphi'_S = \psi$; that is, the following diagram is commutative:*

$$\begin{array}{ccc} R' & \xrightarrow{\varphi'_S} & S^{-1}R' \\ & \searrow^{\psi} & \downarrow{\scriptstyle \rho} \\ & & R'' \end{array}$$

In other words, $S^{-1}R'$ is the *universal example* of an R'-algebra in which the elements of S become units.

Let $\tau \colon R' \to R''$ be an R-algebra map. Then there is a commutative diagram of

R-algebra maps

$$\begin{array}{ccc} R' & \xrightarrow{\tau} & R'' \\ {\scriptstyle\varphi_S}\downarrow & & \downarrow{\scriptstyle\varphi'_S} \\ S^{-1}R' & \xrightarrow{S^{-1}\tau} & S^{-1}R'' \end{array}$$

Further, $S^{-1}\tau$ is an $S^{-1}R$-algebra map.

Let $T \subset R'$ be the image of $S \subset R$. Then T is multiplicative. Further,

$$S^{-1}R' = T^{-1}R',$$

even though $R' \times S$ and $R' \times T$ are rarely equal, because the two UMPs are essentially the same; indeed, any ring map $R' \to R''$ may be viewed as an R-algebra map, and trivially the elements of S become units in R'' if and only if the elements of T do.

Exercise **(11.20)**. — Let R'/R be a integral extension of rings, S a multiplicative subset of R. Show that $S^{-1}R'$ is integral over $S^{-1}R$.

Exercise **(11.21)**. — Let R be a domain, K its fraction field, L a finite extension field, and $\overline{R}$ the integral closure of R in L. Show L is the fraction field of $\overline{R}$. Show every element of L can, in fact, be expressed as a fraction b/a with $b \in \overline{R}$ and $a \in R$.

Exercise **(11.22)**. — Let $R \subset R'$ be domains, K and L their fraction fields. Assume that R' is a finitely generated R-algebra, and that L is a finite dimensional K-vector space. Find an $f \in R$ such that R'_f is module finite over R_f.

Proposition **(11.23)**. — *Let R be a ring, S a multiplicative set. Let T' be a multiplicative set of $S^{-1}R$, and set $T := \varphi_S^{-1}(T')$. Assume $S \subset T$. Then*

$$(T')^{-1}(S^{-1}R) = T^{-1}R.$$

Proof: Let's check $(T')^{-1}(S^{-1}R)$ has the UMP characterizing $T^{-1}R$. Clearly $\varphi_{T'}\varphi_S$ carries T into $\big((T')^{-1}(S^{-1}R)\big)^\times$. Next, let $\psi\colon R \to R'$ be a map carrying T into $R'^\times$. We must show ψ factors uniquely through $(T')^{-1}(S^{-1}R)$.

First, ψ carries S into $R'^\times$ since $S \subset T$. So ψ factors through a unique map $\rho\colon S^{-1}R \to R'$. Now, given $r \in T'$, write $r = x/s$. Then $x/1 = s/1 \cdot r \in T'$ since $S \subset T$. So $x \in T$. Hence $\rho(r) = \psi(x) \cdot \rho(1/s) \in (R')^\times$. So ρ factors through a unique map $\rho'\colon (T')^{-1}(S^{-1}R) \to R'$. Hence $\psi = \rho'\varphi_{T'}\varphi_S$, and ρ' is clearly unique, as required. □

Corollary **(11.24)**. — *Let R be a ring, $\mathfrak{p} \subset \mathfrak{q}$ prime ideals. Then $R_\mathfrak{p}$ is the localization of $R_\mathfrak{q}$ at the prime ideal $\mathfrak{p}R_\mathfrak{q}$.*

Proof: Set $S := R - \mathfrak{q}$ and $T' := R_\mathfrak{q} - \mathfrak{p}R_\mathfrak{q}$. Set $T := \varphi_S^{-1}(T')$. Then $T = R - \mathfrak{p}$ by **(11.16)**(2). So $S \subset T$, and **(11.23)** yields the assertion. □

Exercise **(11.25)**. — Let R be a ring, S and T multiplicative sets.

(1) Set $T' := \varphi_S(T)$ and assume $S \subset T$. Prove

$$T^{-1}R = T'^{-1}(S^{-1}R) = T^{-1}(S^{-1}R).$$

(2) Set $U := \{st \in R \mid s \in S \text{ and } t \in T\}$. Prove

$$T^{-1}(S^{-1}R) = S^{-1}(T^{-1}R) = U^{-1}R.$$

(3) Let $S' := \{t' \in R \mid t't \in S \text{ for some } t \in R\}$. Prove $S'^{-1}R = S^{-1}R$.

PROPOSITION **(11.26)**. — *Let R be a ring, S a multiplicative set, X a variable. Then $(S^{-1}R)[X] = S^{-1}\big(R[X]\big)$.*

PROOF: Let's check $(S^{-1}R)[X]$ and $S^{-1}(R[X])$ have the same UMP: a ring map $\psi\colon R \to R'$ factors uniquely through either one if $\psi(S) \subset (R')^\times$ and if an $x \in R'$ is preassigned as the image of X. First, since $\psi(S) \subset (R')^\times$, there is a unique R-algebra map $S^{-1}R \to R'$, so a unique $(S^{-1}R)$-algebra map $(S^{-1}R)[X] \to R'$ sending X to x. Second, there is a unique R-algebra map $R[X] \to R'$ sending X to x, so a unique $R[X]$-algebra map $R[X] \to R'$ sending X to x, and so a unique $R[X]$-algebra map $S^{-1}(R[X]) \to R'$ since $\psi(S) \subset (R')^\times$, as required. □

COROLLARY **(11.27)**. — *Let R be a ring, S a multiplicative set, X a variable, $\mathfrak{p}$ an ideal of $R[X]$. Set $R' := S^{-1}R$, and let $\varphi\colon R[X] \to R'[X]$ be the canonical map. Then $\mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \emptyset$ if and only if $\mathfrak{p}R'[X]$ is prime and $\mathfrak{p} = \varphi^{-1}\big(\mathfrak{p}R'[X]\big)$.*

PROOF: The assertion results directly from **(11.27)** and **(11.16)**(2). □

EXERCISE **(11.28)**. — Let R be a domain, S a multiplicative set with $0 \notin S$. Assume R is normal. Show that $S^{-1}R$ is normal.

12. Localization of Modules

Formally, we localize a module just as we do a ring. However, the result is a module over the localized ring, and comes equipped with a linear map from the original module; in fact, the result is the universal module with these two properties. Further, as a functor, localization is the left adjoint of restriction of scalars. Hence, localization preserves direct limits, or equivalently, direct sums and cokernels. Therefore, by Watts' Theorem, localization is naturally isomorphic to tensor product with the localized ring. Moreover, localization is exact; so the localized ring is flat. We end by discussing various compatibilities and examples.

PROPOSITION **(12.1)**. — *Let R be a ring, S a multiplicative set. Then a module M has a compatible $S^{-1}R$-module structure if and only if, for all $s \in S$, the multiplication map $\mu_s \colon M \to M$ is bijective; if so, then the $S^{-1}R$-structure is unique.*

PROOF: Assume M has a compatible $S^{-1}R$-structure, and take $s \in S$. Then $\mu_s = \mu_{s/1}$. So $\mu_s \cdot \mu_{1/s} = \mu_{(s/1)(1/s)} = 1$. Similarly, $\mu_{1/s} \cdot \mu_s = 1$. So μ_s is bijective.

Conversely, assume μ_s is bijective for all $s \in S$. Then $\mu_R \colon R \to \operatorname{End}_{\mathbb{Z}}(M)$ sends S into the units of $\operatorname{End}_{\mathbb{Z}}(M)$. Hence μ_R factors through a unique ring map $\mu_{S^{-1}R} \colon S^{-1}R \to \operatorname{End}_{\mathbb{Z}}(M)$ by **(11.5)**. Thus M has a unique compatible $S^{-1}R$-structure by **(4.5)**. □

(12.2) (*Localization of modules*). — Let R be a ring, S a multiplicative set, M a module. Define a relation on $M \times S$ by $(m, s) \sim (n, t)$ if there is $u \in S$ such that $utm = usn$. As in **(11.1)**, this relation is an equivalence relation.

Denote by $S^{-1}M$ the set of equivalence classes, and by m/s the class of (m, s). Then $S^{-1}M$ is an $S^{-1}R$-module with addition given by $m/s + n/t := (tm + sn)/st$ and scalar multiplication by $a/s \cdot m/t := am/st$ similar to **(11.1)**. We call $S^{-1}M$ the **localization of** M at S.

For example, given an ideal $\mathfrak{a}$, then $S^{-1}\mathfrak{a} = \mathfrak{a}S^{-1}R$ owing to **(11.11)**(1). Further, given an R-algebra R', the $S^{-1}R$-module $S^{-1}R'$ constructed here underlies the $S^{-1}R$-algebra $S^{-1}R'$ of **(11.19)**.

Define $\varphi_S \colon M \to S^{-1}M$ by $\varphi_S(m) := m/1$. Clearly, φ_S is R-linear.

Note that $\mu_s \colon S^{-1}M \to S^{-1}M$ is bijective for all $s \in S$ by **(12.1)**.

If $S = \{f^n \mid n \geq 0\}$ for some $f \in R$, then we call $S^{-1}M$ the **localization of** M **at** f, and set $M_f := S^{-1}M$ and $\varphi_f := \varphi_S$.

Similarly, if $S = R - \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, then we call $S^{-1}M$ the **localization of** M **at** $\mathfrak{p}$, and set $M_{\mathfrak{p}} := S^{-1}M$ and $\varphi_{\mathfrak{p}} := \varphi_S$.

THEOREM **(12.3)** (UMP). — *Let R be a ring, S a multiplicative set, and M a module. Then $S^{-1}M$ is the universal example of an $S^{-1}R$-module equipped with an R-linear map from M.*

PROOF: The proof is like that of **(11.5)**: given an R-linear map $\psi \colon M \to N$ where N is an $S^{-1}R$-module, it is easy to prove that ψ factors uniquely via the $S^{-1}R$-linear map $\rho \colon S^{-1}M \to N$ well defined by $\rho(m/s) := 1/s \cdot \psi(m)$. □

EXERCISE **(12.4)**. — Let R be a ring, S a multiplicative set, and M a module. Show that $M = S^{-1}M$ if and only if M is an $S^{-1}R$-module.

EXERCISE **(12.5)**. — Let R be a ring, $S \subset T$ multiplicative sets, M a module. Set $T_1 := \varphi_S(T) \subset S^{-1}R$. Show $T^{-1}M = T^{-1}(S^{-1}M) = T_1^{-1}(S^{-1}M)$.

EXERCISE **(12.6)**. — Let R be a ring, S a multiplicative set. Show that S becomes a filtered category when equipped as follows: given $s, t \in S$, set

$$\mathrm{Hom}(s,t) := \{x \in R \mid xs = t\}.$$

Given a module M, define a functor $S \to ((R\text{-mod}))$ as follows: for $s \in S$, set $M_s := M$; to each $x \in \mathrm{Hom}(s,t)$, associate $\mu_x \colon M_s \to M_t$. Define $\beta_s \colon M_s \to S^{-1}M$ by $\beta_s(m) := m/s$. Show the β_s induce an isomorphism $\varinjlim M_s \xrightarrow{\sim} S^{-1}M$.

EXERCISE **(12.7)**. — Let R be a ring, S a multiplicative set, M a module. Prove $S^{-1}M = 0$ if $\mathrm{Ann}(M) \cap S \neq \emptyset$. Prove the converse if M is finitely generated.

(12.8) (*Functoriality*). — Let R be a ring, S a multiplicative set, $\alpha \colon M \to N$ an R-linear map. Then $\varphi_S\alpha$ carries M to the $S^{-1}R$-module $S^{-1}N$. So **(12.3)** yields a unique $S^{-1}R$-linear map $S^{-1}\alpha$ making the following diagram commutative:

$$\begin{array}{ccc} M & \xrightarrow{\varphi_S} & S^{-1}M \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle S^{-1}\alpha} \\ N & \xrightarrow{\varphi_S} & S^{-1}N \end{array}$$

The construction in the proof of **(12.3)** yields

$$(S^{-1}\alpha)(m/s) = \alpha(m)/s. \tag{12.8.1}$$

Thus, canonically, we obtain the following map, and clearly, it is R-linear:

$$\mathrm{Hom}_R(M,\, N) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M,\, S^{-1}N). \tag{12.8.2}$$

Any R-linear map $\beta \colon N \to P$ yields $S^{-1}(\beta\alpha) = (S^{-1}\beta)(S^{-1}\alpha)$ owing to uniqueness or to **(12.8.1)**. Thus $S^{-1}(\bullet)$ *is a linear functor* from $((R\text{-mod}))$ to $((S^{-1}R\text{-mod}))$.

THEOREM **(12.9)**. — *Let R be a ring, S a multiplicative set. Then the functor $S^{-1}(\bullet)$ is the left adjoint of the functor of restriction of scalars.*

PROOF: Let N be an $S^{-1}R$-module. Then $N = S^{-1}N$ by **(12.4)**, and the map **(12.8.2)** is bijective with inverse taking $\beta \colon S^{-1}M \to N$ to $\beta\varphi_S \colon M \to N$. And **(12.8.2)** is natural in M and N by **(6.3)**. Thus the assertion holds. □

COROLLARY **(12.10)**. — *Let R be a ring, S a multiplicative set. Then the functor $S^{-1}(\bullet)$ preserves direct limits, or equivalently, direct sums and cokernels.*

PROOF: By **(12.9)**, the functor is a left adjoint. Hence it preserves direct limits by **(6.12)**; equivalently, it preserves direct sums and cokernels by **(6.10)**. □

EXERCISE **(12.11)**. — Let R be a ring, S a multiplicative set, P a projective module. Then $S^{-1}P$ is a projective $S^{-1}R$-module.

COROLLARY **(12.12)**. — *Let R be a ring, S a multiplicative set. Then the functors $S^{-1}(\bullet)$ and $S^{-1}R \otimes_R \bullet$ are canonically isomorphic.*

PROOF: As $S^{-1}(\bullet)$ preserves direct sums and cokernels by **(12.10)**, the assertion is an immediate consequence of Watts Theorem **(8.15)**.

Alternatively, both functors are left adjoints of the same functor by **(12.9)** and by **(8.10)**. So they are canonically isomorphic by **(6.4)**. □

EXERCISE **(12.13)**. — Let R be a ring, S a multiplicative set, M and N modules. Show $S^{-1}(M \otimes_R N) = S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} S^{-1}N = S^{-1}M \otimes_R S^{-1}N$.

DEFINITION **(12.14)**. — Let R be a ring, S a multiplicative set, M a module. Given a submodule N, its **saturation** N^S is defined by

$$N^S := \{m \in M \mid \text{there is } s \in S \text{ with } sm \in N\}.$$

If $N = N^S$, then we say N is **saturated**.

PROPOSITION **(12.15)**. — *Let R be a ring, M a module, N and P submodules. Let S be a multiplicative set, and K an $S^{-1}R$-submodule of $S^{-1}M$.*

(1) *Then* (a) *N^S is a submodule of M, and* (b) *$S^{-1}N$ is a submodule of $S^{-1}M$.*
(2) *Then* (a) *$\varphi_S^{-1}K = (\varphi_S^{-1}K)^S$ and* (b) *$K = S^{-1}(\varphi_S^{-1}K)$.*
(3) *Then $\varphi_S^{-1}(S^{-1}N) = N^S$; in particular, $\mathrm{Ker}(\varphi_S) = 0^S$.*
(4) *Then* (a) *$(N \cap P)^S = N^S \cap P^S$ and* (b) *$S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.*
(5) *Then* (a) *$(N + P)^S \supset N^S + P^S$ and* (b) *$S^{-1}(N + P) = S^{-1}N + S^{-1}P$.*

PROOF: Assertion (1)(b) holds because $N \times S$ is a subset of $M \times S$ and is equipped with the induced equivalence relation.

Assertions (1)(a), (2) and (3) can be proved as in **(11.13)**(3) and **(11.15)**(1), (2).

As to (4)(a), clearly $(N \cap P)^S \subset N^S \cap P^S$. Conversely, given $m \in N^S \cap P^S$, there are $s, t \in S$ with $sm \in N$ and $tm \in P$. Then $stm \in N \cap P$ and $st \in S$. So $m \in (N \cap P)^S$. Thus (a) holds. Alternatively, (4)(b) and (3) yield (4)(a).

As to (4)(b), since $N \cap P \subset N$, P, using (1) yields $S^{-1}(N \cap P) \subset S^{-1}N \cap S^{-1}P$. But, given $m/s = n/t \in S^{-1}N \cap S^{-1}P$, there is a $u \in S$ with $utm = usn \in N \cap P$. Hence $utm/uts = usn/uts \in S^{-1}(N \cap P)$. Thus (b) holds.

As to (5)(a), given $n \in N^S$ and $p \in P^S$, there are $s, t \in S$ with $sn \in N$ and $tp \in P$. Then $st \in S$ and $st(n + p) \in N + P$. Thus (5)(a) holds.

As to (5)(b), note N, $P \subset N + P$. So (1)(b) yields $S^{-1}(N + P) \supset S^{-1}N + S^{-1}P$. But the opposite inclusion holds as $(n + p)/s = n/s + p/s$. Thus (5)(b) holds. □

THEOREM **(12.16)** (Exactness of Localization). — *Let R be a ring, and S a multiplicative set. Then the functor $S^{-1}(\bullet)$ is exact.*

PROOF: As $S^{-1}(\bullet)$ preserves injections by **(12.15)**(1) and cokernels by **(12.10)**, it is exact by **(9.3)**.

Alternatively, given an exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$, for each $s \in S$, take a copy $M'_s \to M_s \to M''_s$. Using **(12.6)**, make S into a filtered category, and make these copies into a functor from S to the category of 3-term exact sequences; its limit is the following sequence, which is exact by **(7.10)**, as desired:

$$S^{-1}M' \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}M''.$$

The latter argument can be made more direct as follows. Since $\beta\alpha = 0$, we have $(S^{-1}\beta)(S^{-1}\alpha) = S^{-1}(\beta\alpha) = 0$. Hence $\mathrm{Ker}(S^{-1}\beta) \supset \mathrm{Im}(S^{-1}\alpha)$. Conversely, given $m/s \in \mathrm{Ker}(S^{-1}\beta)$, there is $t \in S$ with $t\beta(m) = 0$. So $\beta(tm) = 0$. So exactness yields $m' \in M'$ with $\alpha(m') = tm$. So $(S^{-1}\alpha)(m'/ts) = m/s$. Hence $\mathrm{Ker}(S^{-1}\beta) \subset \mathrm{Im}(S^{-1}\alpha)$. Thus $\mathrm{Ker}(S^{-1}\beta) = \mathrm{Im}(S^{-1}\alpha)$, as desired. □

COROLLARY **(12.17)**. — *Let R be a ring, S a multiplicative set. Then $S^{-1}R$ is flat over R.*

PROOF: The functor $S^{-1}(\bullet)$ is exact by **(12.16)**, and is isomorphic to $S^{-1}R\otimes_R\bullet$ by **(12.12)**. Thus $S^{-1}R$ is flat.

Alternatively, using **(12.6)**, write $S^{-1}R$ as a filtered direct limit of copies of R. But R is flat by **(9.6)**. Thus $S^{-1}R$ is flat by **(9.11)**. □

COROLLARY **(12.18)**. — *Let R be a ring, S a multiplicative set, and $\mathfrak{a}$ an ideal. Set $R' := R/\mathfrak{a}$. Then $S^{-1}R' = S^{-1}R/S^{-1}\mathfrak{a} = S^{-1}R/\mathfrak{a}S^{-1}R$.*

PROOF: The assertion results from **(12.16)** and **(12.2)**. □

COROLLARY **(12.19)**. — *Let R be a ring, $\mathfrak{p}$ a prime. Then* $\operatorname{Frac}(R/\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.

PROOF: We have $\operatorname{Frac}(R/\mathfrak{p}) = (R/\mathfrak{p})_{\mathfrak{p}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ by **(11.19)** and **(12.18)**. □

PROPOSITION **(12.20)**. — *Let R be a ring, M a module, S a multiplicative set.*

(1) *Let $m_1,\dots,m_n \in M$. If M is finitely generated and if the $m_i/1 \in S^{-1}M$ generate over $S^{-1}R$, then there's $f \in S$ so that the $m_i/1 \in M_f$ generate over R_f.*

(2) *Assume M is finitely presented and $S^{-1}M$ is a free $S^{-1}R$-module of rank n. Then there is $h \in S$ such that M_h is a free R_h-module of rank n.*

PROOF: To prove (1), define $\alpha\colon R^n \to M$ by $\alpha(e_i) := m_i$ with e_i the ith standard basis vector. Set $C := \operatorname{Coker}(\alpha)$. Then $S^{-1}C = \operatorname{Coker}(S^{-1}\alpha)$ by **(12.10)**. Assume the $m_i/1 \in S^{-1}M$ generate over $S^{-1}R$. Then $S^{-1}\alpha$ is surjective by **(4.10)**(1) as $S^{-1}(R^n) = (S^{-1}R)^n$ by **(12.10)**. Hence $S^{-1}C = 0$.

In addition, assume M is finitely generated. Then so is C. Hence, **(12.7)** yields $f \in S$ such that $C_f = 0$. Hence α_f is surjective. So the $m_i/1$ generate M_f over R_f again by **(4.10)**(1). Thus (1) holds.

For (2), let $m_1/s_1,\dots,m_n/s_n$ be a free basis of $S^{-1}M$ over $S^{-1}R$. Then so is $m_1/1,\dots,m_n/1$ as the $1/s_i$ are units. Form α and C as above, and set $K := \operatorname{Ker}(\alpha)$. Then **(12.16)** yields $S^{-1}K = \operatorname{Ker}(S^{-1}\alpha)$ and $S^{-1}C = \operatorname{Coker}(S^{-1}\alpha)$. But $S^{-1}\alpha$ is bijective. Hence $S^{-1}K = 0$ and $S^{-1}C = 0$.

Since M is finitely generated, C is too. Hence, as above, there is $f \in S$ such that $C_f = 0$. Then $0 \to K_f \to R_f^n \xrightarrow{\alpha_f} M_f \to 0$ is exact by **(12.16)**. Take a finite presentation $R^p \to R^q \to M \to 0$. By **(12.16)**, it yields a finite presentation $R_f^p \to R_f^q \to M_f \to 0$. Hence K_f is a finitely generated R_f-module by **(5.24)**.

Let $S_1 \subset R_f$ be the image of S. Then **(12.5)** yields $S_1^{-1}(K_f) = S^{-1}K$. But $S^{-1}K = 0$. Hence there is $g/1 \in S_1$ such that $(K_f)_{g/1} = 0$. Set $h := fg$. Let's show $K_h = 0$. Let $x \in K$. Then there is a such that $(g^a x)/1 = 0$ in K_f. Hence there is b such that $f^b g^a x = 0$ in K. Take $c \geq a, b$. Then $h^c x = 0$. Thus $K_h = 0$. But $C_f = 0$ implies $C_h = 0$. Hence $\alpha_h\colon R_h^n \to M_h$ is an isomorphism, as desired. □

PROPOSITION **(12.21)**. — *Let R be a ring, S a multiplicative set, and M and N modules. Then there is a canonical homomorphism*

$$\sigma\colon S^{-1}\operatorname{Hom}_R(M,N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

Further, σ is injective if M is finitely generated; σ is an isomorphism if M is finitely presented.

PROOF: The assertions result from **(9.13)** with $R' := S^{-1}R$, since $S^{-1}R$ is flat by **(12.17)** and since $S^{-1}R \otimes P = S^{-1}P$ for every R-module P by **(12.12)**. □

EXAMPLE **(12.22)**. — Set $R := \mathbb{Z}$ and $S := \mathbb{Z} - \langle 0 \rangle$ and $M := \mathbb{Q}/\mathbb{Z}$. Then M is faithful since $z \in S$ implies $z \cdot (1/2z) = 1/2 \neq 0$; thus, $\mu_R \colon R \to \operatorname{Hom}_R(M, M)$ is injective. But $S^{-1}R = \mathbb{Q}$. So **(12.16)** yields $S^{-1} \operatorname{Hom}_R(M, M) \neq 0$. On the other hand, $S^{-1}M = 0$ as $s \cdot r/s = 0$ for any $r/s \in M$. So the map $\sigma(M, M)$ of **(12.21)** is not injective. Thus **(12.21)**(2) can fail if M is not finitely generated.

EXAMPLE **(12.23)**. — Take $R := \mathbb{Z}$ and $S := \mathbb{Z} - 0$ and $M_n := \mathbb{Z}/\langle n \rangle$ for $n \geq 2$. Then $S^{-1}M_n = 0$ for all n as $nm \equiv 0 \pmod{n}$ for all m. On the other hand, $(1, 1, \dots)/1$ is nonzero in $S^{-1}\bigl(\prod M_n\bigr)$ as the kth component of $m \cdot (1, 1, \dots)$ is nonzero in $\prod M_n$ for $k > m$ if m is nonzero. Thus $S^{-1}\bigl(\prod M_n\bigr) \neq \prod (S^{-1}M_n)$.

Also $S^{-1}\mathbb{Z} = \mathbb{Q}$. So **(12.12)** yields $\mathbb{Q} \otimes \bigl(\prod M_n\bigr) \neq \prod (\mathbb{Q} \otimes M_n)$, whereas **(8.11)** yields $\mathbb{Q} \otimes \bigl(\bigoplus M_n\bigr) = \bigoplus (\mathbb{Q} \otimes M_n)$.

EXERCISE **(12.24)**. — Set $R := \mathbb{Z}$ and $S = \mathbb{Z} - \langle 0 \rangle$. Set $M := \bigoplus_{n \geq 2} \mathbb{Z}/\langle n \rangle$ and $N := M$. Show that the map σ of **(12.21)** is not injective.

13. Support

The spectrum of a ring is this topological space: its points are all the prime ideals; each closed set consists of those primes containing a given ideal. The support of a module is this subset: its points are the primes at which the localized module is nonzero. We relate the support to the closed set of the annihilator. We prove that a sequence is exact if and only if it is exact after localizing at each maximal ideal. Lastly, we prove that a module is finitely generated and projective if and only if it is locally free of finite rank.

(13.1) (*Spectrum of a ring*). — Let R be a ring. Its set of prime ideals is denoted $\operatorname{Spec}(R)$, and is called the (prime) **spectrum** of R.

Let $\mathfrak{a}$ be an ideal. Let $\mathbf{V}(\mathfrak{a})$ denote the subset of $\operatorname{Spec}(R)$ of those primes that contain $\mathfrak{a}$. We call $\mathbf{V}(\mathfrak{a})$ the **variety** of $\mathfrak{a}$.

Let $\mathfrak{b}$ be another ideal. Then by the Scheinnullstellensatz, $\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{b})$ if and only if $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$. Further, **(2.2)** yields

$$\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) = \mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{V}(\mathfrak{a}\mathfrak{b}).$$

A prime ideal $\mathfrak{p}$ contains the ideals $\mathfrak{a}_\lambda$ in an arbitrary collection if and only if $\mathfrak{p}$ contains their sum $\sum \mathfrak{a}_\lambda$; hence,

$$\bigcap \mathbf{V}(\mathfrak{a}_\lambda) = \mathbf{V}\big(\textstyle\sum \mathfrak{a}_\lambda\big).$$

Finally, $\mathbf{V}(R) = \emptyset$, and $\mathbf{V}(\langle 0 \rangle) = \operatorname{Spec}(R)$. Thus the subsets $\mathbf{V}(\mathfrak{a})$ of $\operatorname{Spec}(R)$ are the closed sets of a topology; it is called the **Zariski topology**.

Given an element $f \in R$, we call the open set

$$\mathbf{D}(f) := \operatorname{Spec}(R) - \mathbf{V}(\langle f \rangle)$$

a **principal open set**. These sets form a basis for the topology of $\operatorname{Spec}(R)$; indeed, given any prime $\mathfrak{p} \not\supset \mathfrak{a}$, there is an $f \in \mathfrak{a} - \mathfrak{p}$, and so $\mathfrak{p} \in \mathbf{D}(f) \subset \operatorname{Spec}(R) - \mathbf{V}(\mathfrak{a})$.

A ring map $\varphi\colon R \to R'$ induces a set map

$$\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(R') \to \operatorname{Spec}(R) \quad \text{by} \quad \operatorname{Spec}(\varphi)(\mathfrak{p}') := \varphi^{-1}(\mathfrak{p}').$$

Clearly, $\operatorname{Spec}(\varphi)^{-1}\,\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{a}R')$; hence, $\operatorname{Spec}(\varphi)$ is continuous. Thus $\operatorname{Spec}(\bullet)$ is a contravariant functor from ((Rings)) to ((Top spaces)).

For example, the quotient map $R \to R/\mathfrak{a}$ induces a closed embedding

$$\operatorname{Spec}(R/\mathfrak{a}) \hookrightarrow \operatorname{Spec}(R),$$

whose image is $\mathbf{V}(\mathfrak{a})$, owing to **(1.7)** and **(2.8)**. Furthermore, the localization map $R \to R_f$ induces an open embedding

$$\operatorname{Spec}(R_f) \hookrightarrow \operatorname{Spec}(R),$$

whose image is $\mathbf{D}(f)$, owing to **(11.16)**.

Exercise **(13.2)**. — Let R be a ring, $\mathfrak{p} \in \operatorname{Spec}(R)$. Show that $\mathfrak{p}$ is a closed point — that is, $\{\mathfrak{p}\}$ is a closed set — if and only if $\mathfrak{p}$ is a maximal ideal.

Proposition **(13.3)**. — *Let R be a ring, $X := \operatorname{Spec}(R)$. Then X is **quasi-compact:** if $X = \bigcup_{\lambda\in\Lambda} U_\lambda$ with U_λ open, then $X = \bigcup_{i=1}^{n} U_{\lambda_i}$ for some $\lambda_i \in \Lambda$.*

Proof: Say $U_\lambda = X - \mathbf{V}(\mathfrak{a}_\lambda)$. Then $\mathbf{V}\big(\sum \mathfrak{a}_\lambda\big) = \bigcap \mathbf{V}(\mathfrak{a}_\lambda) = \emptyset$. So $\sum \mathfrak{a}_\lambda$ lies in no prime ideal. Hence there are $\lambda_1, \dots, \lambda_n \in \Lambda$ and $f_{\lambda_i} \in \mathfrak{a}_{\lambda_i}$ for all i with

$\sum f_{\lambda_i} = 1$. Hence $\sum \mathfrak{a}_{\lambda_i} = R$; so $\mathbf{V}\big(\sum \mathfrak{a}_{\lambda_i}\big) = \bigcap \mathbf{V}(\mathfrak{a}_{\lambda_i}) = \emptyset$; so $X = \bigcup U_{\lambda_i}$. □

Exercise **(13.4)**. — Let R be a ring, $X := \operatorname{Spec}(R)$, and U an open subset. Show U is quasi-compact if and only if $X - U = V(\mathfrak{a})$ where $\mathfrak{a}$ is finitely generated.

Definition **(13.5)**. — Let R be a ring, M a module. Its **support** is the set

$$\operatorname{Supp}(M) := \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0 \,\}.$$

Proposition **(13.6)**. — *Let R be a ring, M a module.*

(1) *Let $0 \to L \to M \to N \to 0$ be exact. Then $\operatorname{Supp}(L) \cup \operatorname{Supp}(N) = \operatorname{Supp}(M)$.*
(2) *Let M_λ be submodules with $\sum M_\lambda = M$. Then $\bigcup \operatorname{Supp}(M_\lambda) = \operatorname{Supp}(M)$.*
(3) *Then $\operatorname{Supp}(M) \subset \boldsymbol{V}(\operatorname{Ann}(M))$, with equality if M is finitely generated.*

Proof: Consider (1). For every prime $\mathfrak{p}$, the sequence $0 \to L_{\mathfrak{p}} \to M_{\mathfrak{p}} \to N_{\mathfrak{p}} \to 0$ is exact by **(12.16)**. Hence $M_{\mathfrak{p}} \neq 0$ if and only if $L_{\mathfrak{p}} \neq 0$ or $N_{\mathfrak{p}} \neq 0$. Thus (1) holds.

In (2), $M_\lambda \subset M$. So (1) yields $\bigcup \operatorname{Supp}(M_\lambda) \subset \operatorname{Supp}(M)$. To prove the opposite inclusion, take $\mathfrak{p} \notin \bigcup \operatorname{Supp}(M_\lambda)$. Then $(M_\lambda)_{\mathfrak{p}} = 0$ for all λ. By hypothesis, the natural map $\bigoplus M_\lambda \to M$ is surjective. So $\bigoplus (M_\lambda)_{\mathfrak{p}} \to M_{\mathfrak{p}}$ is surjective by **(12.10)**. Hence $M_{\mathfrak{p}} = 0$. Alternatively, given $m/s \in M_{\mathfrak{p}}$, express m as a finite sum $m = \sum m_\lambda$ with $m_\lambda \in M_\lambda$. For each such λ, there is $t_\lambda \in R - \mathfrak{p}$ with $t_\lambda m_\lambda = 0$. Set $t := \prod t_\lambda$. Then $tm = 0$ and $t \notin \mathfrak{p}$. So $m/s = 0$ in $M_{\mathfrak{p}}$. Hence again, $M_{\mathfrak{p}} = 0$. Thus $\mathfrak{p} \notin \operatorname{Supp}(M)$, and so (2) holds.

Consider (3). Let $\mathfrak{p}$ be a prime. By **(12.7)**, $M_{\mathfrak{p}} = 0$ if $\operatorname{Ann}(M) \cap (R - \mathfrak{p}) \neq \emptyset$, and the converse holds if M is finitely generated. But $\operatorname{Ann}(M) \cap (R - \mathfrak{p}) \neq \emptyset$ if and only if $\operatorname{Ann}(M) \not\subset \mathfrak{p}$. The assertion follows directly. □

Definition **(13.7)**. — Let R be a ring, M a module, $x \in R$. We say x is **nilpotent** on M if there is $n \geq 1$ with $x^n m = 0$ for all $m \in M$, that is, if $x \in \sqrt{\operatorname{Ann}(M)}$. We denote the set of nilpotents by $\operatorname{nil}(M)$; that is, $\operatorname{nil}(M) := \sqrt{\operatorname{Ann}(M)}$.

Proposition **(13.8)**. — *Let R be a ring, M a finitely generated module. Then*

$$\operatorname{nil}(M) = \textstyle\bigcap_{\mathfrak{p} \in \operatorname{Supp}(M)} \mathfrak{p}.$$

Proof: First, $\operatorname{nil}(M) = \bigcap_{\mathfrak{p} \supset \operatorname{Ann}(M)} \mathfrak{p}$ by the Scheinnullstellensatz **(3.17)**. But $\mathfrak{p} \supset \operatorname{Ann}(M)$ if and only if $\mathfrak{p} \in \operatorname{Supp}(M)$ by **(13.6)**(3). □

Proposition **(13.9)**. — *Let R be a ring, M and N modules. Then*

$$\operatorname{Supp}(M \otimes_R N) \subset \operatorname{Supp}(M) \cap \operatorname{Supp}(N), \qquad \textbf{(13.9.1)}$$

with equality if M and N are finitely generated.

Proof: First, $(M \otimes_R N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}}$ by **(12.13)**; whence, **(13.9.1)** holds. The opposite inclusion follows from **(10.11)** if M and N are finitely generated. □

Corollary **(13.10)**. — *Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Then*

$$\operatorname{Supp}(M/\mathfrak{a}M) \subset \operatorname{Supp}(M) \cap \boldsymbol{V}(\mathfrak{a}).$$

with equality if M is finitely generated.

Proof: First, **(8.13)**(1) yields $M/\mathfrak{a}M = M \otimes R/\mathfrak{a}$. But $\operatorname{Ann}(R/\mathfrak{a}) = \mathfrak{a}$; hence **(13.6)**(3) yields $\operatorname{Supp}(R/\mathfrak{a}) = \mathbf{V}(\mathfrak{a})$. Thus **(13.9)** yields the assertion. □

EXERCISE **(13.11)**. — Let R be a ring, M a module, $\mathfrak{p} \in \operatorname{Supp}(M)$. Prove

$$\mathbf{V}(\mathfrak{p}) \subset \operatorname{Supp}(M).$$

EXERCISE **(13.12)**. — Let $\mathbb{Z}$ be the integers, $\mathbb{Q}$ the rational numbers, and set $M := \mathbb{Q}/\mathbb{Z}$. Find $\operatorname{Supp}(M)$, and show that it is not Zariski closed.

PROPOSITION **(13.13)**. — *Let R be a ring, M a module. These conditions are equivalent:* (1) $M = 0$*;* (2) $\operatorname{Supp}(M) = \emptyset$*;* (3) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m}$.

PROOF: Trivially, if (1) holds, then $S^{-1}M = 0$ for any multiplicative set S. In particular, (2) holds. Trivially, (2) implies (3).

Finally, assume $M \neq 0$, and take a nonzero $m \in M$, and set $\mathfrak{a} := \operatorname{Ann}(m)$. Then $1 \notin \mathfrak{a}$, so $\mathfrak{a}$ lies in some maximal ideal $\mathfrak{m}$. Then, for all $f \in R - \mathfrak{m}$, we have $fm \neq 0$. Hence $m/1 \neq 0$ in $M_{\mathfrak{m}}$. Thus (3) implies (1). □

EXERCISE **(13.14)**. — Let R be a ring, P a module, and M, N submodules. Show $M = N$ if $M_{\mathfrak{m}} = N_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. First assume $M \subset N$.

EXERCISE **(13.15)**. — Prove these three conditions on a ring R are equivalent:

(1) R is reduced.
(2) $S^{-1}R$ is reduced for all multiplicatively closed sets S.
(3) $R_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$.

EXERCISE **(13.16)**. — Let R be a ring, Σ the set of minimal primes. Prove this:

(1) If $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$, then the $\mathfrak{p} \in \Sigma$ are pairwise comaximal.
(2) $R = \prod_{i=1}^{n} R_i$ where R_i is a domain if and only if $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$ and Σ is finite. If so, then $R_i = R/\mathfrak{p}_i$ with $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \Sigma$.

PROPOSITION **(13.17)**. — *A sequence of modules $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is exact if and only if its localization $L_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} M_{\mathfrak{m}} \xrightarrow{\beta_{\mathfrak{m}}} N_{\mathfrak{m}}$ is exact at each maximal ideal* $\mathfrak{m}$.

PROOF: If the sequence is exact, then so is its localization by **(12.16)**.

Consider the converse. First $\operatorname{Im}(\beta_{\mathfrak{m}}\alpha_{\mathfrak{m}}) = 0$. But $\operatorname{Im}(\beta_{\mathfrak{m}}\alpha_{\mathfrak{m}}) = \big(\operatorname{Im}(\beta\alpha)\big)_{\mathfrak{m}}$ by **(12.16)** and **(9.3)**. Hence $\operatorname{Im}(\beta\alpha) = 0$ by **(13.13)**. So $\beta\alpha = 0$. Thus $\operatorname{Im}(\alpha) \subset \operatorname{Ker}(\beta)$.

Set $H := \operatorname{Ker}(\beta)/\operatorname{Im}(\alpha)$. Then $H_{\mathfrak{m}} = \operatorname{Ker}(\beta_{\mathfrak{m}})/\operatorname{Im}(\alpha_{\mathfrak{m}})$ by **(12.16)** and **(9.3)**. So $H_{\mathfrak{m}} = 0$ owing to the hypothesis. Hence $H = 0$ by **(13.13)**, as required. □

EXERCISE **(13.18)**. — Let R be a ring, M a module. Prove elements $m_\lambda \in M$ generate M if and only if, at every maximal ideal $\mathfrak{m}$, their images m_λ generate $M_{\mathfrak{m}}$.

PROPOSITION **(13.19)**. — *Let R be a ring, S a multiplicative set, M a module. Then the following conditions are equivalent:*

(1) *M is flat over R.*
(2) *$S^{-1}M$ is flat over $S^{-1}R$ and over R.*
(3) *At every maximal ideal $\mathfrak{m}$, the localization $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$.*

PROOF: Assume (1) holds. Let $\alpha\colon N' \to N$ be an injection of $S^{-1}R$-modules. Then $M \otimes_R \alpha\colon M \otimes_R N' \to M \otimes_R N$ is injective. Now, **(12.4)** yields $\alpha = S^{-1}\alpha$. So **(12.13)** yields $M \otimes_R \alpha = S^{-1}M \otimes_{S^{-1}R} \alpha$. Hence $S^{-1}M \otimes_{S^{-1}R} \alpha$ is injective; that is, $S^{-1}M$ is flat over $S^{-1}R$. Therefore, $S^{-1}M$ is flat over R by **(12.17)** and **(9.7)**. Thus (2) holds. Trivially, (2) implies (3).

Assume (3) holds. Let $\alpha\colon N' \to N$ be an injection of R-modules. Then $\alpha_{\mathfrak{m}}$

is injective by **(13.17)**. So $M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} \alpha_{\mathfrak{m}}$ is injective. Now, that map is equal to $(M \otimes \alpha)_{\mathfrak{m}}$ by **(12.13)**, hence is injective. Therefore, $M \otimes \alpha$ is injective by **(13.17)**; that is, (1) holds. □

Definition **(13.20)**. — Let R be a ring, M a module. We say M is **locally finitely generated** if each $\mathfrak{p} \in \operatorname{Spec}(R)$ has a neighborhood on which M becomes finitely generated; more precisely, there exists $f \in R - \mathfrak{p}$ such that M_f is finitely generated over R_f. Similarly, we define the properties **locally finitely presented**, **locally free of finite rank**, and **locally free of rank** n.

Proposition **(13.21)**. — *Let R be a ring, M a module.*

(1) *If M is locally finitely generated, then it is finitely generated.*
(2) *If M is locally finitely presented, then it is finitely presented.*

Proof: By **(13.3)**, there are $f_1, \dots, f_n \in R$ with $\bigcup \mathbf{D}(f_i) = \operatorname{Spec}(R)$ and finitely many $m_{i,j} \in M$ such that, for some $n_{i,j} \geq 0$, the $m_{i,j}/f_i^{n_{i,j}}$ generate M_{f_i}. Clearly, for each i, the $m_{i,j}/1$ also generate M_{f_i}.

Given any maximal ideal $\mathfrak{m}$, there is i such that $f_i \notin \mathfrak{m}$. Let S_1 be the image of $R - \mathfrak{m}$ in R_{f_i}. Then **(12.5)** yields $M_{\mathfrak{m}} = S_1^{-1}(M_{f_i})$. Hence the $m_{i,j}/1$ generate $M_{\mathfrak{m}}$. Thus **(13.18)** yields (1).

Assume M is locally finitely presented. Then M is finitely generated by (1). So there is a surjection $R^k \twoheadrightarrow M$. Let K be its kernel. Then K is locally finitely generated owing to **(5.24)**. Hence K too is finitely generated by (1). So there is a surjection $R^\ell \twoheadrightarrow K$. It yields the desired finite presentation $R^\ell \to R^k \to M \to 0$. Thus (2) holds. □

Theorem **(13.22)**. — *These conditions on an R-module P are equivalent:*

(1) *P is finitely generated and projective.*
(2) *P is finitely presented and flat.*
(3) *P is finitely presented, and $P_{\mathfrak{m}}$ is free over $R_{\mathfrak{m}}$ at each maximal ideal $\mathfrak{m}$.*
(4) *P is locally free of finite rank.*
(5) *P is finitely generated, and for each $\mathfrak{p} \in \operatorname{Spec}(R)$, there are f and n such that $\mathfrak{p} \in \boldsymbol{D}(f)$ and $P_{\mathfrak{q}}$ is free of rank n over $R_{\mathfrak{q}}$ at each $\mathfrak{q} \in \boldsymbol{D}(f)$.*

Proof: Condition (1) implies (2) by **(10.12)**.

Let $\mathfrak{m}$ be a maximal ideal. Then $R_{\mathfrak{m}}$ is local by **(11.18)**. If P is finitely presented, then $P_{\mathfrak{m}}$ is finitely presented, because localization preserves direct sums and cokernels by **(12.10)**.

Assume (2). Then $P_{\mathfrak{m}}$ is flat by **(13.19)**, so free by **(10.12)**. Thus (3) holds.

Assume (3). Fix a surjective map $\alpha\colon M \to N$. Then $\alpha_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective. So $\operatorname{Hom}(P_{\mathfrak{m}}, \alpha_{\mathfrak{m}})\colon \operatorname{Hom}(P_{\mathfrak{m}}, M_{\mathfrak{m}}) \to \operatorname{Hom}(P_{\mathfrak{m}}, N_{\mathfrak{m}})$ is surjective by **(5.22)** and **(5.21)**. But $\operatorname{Hom}(P_{\mathfrak{m}}, \alpha_{\mathfrak{m}}) = \operatorname{Hom}(P, \alpha)_{\mathfrak{m}}$ by **(12.21)** as P is finitely presented. Further, $\mathfrak{m}$ is arbitrary. Hence $\operatorname{Hom}(P, \alpha)$ is surjective by **(13.17)**. Therefore, P is projective by **(5.22)**. Thus (1) holds.

Again assume (3). Given any prime $\mathfrak{p}$, take a maximal ideal $\mathfrak{m}$ containing it. By hypothesis, $P_{\mathfrak{m}}$ is free; its rank is finite as $P_{\mathfrak{m}}$ is finitely generated. By **(12.20)**(2), there is $f \in R - \mathfrak{m}$ such that P_f is free of finite rank over R_f. Thus (4) holds.

Assume (4). Then P is locally finitely presented. So P is finitely presented by **(13.21)**(2). Further, given $\mathfrak{p} \in \operatorname{Spec}(R)$, there are $f \in R - \mathfrak{p}$ and n such that M_f is locally free of rank n over R_f. Given $\mathfrak{q} \in \mathbf{D}(f)$, let S_1 be the image of $R - \mathfrak{q}$ in R_f. Then **(12.5)** yields $M_{\mathfrak{q}} = S_1^{-1}(M_f)$. Hence $M_{\mathfrak{q}}$ is locally free of rank n over

$R_{\mathfrak{q}}$. Thus (5) holds. Further, (3) results from taking $\mathfrak{p} := \mathfrak{m}$ and $\mathfrak{q} := \mathfrak{m}$.

Finally, assume (5), and let's prove (4). Given $\mathfrak{p} \in \operatorname{Spec}(R)$, let f and n be provided by (5). Take a free basis $p_1/f^{k_1}, \dots, p_n/f^{k_n}$ of $P_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$. The p_i define a map $\alpha\colon R^n \to P$, and $\alpha_{\mathfrak{p}}\colon R^n_{\mathfrak{p}} \to P_{\mathfrak{p}}$ is bijective, in particular, surjective.

As P is finitely generated, **(12.20)**(1) provides $g \in R - \mathfrak{p}$ such that $\alpha_g\colon R^n_g \to P_g$ is surjective. It follows that $\alpha_{\mathfrak{q}}\colon R^n_{\mathfrak{q}} \to P_{\mathfrak{q}}$ is surjective for every $\mathfrak{q} \in \mathbf{D}(g)$. If also $\mathfrak{q} \in \mathbf{D}(f)$, then by hypothesis $P_{\mathfrak{q}} \simeq R^n_{\mathfrak{q}}$. So $\alpha_{\mathfrak{q}}$ is bijective by **(10.4)**.

Set $h := fg$. Clearly, $\mathbf{D}(f) \cap \mathbf{D}(g) = \mathbf{D}(h)$. By **(13.1)**, $\mathbf{D}(h) = \operatorname{Spec}(R_h)$. Clearly, $\alpha_{\mathfrak{q}} = (\alpha_h)_{(\mathfrak{q}R_h)}$ for all $\mathfrak{q} \in \mathbf{D}(h)$. Hence $\alpha_h\colon R^n_h \to P_h$ is bijective owing to **(13.17)** with R_h for R. Thus (4) holds. □

Exercise **(13.23)**. — Given n, prove an R-module P is locally free of rank n if and only if P is finitely generated and $P_{\mathfrak{m}} \simeq R^n_{\mathfrak{m}}$ holds at each maximal ideal $\mathfrak{m}$.

14. Krull–Cohen–Seidenberg Theory

Krull–Cohen–Seidenberg Theory relates the prime ideals in a ring to those in an integral extension. We prove each prime has at least one prime lying over it — that is, contracting to it. The overprime can be taken to contain any ideal that contracts to an ideal contained in the given prime; this stronger statement is known as the Going-up Theorem. Further, one prime is maximal if and only if the other is, and two overprimes cannot be nested. On the other hand, the Going-down Theorem asserts that, given nested primes in the subring and a prime lying over the larger, there is a subprime lying over the smaller, either if the subring is normal and the overring is a domain or if the extension is flat even if it's not integral.

LEMMA **(14.1)**. — *Let $R \subset R'$ be an integral extension of domains. Then R' is a field if and only if R is.*

PROOF: First, suppose R' is a field. Let $x \in R$ be nonzero. Then $1/x \in R'$, so satisfies an equation of integral dependence:

$$(1/x)^n + a_1(1/x)^{n-1} + \cdots + a_n = 0$$

with $n \geq 1$ and $a_i \in R$. Multiplying the equation by x^{n-1}, we obtain

$$1/x = -(a_1 + a_{n-2}x + \cdots + a_n x^{n-1}) \in R.$$

Conversely, suppose R is a field. Let $y \in R'$ be nonzero. Then y satisfies an equation of integral dependence

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

with $n \geq 1$ and $a_i \in R$. Rewriting the equation, we obtain

$$y(y^{n-1} + \cdots + a_{n-1}) = -a_n.$$

Take n minimal. Then $a_n \neq 0$ as R' is a domain. So dividing by $-a_n y$, we obtain

$$1/y = (-1/a_n)(y^{n-1} + \cdots + a_{n-1}) \in R'. \qquad \square$$

DEFINITION **(14.2)**. — Let R be a ring, R' an R-algebra, $\mathfrak{p}$ a prime of R, and $\mathfrak{p}'$ a prime of R'. We say $\mathfrak{p}'$ **lies over** $\mathfrak{p}$ if $\mathfrak{p}'$ contracts to $\mathfrak{p}$.

THEOREM **(14.3)**. — *Let $R \subset R'$ be an integral extension of rings, and $\mathfrak{p}$ a prime of R. Let $\mathfrak{p}' \subset \mathfrak{q}'$ be nested primes of R', and $\mathfrak{a}'$ an arbitrary ideal of R'.*

(1) (Maximality) *Suppose $\mathfrak{p}'$ lies over $\mathfrak{p}$. Then $\mathfrak{p}'$ is maximal if and only if $\mathfrak{p}$ is.*
(2) (Incomparability) *Suppose both $\mathfrak{p}'$ and $\mathfrak{q}'$ lie over $\mathfrak{p}$. Then $\mathfrak{p}' = \mathfrak{q}'$.*
(3) (Lying over) *Then there is a prime $\mathfrak{r}'$ of R' lying over $\mathfrak{p}$.*
(4) (Going up) *Suppose $\mathfrak{a}' \cap R \subset \mathfrak{p}$. Then in* (3) *we can take $\mathfrak{r}'$ to contain $\mathfrak{a}'$.*

PROOF: Assertion (1) follows from **(14.1)** applied to the extension $R/\mathfrak{p} \subset R'/\mathfrak{p}'$, which is integral as $R \subset R'$ is, since, if $y \in R'$ satisfies $y^n + a_1 y^{n-1} + \cdots + a_n = 0$, then reduction modulo $\mathfrak{p}'$ yields an equation of integral dependence over $R/\mathfrak{p}$.

To prove (2), localize at $R - \mathfrak{p}$, and form this commutative diagram:

$$\begin{array}{ccc} R' & \to & R'_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ R & \to & R_{\mathfrak{p}} \end{array}$$

Here $R_\mathfrak{p} \to R'_\mathfrak{p}$ is injective by **(12.15)**(1), and the extension is integral by **(11.20)**.

Here $\mathfrak{p}'R'_\mathfrak{p}$ and $\mathfrak{q}'R'_\mathfrak{p}$ are nested primes of $R'_\mathfrak{p}$ by **(11.16)**(2). By the same token, both lie over $\mathfrak{p}R_\mathfrak{p}$, because both their contractions in $R_\mathfrak{p}$ contract to $\mathfrak{p}$ in R. Thus we may replace R by $R_\mathfrak{p}$ and R' by $R'_\mathfrak{p}$, and so assume R is local with $\mathfrak{p}$ as maximal ideal by **(11.18)**. Then $\mathfrak{p}'$ is maximal by (1); whence, $\mathfrak{p}' = \mathfrak{q}'$.

To prove (3), again we may replace R by $R_\mathfrak{p}$ and R' by $R'_\mathfrak{p}$: if $\mathfrak{r}''$ is a prime ideal of $R'_\mathfrak{p}$ lying over $\mathfrak{p}R_\mathfrak{p}$, then the contraction $\mathfrak{r}'$ of $\mathfrak{r}''$ in R' lies over $\mathfrak{p}$. So we may assume R is local with $\mathfrak{p}$ as unique maximal ideal. Now, R' has a maximal ideal $\mathfrak{r}'$ by 2.25; further, $\mathfrak{r}'$ contracts to a maximal ideal $\mathfrak{r}$ of R by (1). Thus $\mathfrak{r} = \mathfrak{p}$.

Finally, (4) follows from (3) applied to the extension $R/(\mathfrak{a}' \cap R) \subset R'/\mathfrak{a}'$. □

EXERCISE **(14.4)**. — Let $R \subset R'$ be an integral extension of rings, and $\mathfrak{p}$ a prime of R. Suppose R' has just one prime $\mathfrak{p}'$ over $\mathfrak{p}$. Show (a) that $\mathfrak{p}'R'_\mathfrak{p}$ is the only maximal ideal of $R'_\mathfrak{p}$, (b) that $R'_{\mathfrak{p}'} = R'_\mathfrak{p}$, and (c) that $R'_{\mathfrak{p}'}$ is integral over $R_\mathfrak{p}$.

EXERCISE **(14.5)**. — Let $R \subset R'$ be an integral extension of domains, and $\mathfrak{p}$ a prime of R. Suppose R' has at least two distinct primes $\mathfrak{p}'$ and $\mathfrak{q}'$ lying over $\mathfrak{p}$. Show that $R'_{\mathfrak{p}'}$ is not integral over $R_\mathfrak{p}$. Show that, in fact, if y lies in $\mathfrak{q}'$, but not in $\mathfrak{p}'$, then $1/y \in R'_{\mathfrak{p}'}$ is not integral over $R_\mathfrak{p}$.

EXERCISE **(14.6)**. — Let k be a field, and X an indeterminate. Set $R' := k[X]$, and $Y := X^2$, and $R := k[Y]$. Set $\mathfrak{p} := (Y-1)R$ and $\mathfrak{p}' := (X-1)R'$. Is $R'_{\mathfrak{p}'}$ integral over $R_\mathfrak{p}$? Explain.

LEMMA **(14.7)**. — *Let $R \subset R'$ be a ring extension, X a variable, $f \in R[X]$ a monic polynomial. Suppose $f = gh$ with g, $h \in R'[X]$ monic. Then the coefficients of g and h are integral over R.*

PROOF: Set $R_1 := R'[X]/\langle g \rangle$. Let x_1 be the residue of X. Then 1, x_1, $x_1^2, \dots$ form a free basis of R_1 over R' by **(10.17)** as g is monic; hence, $R' \subset R_1$. Now, $g(x_1) = 0$; so g factors as $(X - x_1)g_1$ with $g_1 \in R_1[X]$ monic of degree 1 less than g. Repeat this process, extending R_1. Continuing, obtain $g(X) = \prod(X - x_i)$ and $h(X) = \prod(X - y_j)$ with all x_i and y_j in an extension of R'. The x_i and y_j are integral over R as they are roots of f. But the coefficients of g and h are polynomials in the x_i and y_j; so they too are integral over R. □

PROPOSITION **(14.8)**. — *Let R be a normal domain, $K := \mathrm{Frac}(R)$, and L/K a field extension. Let $y \in L$ be integral over R, and $p \in K[X]$ its monic minimal polynomial. Then $p \in R[X]$, and so $p(y) = 0$ is an equation of integral dependence.*

PROOF: Since y is integral, there is a monic polynomial $f \in R[X]$ with $f(y) = 0$. Write $f = pq$ with $q \in K[X]$. Then by **(14.7)** the coefficients of p are integral over R, so in R since R is normal. □

THEOREM **(14.9)** (Going down for integral extensions). — *Let $R \subset R'$ be an integral extension of domains, $\mathfrak{p} \subsetneqq \mathfrak{q}$ nested primes of R, and $\mathfrak{q}'$ a prime of R' lying over $\mathfrak{q}$. If R is normal, then there is a prime $\mathfrak{p}'$ lying over $\mathfrak{p}$ and contained in $\mathfrak{q}'$.*

PROOF: First, let us show $\mathfrak{p}R'_{\mathfrak{q}'} \cap R = \mathfrak{p}$. Take $y \in \mathfrak{p}R'_{\mathfrak{q}'} \cap R$. Say $y = x/s$ with $x \in \mathfrak{p}R'$ and $s \in R' - \mathfrak{q}'$. Say $x = \sum_{i=1}^m y_i x_i$ with $y_i \in \mathfrak{p}$ and $x_i \in R'$, and set $R'' := R[x_1, \dots, x_m]$. Then R'' is a finite R-module by **(10.20)** and $xR'' \subset \mathfrak{p}R''$. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be the characteristic polynomial of $\mu_x \colon R'' \to$

R''. Then $a_i \in \mathfrak{p}^i \subset \mathfrak{p}$ by **(10.1)**, and $f(x) = 0$ by the Determinant Trick **(10.2)**.

Set $K := \operatorname{Frac}(R)$. Suppose $f = gh$ with $g, h \in K[X]$ monic. By **(14.7)** the coefficients of g, h lie in R as R is normal. Further, $f \equiv X^n \pmod{\mathfrak{p}}$. So $g \equiv X^r \pmod{\mathfrak{p}}$ and $h \equiv X^{n-r} \pmod{\mathfrak{p}}$ for some r by unique factorization in $\operatorname{Frac}(R/\mathfrak{p})[X]$. Hence g and h have all nonleading coefficients in $\mathfrak{p}$. Replace f by a monic factor of minimal degree. Then f is the minimal polynomial of x over K.

Recall $s = x/y$. So s satisfies the equation

$$s^n + b_1 s^{n-1} + \cdots + b_n = 0 \quad \text{with} \quad b_i := a_i/y^i \in K.$$

This equation is of minimal degree since $y \in R \subset K$ and $\deg(f)$ is minimal for x. But s is integral over R. So all b_i are in R by **(14.8)**.

Assume $y \notin \mathfrak{p}$. Then $b_i \in \mathfrak{p}$ since $a_i = b_i y^i \in \mathfrak{p}$. So $s^n \in \mathfrak{p}R' \subset \mathfrak{q}R' \subset \mathfrak{q}'$. So $s \in \mathfrak{q}'$, a contradiction. Hence $y \in \mathfrak{p}$. Thus $\mathfrak{p}R'_{\mathfrak{q}'} \cap R \subset \mathfrak{p}$. But the opposite inclusion holds trivially. Thus $\mathfrak{p}R'_{\mathfrak{q}'} \cap R = \mathfrak{p}$.

Hence, there is a prime $\mathfrak{p}''$ of $R'_{\mathfrak{q}'}$ with $\mathfrak{p}'' \cap R = \mathfrak{p}$ by **(3.10)**. Set $\mathfrak{p}' := \mathfrak{p}'' \cap R'$. Then $\mathfrak{p}' \cap R = \mathfrak{p}$, and $\mathfrak{p}' \subset \mathfrak{q}'$ by **(11.16)**(2), as desired. □

Lemma **(14.10)**. — *Always, a minimal prime consists entirely of zerodivisors.*

Proof: Let R be the ring, $\mathfrak{p}$ the minimal prime. Then $R_{\mathfrak{p}}$ has only one prime $\mathfrak{p}R_{\mathfrak{p}}$ by **(11.16)**(2). So by the Scheinnullstellensatz, $\mathfrak{p}R_{\mathfrak{p}}$ consists entirely of nilpotents. Hence, given $x \in \mathfrak{p}$, there is $s \in R - \mathfrak{p}$ with $sx^n = 0$ for some $n \geq 1$. Take n minimal. Then $sx^{n-1} \neq 0$, but $(sx^{n-1})x = 0$. Thus x is a zerodivisor. □

Theorem **(14.11)** (Going down for flat algebra). — *Let R be a ring, R' a flat algebra. Let $\mathfrak{p} \subsetneqq \mathfrak{q}$ be nested primes of R, and $\mathfrak{q}'$ a prime of R' lying over $\mathfrak{q}$. Then there is a prime $\mathfrak{p}'$ of R' that lies over $\mathfrak{p}$ and is contained in $\mathfrak{q}'$.*

Proof: By **(9.8)**, $R' \otimes_R (R/\mathfrak{p})$ is flat over $R/\mathfrak{p}$. Further, $R'/\mathfrak{p}R' = R' \otimes_R R/\mathfrak{p}$ by **(8.13)**(1). Hence, owing to **(1.7)**, we may replace R by $R/\mathfrak{p}$ and R' by $R'/\mathfrak{p}R'$, and thus assume R is a domain and $\mathfrak{p} = 0$.

By **(3.11)**, $\mathfrak{q}'$ contains a minimal prime $\mathfrak{p}'$ of R'. Let's show that $\mathfrak{p}'$ lies over $\langle 0 \rangle$. Let $x \in R$ be nonzero. Then the multiplication map $\mu_x \colon R \to R$ is injective. Since R' is flat, $\mu_x \colon R' \to R'$ is also injective. Hence, **(14.10)** implies that x does not belong to the contraction of $\mathfrak{p}'$, as desired. □

Exercise **(14.12)**. — Let R be a reduced ring, Σ the set of minimal primes. Prove that $\operatorname{z.div}(R) = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$ and that $R_{\mathfrak{p}} = \operatorname{Frac}(R/\mathfrak{p})$ for any $\mathfrak{p} \in \Sigma$.

Exercise **(14.13)**. — Let R be a ring, Σ the set of minimal primes, and K the total quotient ring. Assume Σ is finite. Prove these three conditions are equivalent:

(1) R is reduced.
(2) $\operatorname{z.div}(R) = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$, and $R_{\mathfrak{p}} = \operatorname{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$.
(3) $K/\mathfrak{p}K = \operatorname{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$, and $K = \prod_{\mathfrak{p} \in \Sigma} K/\mathfrak{p}K$.

(14.14) (*Arbitrary normal rings*). — An arbitrary ring R is said to be **normal** if $R_{\mathfrak{p}}$ is a normal domain for every prime $\mathfrak{p}$. If R is a domain, then this definition recovers that in **(10.21)**, owing to **(11.28)**.

Exercise **(14.15)**. — Let R be a ring, $\mathfrak{p}_1 \ldots, \mathfrak{p}_r$ all its minimal primes, and K the total quotient ring. Prove that these three conditions are equivalent:

(1) R is normal.

(2) R is reduced and integrally closed in K.
(3) R is a finite product of normal domains R_i.

Assume the conditions hold. Prove the R_i are equal to the $R/\mathfrak{p}_j$ in some order.

15. Noether Normalization

The Noether Normalization Lemma describes the basic structure of a finitely generated algebra over a field; namely, given a chain of ideals, there is a polynomial subring over which the algebra is module finite, and the ideals contract to ideals generated by initial segments of variables. After proving this lemma, we derive several versions of the Nullstellensatz. The most famous is Hilbert's; namely, the radical of any ideal is the intersection of all the maximal ideals containing it.

Then we study the (Krull) dimension: the maximal length of any chain of primes. We prove our algebra is catenary; that is, if two chains have the same ends and maximal lengths, then the lengths are the same. Further, if the algebra is a domain, then its dimension is equal to the transcendence degree of its fraction field.

In an appendix, we give a simple direct proof of the Hilbert Nullstellensatz. At the same time, we prove it in significantly greater generality: for Jacobson rings.

LEMMA **(15.1)** (Noether Normalization). — *Let k be a field, $R := k[x_1, \dots, x_n]$ a finitely generated k-algebra, and $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_r$ a chain of proper ideals of R. Then there are algebraically independent elements $t_1, \dots, t_\nu \in R$ such that*

(1) *R is module finite over $P := k[t_1, \dots t_\nu]$ and*
(2) *for $i = 1, \cdots, r$, there is an h_i such that $\mathfrak{a}_i \cap P = \langle t_1, \dots, t_{h_i} \rangle$.*

If k is infinite, then we may choose the t_i to be k-linear combinations of the x_i.

PROOF: Let $R' := k[X_1, \dots, X_n]$ be the polynomial ring, and $\varphi\colon R' \to R$ the k-algebra map with $\varphi X_i := x_i$. Set $\mathfrak{a}'_0 := \operatorname{Ker}\varphi$ and $\mathfrak{a}'_i := \varphi^{-1}\mathfrak{a}_i$ for $i = 1, \cdots, r$. It suffices to prove the lemma for R' and $\mathfrak{a}'_0 \subset \cdots \subset \mathfrak{a}'_r$: if $t'_i \in R'$ and h'_i work here, then $t_i := \varphi t'_{i+h'_0}$ and $h_i := h'_i - h'_0$ work for R and the $\mathfrak{a}_i$, because the t_i are algebraically independent by **(1.8)**, and clearly (1) and (2) hold. Thus we may assume the x_i are algebraically independent.

The proof proceeds by induction on r (and shows $\nu := n$ works now).

First, assume $r = 1$ and $\mathfrak{a}_1 = t_1 R$ for some nonzero t_1. Then $t_1 \notin k$ because $\mathfrak{a}_1$ is proper. Suppose we have found $t_2, \dots, t_n \in R$ so that x_1 is integral over $P := k[t_1, t_2, \dots, t_n]$ and so that $P[x_1] = R$. Then **(10.20)** yields (1).

Further, by the theory of transcendence bases [1, (8.3), p. 526], [6, Thm. 1.1, p. 356], the elements $t_1, \dots, t_n$ are algebraically independent. Now, take $x \in \mathfrak{a}_1 \cap P$. Then $x = t_1 x'$ where $x' \in R \cap \operatorname{Frac}(P)$. Further, $R \cap \operatorname{Frac}(P) = P$ because P is normal by **(10.26)** as P is a polynomial algebra. Hence $\mathfrak{a}_1 \cap P = t_1 P$. Thus (2) holds too.

To find $t_2, \dots, t_n$, we are going to choose ℓ_i and set $t_i := x_i - x_1^{\ell_i}$. Then clearly $P[x_1] = R$. Now, say $t_1 = \sum a_{(j)} x_1^{j_1} \cdots x_n^{j_n}$ with $(j) := (j_1, \dots, j_n)$ and $a_{(j)} \in k$. Recall $t_1 \notin k$, and note that x_1 satisfies this equation:

$$\sum a_{(j)} x_1^{j_1} (t_2 + x_1^{\ell_2})^{j_2} \cdots (t_n + x_1^{\ell_n})^{j_n} = t_1.$$

Set $e(j) := j_1 + \ell_2 j_2 + \cdots + \ell_n j_n$. Take $\ell > \max\{j_i\}$ and $\ell_i := \ell^i$. Then the $e(j)$ are distinct. Let $e(j')$ be largest among the $e(j)$ with $a_{(j)} \neq 0$. Then $e(j') > 0$, and the above equation may be rewritten as follows:

$$a_{(j')} x_1^{e(j')} + \textstyle\sum_{e<e(j')} p_e x_1^e = 0$$

where $p_e \in P$. Thus x_1 is integral over P, as desired.

Suppose k is infinite. We are going to reorder the x_i, choose $a_i \in k$, and set $t_i := x_i - a_i x_1$. Then clearly $P[x_1] = R$. Now, say $t_1 = H_d + \cdots + H_0$ where H_i is homogeneous of degree i in $x_1, \ldots, x_n$ and where $H_d \neq 0$. Then $d > 0$ as $t_1 \notin k$. Since k is infinite, we may reorder the x_i and take $a_i \in k$ with $H_d(1, a_2, \ldots, a_n) \neq 0$. Then $H_d(1, a_2, \ldots, a_n)$ is the coefficient of x_1^d in $H_d(x_1, t_2 + a_2 x_1, \ldots, t_n + a_n x_1)$. So after we collect like powers of x_1, the equation

$$H_d(x_1, t_2 + a_2 x_1, \ldots, t_n + a_n x_1) + \cdots + H_0(x_1, t_2 + a_2 x_1, \ldots, t_n + a_n x_1) + t_1 = 0$$

becomes an equation of integral dependence for x_1 over P, as desired.

Second, assume $r = 1$ and $\mathfrak{a}_1$ is arbitrary. We may assume $\mathfrak{a}_1 \neq 0$. The proof proceeds by induction on n. The case $n = 1$ follows from the first case (but is simpler) because $k[x_1]$ is a PID. Let $t_1 \in \mathfrak{a}_1$ be nonzero. By the first case, there exist elements $u_2, \ldots, u_n$ such that $t_1, u_2, \ldots u_n$ are algebraically independent and satisfy (1) and (2) with respect to R and $t_1 R$. By induction, there are $t_2, \ldots, t_n$ satisfying (1) and (2) with respect to $k[u_2, \ldots, u_n]$ and $\mathfrak{a}_1 \cap k[u_2, \ldots, u_n]$.

Set $P := k[t_1, \ldots, t_n]$. Since R is module finite over $k[t_1, u_2, \ldots, u_n]$ and the latter is module finite over P, the former is module finite over P by **(10.19)**. Thus (1) holds, and so $t_1, \ldots, t_n$ are algebraically independent. Further, by assumption,

$$\mathfrak{a}_1 \cap k[t_2, \ldots, t_n] = \langle t_2, \ldots, t_h \rangle$$

for some h. But $t_1 \in \mathfrak{a}_1$. So $\mathfrak{a}_1 \cap P \supset \langle t_1, \ldots, t_h \rangle$.

Conversely, given $x \in \mathfrak{a}_1 \cap P$, say $x = \sum_{i=0}^{d} f_i t_1^i$ with $f_i \in k[t_2, \ldots, t_n]$. Since $t_1 \in \mathfrak{a}_1$, we have $f_0 \in \mathfrak{a}_1 \cap k[t_2, \ldots, t_n]$; so $f_0 \in \langle t_2, \ldots, t_h \rangle$. Hence $x \in \langle t_1, \ldots, t_h \rangle$. Thus $\mathfrak{a}_1 \cap P = \langle t_1, \ldots, t_h \rangle$. Thus (2) holds for $r = 1$.

Finally, assume the lemma holds for $r - 1$. Let $u_1, \ldots, u_n \in R$ be algebraically independent elements satisfying (1) and (2) for the sequence $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_{r-1}$, and set $h := h_{r-1}$. By the second case, there exist elements $t_{h+1}, \ldots, t_n$ satisfying (1) and (2) for $k[u_{h+1}, \ldots, u_n]$ and $\mathfrak{a}_r \cap k[u_{h+1}, \ldots, u_n]$. Then, for some h_r,

$$\mathfrak{a}_r \cap k[t_{h+1}, \ldots, t_n] = \langle t_{h+1}, \ldots, t_{h_r} \rangle.$$

Set $t_i := u_i$ for $1 \leq i \leq h$. Set $P := k[t_1, \ldots, t_n]$. Then, by assumption, R is module finite over $k[u_1, \ldots, u_n]$, and $k[u_1, \ldots, u_n]$ is module finite over P; hence, R is module finite over P by **(10.19)**. Thus (1) holds, and $t_1, \ldots, t_n$ are algebraically independent over k.

Fix i with $1 \leq i \leq r$. Set $m := h_i$. Then $t_1, \ldots, t_m \in \mathfrak{a}_i$. Given $x \in \mathfrak{a}_i \cap P$, say $x = \sum f_{(v)} t_1^{v_1} \cdots t_m^{v_m}$ with $(v) = (v_1, \ldots, v_m)$ and $f_{(v)} \in k[t_{m+1}, \ldots, t_n]$. Then $f_{(0)}$ lies in $\mathfrak{a}_i \cap k[t_{m+1}, \ldots, t_n]$. We are going to see the latter intersection is equal to $\langle 0 \rangle$. It is so if $i \leq r - 1$ because it lies in $\mathfrak{a}_i \cap k[u_{m+1}, \ldots, u_n]$, which is equal to $\langle 0 \rangle$. Further, if $i = r$, then, by assumption, $\mathfrak{a}_i \cap k[t_{m+1}, \ldots, t_n] = \langle t_{m+1}, \ldots, t_m \rangle = 0$. Thus $f_{(0)} = 0$. Hence $x \in \langle t_1, \ldots, t_{h_i} \rangle$. Thus $\mathfrak{a}_i \cap P \subset \langle t_1, \ldots, t_{h_i} \rangle$. So the two are equal. Thus (2) holds, and the proof is complete. □

Exercise **(15.2)**. — Let $k := \mathbb{F}_q$ be the finite field with q elements, and $k[X, Y]$ the polynomial ring. Set $f := X^q Y - X Y^q$ and $R := k[X, Y]/\langle f \rangle$. Let x, $y \in R$ be the residues of X, Y. For every $a \in k$, show that R is not module finite over $P := k[y - ax]$. (Thus, in **(15.1)**, no k-linear combination works.) First, take $a = 0$.

EXERCISE **(15.3)**. — Let k be a field, and X, Y, Z variables. Set

$$R := k[X, Y, Z]/\langle X^2 - Y^3 - 1, XZ - 1\rangle,$$

and let x, y, $z \in R$ be the residues of X, Y, Z. Fix $a, b \in k$, and set $t := x + ay + bz$ and $P := k[t]$. Show that x and y are integral over P for any a, b and that z is integral over P if and only if $b \neq 0$.

THEOREM **(15.4)** (Weak Nullstellensatz). — *Let k be a field, and R a finitely generated k-algebra. Suppose R is a field. Then R is a finite extension field of k.*

PROOF: By the Noether Normalization Lemma **(15.1)**, R is module finite over a polynomial subring $P := k[t_1, \dots, t_\nu]$. Then $P \subset R$ is an integral extension by **(10.15)**. Since R is a field, so is P by **(14.1)**. Hence $\nu = 0$. So $P = k$. Thus R is module finite over k, as asserted. □

COROLLARY **(15.5)**. — *Let k be a field, $R := k[x_1, \dots, x_n]$ a finitely generated k-algebra, and $\mathfrak{m}$ a maximal ideal of R. Assume k is algebraically closed. Then there are $a_1, \dots, a_n \in k$ such that $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n\rangle$.*

PROOF: Set $K := R/\mathfrak{m}$. Then K is a finite extension field of k by the Weak Nullstellensatz **(15.4)**. But k is algebraically closed. Hence $k = K$. Let $a_i \in k$ be the residue of x_i, and set $\mathfrak{n} := \langle x_1 - a_1, \dots, x_n - a_n\rangle$. Then $\mathfrak{n} \subset \mathfrak{m}$.

Let $R' := k[X_1, \dots, X_n]$ be the polynomial ring, and $\varphi\colon R' \to R$ the k-algebra map with $\varphi X_i := x_i$. Set $\mathfrak{n}' := \langle X_1 - a_1, \dots, X_n - a_n\rangle$. Then $\varphi(\mathfrak{n}') = \mathfrak{n}$. But $\mathfrak{n}'$ is maximal by **(2.17)**. So $\mathfrak{n}$ is maximal. Hence $\mathfrak{n} = \mathfrak{m}$, as desired. □

THEOREM **(15.6)** (Hilbert Nullstellensatz). — *Let k be a field, and R a finitely generated k-algebra. Let $\mathfrak{a}$ be a proper ideal of R. Then*

$$\sqrt{\mathfrak{a}} = \textstyle\bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$$

where $\mathfrak{m}$ runs through all maximal ideals containing $\mathfrak{a}$.

PROOF: We may assume $\mathfrak{a} = 0$ by replacing R by $R/\mathfrak{a}$. Clearly $\sqrt{0} \subset \bigcap \mathfrak{m}$. Conversely, take $f \notin \sqrt{0}$. Then $R_f \neq 0$ by **(11.2)**. So R_f has a maximal ideal $\mathfrak{n}$ by **(2.25)**. Let $\mathfrak{m}$ be its contraction in R. Now, R is a finitely generated k-algebra by hypothesis; hence, R_f is one too owing to **(11.10)**. Therefore, by the weak Nullstellensatz, $R_f/\mathfrak{n}$ is a finite extension field of k.

Set $K := R/\mathfrak{m}$. By construction, K is a k-subalgebra of $R_f/\mathfrak{n}$. Therefore, K is a finite-dimensional k-vector space. So $k \subset K$ is an integral extension by **(10.15)**. Since k is a field, so is K by **(14.1)**. Thus $\mathfrak{m}$ is maximal. But $f/1$ is a unit in R_f; so $f/1 \notin \mathfrak{n}$. Hence $f \notin \mathfrak{m}$. So $f \notin \bigcap \mathfrak{m}$. Thus $\sqrt{0} = \bigcap \mathfrak{m}$. □

EXERCISE **(15.7)**. — Let k be a field, K an algebraically closed extension field. (So K contains a copy of every finite extension field.) Let $P := k[X_1, \dots, X_n]$ be the polynomial ring, and $f, f_1, \dots, f_r \in P$. Assume f vanishes at every zero in K^n of $f_1, \dots, f_r$; in other words, if $(a) := (a_1, \dots, a_n) \in K^n$ and $f_1(a) = 0, \dots, f_r(a) = 0$, then $f(a) = 0$ too. Prove that there are polynomials $g_1, \dots, g_r \in P$ and an integer N such that $f^N = g_1 f_1 + \cdots + g_r f_r$.

LEMMA **(15.8)**. — *Let k be a field, R a finitely generated k-algebra. Assume R is a domain, and set $K := \operatorname{Frac}(R)$ and $d := \operatorname{tr.deg}_k K$. Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes of R. Then $r \leq d$, with equality if and only if r is maximal.*

PROOF: By the Noether Normalization Lemma **(15.1)**, R is module finite over a polynomial subring $P := k[t_1, \dots, t_m]$ such that $\mathfrak{p}_i \cap P = \langle t_1, \dots, t_{h_i} \rangle$ for suitable h_i. Set $M := \mathrm{Frac}(P)$. Then $m = \mathrm{tr.deg}_k M$. But $P \subset R$ is an integral extension by **(10.15)**. So $M \subset K$ is algebraic. Hence $m = d$. Now, Incomparability **(14.3)**(2) yields $h_i < h_{i+1}$ for all i. Hence $r \le h_r$. But $h_r \le m$ and $m = d$. Thus $r \le d$.

If $r = d$, then r is maximal, as it was just proved that no chain can be longer. Conversely, assume r is maximal. Then $\mathfrak{p}_0 = 0$ since R is a domain. So $h_0 = 0$. Further, $\mathfrak{p}_r$ is maximal since $\mathfrak{p}_r$ is contained in some maximal ideal and it is prime. So $\mathfrak{p}_r \cap P$ is maximal by Maximality **(14.3)**(1). Hence $h_r = m$.

Suppose there is an i such that $h_i + 1 < h_{i+1}$. Then

$$(\mathfrak{p}_i \cap P) \subsetneqq \langle t_1, \dots, t_{h_i+1} \rangle \subsetneqq (\mathfrak{p}_{i+1} \cap P).$$

Now, $P/(\mathfrak{p}_i \cap P)$ is, by **(1.8)**, equal to $k[t_{h_i+1}, \dots, t_m]$; the latter is a polynomial ring, so normal by **(10.26)**(1). Also, the extension $P/(\mathfrak{p}_i \cap P) \subset R/\mathfrak{p}_i$ is integral as $P \subset R$ is. Hence, the Going-down Theorem **(14.9)** yields a prime $\mathfrak{p}$ with $\mathfrak{p}_i \subset \mathfrak{p} \subset \mathfrak{p}_{i+1}$ and $\mathfrak{p} \cap P = \langle t_1, \dots, t_{h_i+1} \rangle$. Then $\mathfrak{p}_i \subsetneqq \mathfrak{p} \subsetneqq \mathfrak{p}_{i+1}$, contradicting the maximality of r. Thus $h_i + 1 = h_{i+1}$ for all i. But $h_0 = 0$. Hence $r = h_r$. But $h_r = m$ and $m = d$. Thus $r = d$, as desired. □

DEFINITION **(15.9)**. — Given a ring R, its (Krull) **dimension** $\dim(R)$ is defined to be the supremum of the **lengths** r of all strictly ascending chains of primes:

$$\dim(R) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \text{ in } R \,\}.$$

EXERCISE **(15.10)**. — Let R be a domain of (finite) dimension r, and $\mathfrak{p}$ a nonzero prime. Prove that $\dim(R/\mathfrak{p}) < r$.

EXERCISE **(15.11)**. — Let R'/R be an integral extension of rings. Prove that $\dim(R) = \dim(R')$.

THEOREM **(15.12)**. — *Let k be a field, R a finitely generated k-algebra. If R is a domain, then* $\dim(R) = \mathrm{tr.deg}_k(\mathrm{Frac}(R))$.

PROOF: The assertion is an immediate consequence of **(15.8)**. □

COROLLARY **(15.13)**. — *Let k be a field, R a finitely generated k-algebra, and $\mathfrak{p}$ a prime of R. Suppose R is a domain. Then*

$$\dim(R_{\mathfrak{p}}) + \dim(R/\mathfrak{p}) = \dim(R).$$

If also $\mathfrak{p}$ is maximal, then $\dim(R_{\mathfrak{p}}) = \dim(R)$.

PROOF: A chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in R gives rise to a pair of chains of primes, one in $R_{\mathfrak{p}}$ and one in $R/\mathfrak{p}$,

$$\mathfrak{p}_0 R_{\mathfrak{p}} \subsetneqq \cdots \subsetneqq \mathfrak{p} R_{\mathfrak{p}} \quad \text{and} \quad 0 = \mathfrak{p}/\mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p}_r/\mathfrak{p},$$

owing to **(11.16)** and to **(1.7)** and **(2.7)**; conversely, every such pair of chains arises from a unique chain in R through $\mathfrak{p}$. But by **(15.8)**, every strictly ascending chain through $\mathfrak{p}$ of maximal length is of length $\dim(R)$. The asserted equation follows.

If also $\mathfrak{p}$ is maximal, then clearly $\dim(R/\mathfrak{p}) = 0$, and so $\dim(R_{\mathfrak{p}}) = \dim(R)$. □

DEFINITION **(15.14)**. — We call a ring **catenary** if, given any two nested primes $\mathfrak{q} \subset \mathfrak{p}$, there exists a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ of maximal length r with $\mathfrak{p}_0 = \mathfrak{q}$ and $\mathfrak{p}_r = \mathfrak{p}$, and any two such chains have the same length r.

THEOREM **(15.15)**. — *Over a field, a finitely generated algebra is catenary.*

PROOF: Let R be the algebra, and $\mathfrak{q} \subset \mathfrak{p}$ two nested primes. Replacing R by $R/\mathfrak{q}$, we may assume R is a domain. Then the proof of **(15.13)** shows that any chain of primes $0 \subsetneqq \cdots \subsetneqq \mathfrak{p}$ of maximal length is of length $\dim(R) - \dim(R/\mathfrak{p})$. □

EXERCISE **(15.16)**. — Let k be a field, R a finitely generated k-algebra, $f \in R$ nonzero. Assume R is a domain. Prove that $\dim(R) = \dim(R_f)$.

EXERCISE **(15.17)**. — Let k be a field, $P := k[f]$ the polynomial ring in one variable f. Set $\mathfrak{p} := \langle f \rangle$ and $R := P_{\mathfrak{p}}$. Find $\dim(R)$ and $\dim(R_f)$.

15. Appendix: Jacobson Rings

(15.18) (*Jacobson Rings*). — We call a ring R **Jacobson** if, given any ideal $\mathfrak{a}$, its radical is equal to the intersection of all maximal ideal containing it; that is,

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m}\supset\mathfrak{a}} \mathfrak{m}. \tag{15.18.1}$$

In general, that intersection contains $\sqrt{\mathfrak{a}}$; so **(15.18.1)** holds if and only if every f outside $\sqrt{\mathfrak{a}}$ lies outside some maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.

Recall the Scheinnullstellensatz, **(3.17)**: it says $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\supset\mathfrak{a}} \mathfrak{p}$ with $\mathfrak{p}$ prime. Thus R is Jacobson if and only if, for every $\mathfrak{p}$ prime, $\mathfrak{p} = \bigcap_{\mathfrak{m}\supset\mathfrak{p}} \mathfrak{m}$ with $\mathfrak{m}$ maximal.

For example, a field k is Jacobson. More generally, a local ring A is Jacobson if and only if its maximal ideal is its only prime. Moreover, owing to the next lemma, the ring of integers $\mathbb{Z}$ and the polynomial ring in one variable $k[X]$ are Jacobson.

Lemma **(15.19)**. — *Let R be a 1-dimensional domain. Assume every nonzero element lies in only finitely many maximal ideals. Then R is Jacobson if and only if the set $\{\mathfrak{m}_\lambda\}_{\lambda\in\Lambda}$ of maximal ideals is infinite.*

Proof: If $\{\mathfrak{m}_\lambda\}$ is finite, take a nonzero $x_\lambda \in \mathfrak{m}_\lambda$ for each λ. Set $x := \prod x_\lambda$. Then $x \neq 0$ and $x \in \bigcap \mathfrak{m}_\lambda$. But $\sqrt{\langle 0\rangle} = \langle 0\rangle$ as R is a domain. So $\sqrt{\langle 0\rangle} \neq \bigcap \mathfrak{m}_\lambda$. Thus R is not Jacobson.

If $\{\mathfrak{m}_\lambda\}$ is infinite, then $\bigcap \mathfrak{m}_\lambda = \langle 0\rangle$ by hypothesis. Let $\mathfrak{p}$ be a nonzero prime. Then $\mathfrak{p}$ is maximal as R is 1-dimensional. Thus R is Jacobson. □

Proposition **(15.20)**. — *A ring R is Jacobson if and only if, for any nonmaximal prime $\mathfrak{p}$ and any $f \notin \mathfrak{p}$, the extension $\mathfrak{p}R_f$ is not maximal.*

Proof: Assume R is Jacobson. Take a nonmaximal prime $\mathfrak{p}$ and an $f \notin \mathfrak{p}$. Then $f \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$. So $\mathfrak{p}R_f$ is not maximal by **(11.16)**.

Conversely, let $\mathfrak{a}$ be an ideal, $f \notin \sqrt{\mathfrak{a}}$. Then $(R/\mathfrak{a})_f \neq 0$. So there is a maximal ideal $\mathfrak{n}$ in $(R/\mathfrak{a})_f$. Let $\mathfrak{m}$ be its contraction in R. Then $\mathfrak{m} \supset \mathfrak{a}$ and $f \notin \mathfrak{m}$. Further, **(4.8)** and **(12.18)** yield $R_f/\mathfrak{m}R_f = (R/\mathfrak{a}/\mathfrak{m}/\mathfrak{a})_f = (R/\mathfrak{a})_f/\mathfrak{n}$. Since $\mathfrak{n}$ is maximal, $R_f/\mathfrak{m}R_f$ is a field. So $\mathfrak{m}$ is maximal by the hypothesis. Thus R is Jacobson. □

Theorem **(15.21)** (Hilbert Nullstellensatz). — *Let R be a Jacobson ring, R' a finitely generated algebra, $\mathfrak{m}$ be a maximal ideal of R', and $\mathfrak{n}$ its contraction in R. Then* (1) *$\mathfrak{m}$ is maximal, and $R'/\mathfrak{m}'$ is algebraic over $R/\mathfrak{m}$, and* (2) *R' is Jacobson.*

Proof: To prove (1), replace R by $R/\mathfrak{m}$ and R' by $R'/\mathfrak{m}'$. Then R is Jacobson, R' is a field as well as a finitely generated algebra, and $R \subset R'$. We must show R is a field and R'/R is a finite field extension. Write $R' = R[x_1, \ldots, x_n]$. Then as $R' = R[x_1, \ldots, x_{n-1}][x_n]$, the tower property for finite extensions **(10.19)** shows it suffices to prove (1) for $n = 1$.

Set $x := x_1$ and $Q = \operatorname{Frac}(R)$. Then $Q[x] = R'$ as $R \subset Q$. Since R' is a field, $1/x \in Q[x]$, Therefore x is algebraic over Q. Say

$$ax^m + a_1x^{m-1} + \cdots + a_m = 0 \quad \text{with} \quad a_i \in R \quad \text{and} \quad a \neq 0.$$

So x is integral over R_a. Further $R_a[x] = R'$. Since R' is a field, R_a is a field by **(14.1)**. But R is a Jacobson domain. So R is a field by **(15.20)** because R_a has

no nonmaximal ideals. Hence $R = R_a$. Thus (1) holds.

To prove (2), let $\mathfrak{p}'$ be a prime ideal of R' and $\mathfrak{p}$ its contraction. Given $a' \in R' - \mathfrak{p}'$ with $\mathfrak{p}'R'_{a'}$ maximal, (1) implies that $\mathfrak{p}$ is maximal and $R'_{a'}/\mathfrak{p}'R'_{a'}$ is algebraic over $R/\mathfrak{p}$. Hence $R'_{a'}/\mathfrak{p}'R'_{a'} = (R'/\mathfrak{p}')_{a'}$ is a field. But then $R'/\mathfrak{p}'$ is integral over $R/\mathfrak{p}$, so $R'/\mathfrak{p}'$ is a field by **(14.1)**. Hence $\mathfrak{p}'$ is maximal. Thus **(15.20)** yields (2). □

16. Chain Conditions

In a ring, often every ideal is finitely generated; if so, we call the ring **Noetherian**. Examples include the ring of integers and any field. We characterize Noetherian rings as those in which every ascending chain of ideals stabilizes, or equivalently, in which every set of ideals has one member maximal under inclusion. We prove the Hilbert Basis Theorem: if a ring is Noetherian, then so is any finitely generated algebra over it. We define and characterize Noetherian modules similarly, and we prove that, over a Noetherian ring, a module is Noetherian if and only if it is finitely generated. Lastly, we study Artinian rings and modules; in them, by definition, every descending chain of ideals, respectively of submodules, stabilizes.

(16.1) (*Noetherian rings*). — We call a ring **Noetherian** if every ideal is finitely generated.

A PID is, trivially, Noetherian. Examples include a field k, the polynomial ring $k[X]$ in one variable, and the ring of integers $\mathbb{Z}$.

Here are two standard examples of non-Noetherian rings. A third is given below in **(16.6)**, and a fourth later in (18.26).

First, form the polynomial ring $k[X_1, X_2, \dots]$ in infinitely many variables. It is non-Noetherian as $\langle X_1, X_2, \dots \rangle$ is not finitely generated (but the ring is a UFD).

Second, in the polynomial ring $k[X, Y]$, form this subring R and its ideal $\mathfrak{a}$:

$$R := \left\{ f := a + Xg \mid a \in k \text{ and } g \in k[X, Y] \right\} \text{ and}$$
$$\mathfrak{a} := \langle X,\, XY,\, XY^2, \dots \rangle.$$

Then $\mathfrak{a}$ is not generated by any $f_1, \dots, f_m \in \mathfrak{a}$. Indeed, let n be the highest power of Y occurring in any f_i. Then $XY^{n+1} \notin \langle f_1, \dots, f_m \rangle$. Thus R is non-Noetherian.

Exercise **(16.2)**. — Let $\mathfrak{a}$ be a finitely generated ideal in an arbitrary ring. Show every set that generates $\mathfrak{a}$ contains a finite subset that generates $\mathfrak{a}$.

Definition **(16.3)**. — We say the **ascending chain condition** (acc) is satisfied if every ascending chain of ideals $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$ **stabilizes**; that is, there is a $j \geq 0$ such that $\mathfrak{a}_j = \mathfrak{a}_{j+1} = \cdots$.

We say the **maximal condition** (maxc) is satisfied if every nonempty set of ideals $\mathcal{S}$ contains ones *maximal* for inclusion, that is, properly contained in no other in $\mathcal{S}$.

Lemma **(16.4)**. — *Acc is satisfied if and only if maxc is.*

Proof: Let $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$ be a chain of ideals. If $\mathfrak{a}_j$ is maximal, then trivially $\mathfrak{a}_j = \mathfrak{a}_{j+1} = \cdots$. Thus maxc implies acc.

Conversely, given a nonempty set of ideals $\mathcal{S}$ with no maximal member, there's $\mathfrak{a}_0 \in \mathcal{S}$; for each $j \geq 0$, there's $\mathfrak{a}_{j+1} \in \mathcal{S}$ with $\mathfrak{a}_j \subsetneqq \mathfrak{a}_{j+1}$. So the Axiom of Countable Choice provides an infinite chain $\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots$. Thus acc implies maxc. □

Proposition **(16.5)**. — *Given a ring R, the following conditions are equivalent:* (1) *R is Noetherian;* (2) *acc is satisfied;* (3) *maxc is satisfied.*

PROOF: Assume (1) holds. Let $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$ be a chain of ideals. Set $\mathfrak{a} := \bigcup \mathfrak{a}_n$. Clearly, $\mathfrak{a}$ is an ideal. So by hypothesis, $\mathfrak{a}$ is finitely generated, say by $x_1, \ldots, x_r$. For each i, there is an j_i such that $x_i \in \mathfrak{a}_{j_i}$. Set $j := \max\{j_i\}$. Then $x_i \in \mathfrak{a}_j$ for all i. So $\mathfrak{a} \subset \mathfrak{a}_j \subset \mathfrak{a}_{j+1} \subset \cdots \subset \mathfrak{a}$. So $\mathfrak{a}_j = \mathfrak{a}_{j+1} = \cdots$. Thus (2) holds.

Assume (2) holds. Then (3) holds by **(16.4)**.

Assume (3) holds. Let $\mathfrak{a}$ be an ideal, a_λ for $\lambda \in \Lambda$ generators, $\mathcal{S}$ the set of ideals generated by finitely many a_λ. Let $\mathfrak{b}$ be a maximal element of $\mathcal{S}$; say $\mathfrak{b}$ is generated by $a_{\lambda_1}, \ldots, a_{\lambda_m}$. Then $\mathfrak{b} \subset \mathfrak{b} + \langle a_\lambda \rangle$ for any λ. So by maximality, $\mathfrak{b} = \mathfrak{b} + \langle a_\lambda \rangle$. Hence $a_\lambda \in \mathfrak{b}$. So $\mathfrak{b} = \mathfrak{a}$; whence, $\mathfrak{a}$ is finitely generated. Thus (1) holds. □

EXAMPLE **(16.6)**. — In the field of rational functions $k(X, Y)$, form this ring:

$$R := k[X,\ Y,\ X/Y,\ X/Y^2,\ X/Y^3, \ldots].$$

Then R is non-Noetherian by **(16.5)**. Indeed, X does not factor into irreducibles: $X = (X/Y) \cdot Y$ and $X/Y = (X/Y^2) \cdot Y$ and so on. Correspondingly, there is an ascending chain of ideals that does not stabilize:

$$\langle X \rangle \subsetneqq \langle X/Y \rangle \subsetneqq \langle X/Y^2 \rangle \subsetneqq \cdots .$$

PROPOSITION **(16.7)**. — *Let R be a Noetherian ring, S a multiplicative set, $\mathfrak{a}$ an ideal. Then $R/\mathfrak{a}$ and $S^{-1}R$ are Noetherian.*

PROOF: If R satisfies the acc, so do $R/\mathfrak{a}$ and $S^{-1}R$ by **(1.7)** and by **(11.16)**(1).

Alternatively, any ideal $\mathfrak{b}/\mathfrak{a}$ of $R/\mathfrak{a}$ is, clearly, generated by the images of generators of $\mathfrak{b}$. Similarly, any ideal $\mathfrak{b}$ of $S^{-1}R$ is generated by the images of generators of $\varphi_S^{-1}\mathfrak{b}$ by **(11.15)**(1)(b). □

EXERCISE **(16.8)**. — Let R be a ring, X a variable, $R[X]$ the polynomial ring. Prove this statement or find a counterexample: if $R[X]$ is Noetherian, then so is R.

THEOREM **(16.9)** (Cohen). — *A ring is Noetherian if every prime ideal is finitely generated.*

PROOF: Let R be a ring. Suppose there are non-finitely-generated ideals. Given a nonempty set of them $\{\mathfrak{a}_\lambda\}$ that is linearly ordered by inclusion, set $\mathfrak{a} := \bigcup \mathfrak{a}_\lambda$. If $\mathfrak{a}$ is finitely generated, then all the generators lie in some $\mathfrak{a}_\lambda$, so generate $\mathfrak{a}_\lambda$, a contradiction. Thus $\mathfrak{a}$ is non-finitely-generated. Hence, by Zorn's Lemma, there is a maximal non-finitely-generated ideal $\mathfrak{p}$. In particular, $\mathfrak{p} \neq R$.

Assume every prime is finitely generated. Then there are $a, b \in R - \mathfrak{p}$ with $ab \in \mathfrak{p}$. So $\mathfrak{p} + \langle a \rangle$ is finitely generated, say by $x_1 + w_1 a, \ldots, x_n + w_n a$ with $x_i \in \mathfrak{p}$. Then $\{x_1, \ldots, x_n, a\}$ generate $\mathfrak{p} + \langle a \rangle$.

Set $\mathfrak{b} = \operatorname{Ann}\big((\mathfrak{p} + \langle a \rangle)/\mathfrak{p}\big)$. Then $\mathfrak{b} \supset \langle b \rangle + \mathfrak{p}$ and $b \notin \mathfrak{p}$. So $\mathfrak{b}$ is finitely generated, say by $y_1, \ldots, y_m$. Take $z \in \mathfrak{p}$. Then $z \in \mathfrak{p} + \langle a \rangle$, so write

$$z = a_1 x_1 + \cdots + a_n x_n + ya$$

with $a_i, y \in R$. Then $ya \in \mathfrak{p}$. So $y \in \mathfrak{b}$. Hence $y = b_1 y_1 + \cdots + b_m y_m$ with $b_j \in R$. Thus $\mathfrak{p}$ is generated by $\{x_1, \ldots, x_n, ay_1, \ldots, ay_m\}$, a contradiction. Thus there are no non-finitely-generated ideals; in other words, R is Noetherian. □

LEMMA **(16.10)**. — *If a ring R is Noetherian, then so is the polynomial ring $R[X]$.*

PROOF: By way of contradiction, assume there is an ideal $\mathfrak{a}$ of $R[X]$ that is not finitely generated. Set $\mathfrak{a}_0 := \langle 0 \rangle$. For each $i \geq 1$, choose inductively $f_i \in \mathfrak{a} - \mathfrak{a}_{i-1}$ of least degree d_i, and set $\mathfrak{a}_i := \langle f_1, \ldots, f_i \rangle$. Let a_i be the leading coefficient of f_i, and $\mathfrak{b}$ the ideal generated by all the a_i. Since R is Noetherian, $\mathfrak{b} = \langle a_1, \ldots, a_n \rangle$ for some n by **(16.2)**. Then $a_{n+1} = r_1 a_1 + \cdots + r_n a_n$ with $r_i \in R$.

By construction, $d_i \leq d_{i+1}$ for all i. Set

$$f := f_{n+1} - (r_1 f_1 X^{d_{n+1}-d_1} + \cdots + r_n f_n X^{d_{n+1}-d_n}).$$

Then $\deg(f) < d_{n+1}$, so $f \in \mathfrak{a}_n$. Therefore, $f_{n+1} \in \mathfrak{a}_n$, a contradiction. □

THEOREM **(16.11)** (Hilbert Basis). — *Let R be a Noetherian ring, R' a finitely generated algebra. Then R' is Noetherian.*

PROOF: Say $x_1, \ldots, x_r$ generate R' over R, and let $P := R[X_1, \ldots, X_r]$ be the polynomial ring in r variables. Then P is Noetherian by **(16.10)** and induction on r. Assigning x_i to X_i defines an R-algebra map $P \to R'$, and obviously, it is surjective. Hence R' is Noetherian by **(16.7)**. □

(16.12) (*Noetherian modules*). — We call a module M **Noetherian** if every submodule is finitely generated. In particular, *a ring is Noetherian as a ring if and only if it is Noetherian as a module,* because its submodules are just the ideals.

We say the **ascending chain condition** (acc) is satisfied in M if every ascending chain of submodules $M_0 \subset M_1 \subset \cdots$ stabilizes. We say the **maximal condition** (maxc) is satisfied in M if every nonempty set of submodules contains ones maximal under inclusion. It is simple to generalize **(16.5)**: *These conditions are equivalent:*

(1) *M is Noetherian;* (2) *acc is satisfied in M;* (3) *maxc is satisfied in M.*

LEMMA **(16.13)**. — *Let R be a ring, M a module. Nested submodules $M_1 \subset M_2$ of M are equal if both these equations hold:*

$$M_1 \cap N = M_2 \cap N \quad \text{and} \quad (M_1 + N)/N = (M_2 + N)/N.$$

PROOF: Given $m_2 \in M_2$, there is $m_1 \in M_1$ with $n := m_2 - m_1 \in N$. Then $n \in M_2 \cap N = M_1 \cap N$. Hence $m_2 \in M_1$. Thus $M_1 = M_2$. □

EXERCISE **(16.14)**. — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence of R-modules, and M_1, M_2 two submodules of M. Prove or give a counterexample to this statement: if $\beta(M_1) = \beta(M_2)$ and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2)$, then $M_1 = M_2$.

PROPOSITION **(16.15)**. — *Let R be a ring, M a module, N a submodule.*

(1) *Then M is finitely generated if N and M/N are finitely generated.*

(2) *Then M is Noetherian if and only if N and M/N are Noetherian.*

PROOF: Assertion (1) is equivalent to **(5.6)** owing to **(5.3)**.

To prove (2), first assume M is Noetherian. A submodule N' of N is also a submodule of M, so N' is finitely generated; thus N is Noetherian. A submodule of M/N is finitely generated as its inverse image in M is so; thus M/N is Noetherian.

Conversely, assume N and M/N are Noetherian. Let P be a submodule of M. Then $P \cap N$ and $(P+N)/N$ are finitely generated. But $P/(P \cap N) \xrightarrow{\sim} (P+N)/N$ by **(4.8.2)**. So (1) implies P is finitely generated. Thus M is Noetherian.

Here is a second proof of (2). First assume M is Noetherian. Then any ascending chain in N is also a chain in M, so it stabilizes. And any chain in M/N is the image of a chain in M, so it too stabilizes. Thus N and M/N are Noetherian.

Conversely, assume N and M/N are Noetherian. Given $M_1 \subset M_2 \subset \cdots \subset M$, both $(M_1 \cap N) \subset (M_2 \cap N) \subset \cdots$ and $(M_1 + N)/N \subset (M_2 + N)/N \subset \cdots$ stabilize, say $M_j \cap N = M_{j+1} \cap N = \cdots$ and $(M_j + N)/N = (M_{j+1} + N)/N = \cdots$. Then $M_j = M_{j+1} = \cdots$ by **(16.13)**. Thus M is Noetherian. □

Corollary **(16.16)**. — *Modules $M_1, \ldots, M_r$ are Noetherian if and only if their direct sum $M_1 \oplus \cdots \oplus M_r$ is Noetherian.*

Proof: The sequence $0 \to M_1 \to M_1 \oplus (M_2 \oplus \cdots \oplus M_r) \to M_2 \oplus \cdots \oplus M_r \to 0$ is exact. So the assertion results from **(16.15)**(2) by induction on r. □

Exercise **(16.17)**. — Let R be a ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ideals such that each $R/\mathfrak{a}_i$ is a Noetherian ring. Prove (1) that $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module, and (2) that, if $\bigcap \mathfrak{a}_i = 0$, then R too is a Noetherian ring.

Theorem **(16.18)**. — *Let R be a Noetherian ring, and M a module. Then the following conditions on M are equivalent:*

(1) M is Noetherian; (2) M is finitely generated; (3) M is finitely presented.

Proof: Assume (2). Then there is an exact sequence $0 \to K \to R^n \to M \to 0$. Now, R^n is Noetherian by **(16.16)** and by **(16.12)**. Hence K is finitely generated, so (3) holds; further, (1) holds by **(16.15)**(2). Trivially, (1) or (3) implies (2). □

Theorem **(16.19)** (E. Artin–Tate). — *Let $R \subset R' \subset R''$ be rings. Assume R is Noetherian. Assume R'' is module finite over R', and R'' is algebra finite over R. Then R' is algebra finite over R.*

Proof: Say $x_1, \ldots, x_m$ generate R'' as an R'-algebra, and $y_1, \ldots, y_n$ generate R'' as an R'-module. Then there exist $z_{ij} \in R'$ and $z_{ijk} \in R'$ with

$$x_i = \sum z_{ij} y_j \quad \text{and} \quad y_i y_j = \sum z_{ijk} y_k. \tag{16.19.1}$$

Let R_0' be the R-algebra generated by the z_{ij} and the z_{ijk}. Since R is Noetherian, so is R_0' by the Hilbert Basis Theorem, **(16.11)**.

Any $x \in R''$ is a polynomial in the x_i with coefficients in R. Therefore, **(16.19.1)** implies that x is a linear combination of the y_j with coefficients in R_0'. But R_0' is a Noetherian ring, and R' is an R_0'-submodule of R''. Hence R' is module finite over R_0' by **(16.15)**. Since R_0' is algebra finite over R, it follows that R' is too. □

Exercise **(16.20)**. — Let G be a finite group acting on a domain R, and R' the subring of invariants. Let $k \subset R'$ be a field. Using **(10.14)**, prove this celebrated theorem of E. Noether (1926): if R is algebra finite over k, then so is R'.

Example **(16.21)**. — Set $\delta := \sqrt{-5}$, set $R := \mathbb{Z}[\delta]$, and set $\mathfrak{p} := (2, 1 + \delta)$. Let's prove that $\mathfrak{p}$ is finitely presented and that $\mathfrak{p}R_\mathfrak{q}$ is free of rank 1 over $R_\mathfrak{q}$ for every maximal ideal $\mathfrak{q}$ of R, but that $\mathfrak{p}$ is not free. Thus the equivalent conditions of **(13.22)** do not imply that P is free.

Since $\mathbb{Z}$ is Noetherian and since R is generated over $\mathbb{Z}$, the Hilbert Basis Theorem **(16.11)** yields that R is Noetherian. So since $\mathfrak{p}$ is generated by two elements, **(16.18)** yields that $\mathfrak{p}$ is finitely presented.

Recall from [1, pp. 417, 421, 425] that $\mathfrak{p}$ is maximal in R, but not principal. Now, $3 \notin \mathfrak{p}$; otherwise, $1 \in \mathfrak{p}$ as $2 \in \mathfrak{p}$, but $\mathfrak{p} \neq R$. So $(1 - \delta)/3 \in R_\mathfrak{p}$. Hence $(1 + \delta)R_\mathfrak{p}$ contains $(1 + \delta)(1 - \delta)/3$, or 2. So $(1 + \delta)R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$. Since $R_\mathfrak{p}$ is a domain, the map $\mu_{1+\delta}\colon R_\mathfrak{p} \to \mathfrak{p}R_\mathfrak{p}$ is injective, so bijective. Thus $\mathfrak{p}R_\mathfrak{p}$ is free of rank 1.

Let $\mathfrak{q}$ be a maximal ideal distinct from $\mathfrak{p}$. Then $\mathfrak{p} \cap (R - \mathfrak{q}) \neq \emptyset$; so, $\mathfrak{p}R_{\mathfrak{q}} = R_{\mathfrak{q}}$ by **(11.11)**(2). Thus $\mathfrak{p}R_{\mathfrak{q}}$ is free of rank 1.

Finally, suppose $\mathfrak{p} \simeq R^n$. Set $S := R - 0$. Then $S^{-1}R$ is the fraction field, K say, of R. So $S^{-1}\mathfrak{p} \simeq K^n$. But the inclusion $\mathfrak{p} \hookrightarrow R$ yields an injection $S^{-1}\mathfrak{p} \hookrightarrow K$. Hence $S^{-1}\mathfrak{p} \xrightarrow{\simeq} K$, since $S^{-1}\mathfrak{p}$ is a nonzero K-vector space. Therefore, $n = 1$. So $\mathfrak{p} \simeq R$. Hence $\mathfrak{p}$ is generated by one element. But $\mathfrak{p}$ is not principal. So there is a contradiction. Thus $\mathfrak{p}$ is not free.

Definition **(16.22)**. — We say a module M is **Artinian** or the **descending chain condition** (dcc) is satisfied in M if every descending chain of submodules stabilizes.

We say the ring itself is **Artinian** if it is an Artinian module.

We say the **minimal condition** (minc) is satisfied in M if every nonempty set of submodules has a minimal member.

Proposition **(16.23)**. — *Let $M_1, \ldots, M_r, M$ be modules, N a submodule of M.*

(1) *Then M is Artinian if and only if minc is satisfied in M.*
(2) *Then M is Artinian if and only if N and M/N are Artinian.*
(3) *Then $M_1, \ldots, M_r$ are Artinian if and only if $M_1 \oplus \cdots \oplus M_r$ is Artinian.*

Proof: It is easy to adapt the proof of **(16.4)**, the second proof of **(16.15)**(2), and the proof of **(16.16)**. □

Exercise **(16.24)**. — Let k be a field, R an algebra. Assume that R is finite dimensional as a k-vector space. Prove that R is Noetherian and Artinian.

Exercise **(16.25)**. — Let p be a prime number, and set $M := \mathbb{Z}[1/p]/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. Prove that any $\mathbb{Z}$-submodule $N \subset M$ is either finite or all of M. Deduce that M is an Artinian $\mathbb{Z}$-module, and that it is not Noetherian.

Exercise **(16.26)**. — Let R be an Artinian ring. Prove that R is a field if it is a domain. Deduce that, in general, every prime ideal $\mathfrak{p}$ of R is maximal.

17. Associated Primes

Given a module, a prime is **associated** to it if the prime is equal to the annihilator of an element. Given a subset of the set of all associated primes, we prove there is a submodule whose own associated primes constitute that subset. If the ring is Noetherian, then the set of annihilators of elements has maximal members; we prove the latter are prime, so associated. Then the union of all the associated primes is the set of zerodivisors on the module. If also the module is finitely generated, then the intersection is the set of nilpotents. Lastly, we prove there is then a finite chain of submodules whose successive quotients are cyclic with prime annihilators; these primes include all associated primes, which are, therefore, finite in number.

DEFINITION **(17.1)**. — Let R be a ring, M a module. A prime ideal $\mathfrak{p}$ is said to be **associated** to M if there is a (nonzero) $m \in M$ with $\mathfrak{p} = \operatorname{Ann}(m)$. The set of associated primes is denoted by $\operatorname{Ass}(M)$ or $\operatorname{Ass}_R(M)$.

The primes that are minimal in $\operatorname{Ass}(M)$ are called the **minimal primes** of M; the others, the **embedded primes.**

Warning: following a old custom, we mean by the **associated primes** of an ideal $\mathfrak{a}$ not those of $\mathfrak{a}$ viewed as an abstract module, but rather those of $R/\mathfrak{a}$.

LEMMA **(17.2)**. — *Let R be a ring, M a module, and $\mathfrak{p}$ a prime ideal. Then $\mathfrak{p} \in \operatorname{Ass}(M)$ if and only if there is an R-injection $R/\mathfrak{p} \hookrightarrow M$.*

PROOF: Assume $\mathfrak{p} = \operatorname{Ann}(m)$ with $m \in M$. Define a map $R \to M$ by $x \mapsto xm$. This map induces an R-injection $R/\mathfrak{p} \hookrightarrow M$.

Conversely, suppose there is an R-injection $R/\mathfrak{p} \hookrightarrow M$, and let $m \in M$ be the image of 1. Then $\mathfrak{p} = \operatorname{Ann}(m)$, so $\mathfrak{p} \in \operatorname{Ass}(M)$. □

PROPOSITION **(17.3)**. — *Let M be a module. Then $\operatorname{Ass}(M) \subset \operatorname{Supp}(M)$.*

PROOF: Let $\mathfrak{p} \in \operatorname{Ass}_R(M)$. Say $\mathfrak{p} = \operatorname{Ann}(m)$. Then $m/1 \in M_{\mathfrak{p}}$ is nonzero as no $x \in (R - \mathfrak{p})$ satisfies $xm = 0$. Alternatively, **(17.2)** yields an R-injection $R/\mathfrak{p} \hookrightarrow M$. It induces an injection $(R/\mathfrak{p})_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{p}}$ by **(12.16)**. But $(R/\mathfrak{p})_{\mathfrak{p}} = \operatorname{Frac}(R/\mathfrak{p})$ by **(12.19)**. Thus $M_{\mathfrak{p}} \neq 0$ and so $\mathfrak{p} \in \operatorname{Supp}(M)$. □

LEMMA **(17.4)**. — *Let R be a ring, $\mathfrak{p}$ a prime ideal, $m \in R/\mathfrak{p}$ a nonzero element. Then* (1) $\operatorname{Ann}(m) = \mathfrak{p}$ *and* (2) $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

PROOF: To prove (1), say m is the residue of $y \in R$. Let $x \in R$. Then $xm = 0$ if and only if $xy \in \mathfrak{p}$, so if and only if $x \in \mathfrak{p}$, as $\mathfrak{p}$ is prime and $m \neq 0$. Thus (1) holds.

Trivially, (1) implies (2). □

PROPOSITION **(17.5)**. — *Let M be a module, N a submodule. Then*

$$\operatorname{Ass}(N) \subset \operatorname{Ass}(M) \subset \operatorname{Ass}(N) \cup \operatorname{Ass}(M/N).$$

PROOF: Take $m \in N$. Then the annihilator of m is the same whether m is regarded as an element of N or of M. So $\operatorname{Ass}(N) \subset \operatorname{Ass}(M)$.

Let $\mathfrak{p} \in \operatorname{Ass}(M)$. Then **(17.2)** yields an R-injection $R/\mathfrak{p} \hookrightarrow M$. Denote its image by E. If $E \cap N = 0$, then the composition $R/\mathfrak{p} \to M \to M/N$ is injective; hence, $\mathfrak{p} \in \operatorname{Ass}(M/N)$ by **(17.2)**. Else, take a nonzero $m \in E \cap N$. Then $\operatorname{Ann}(m) = \mathfrak{p}$ by **(17.4)**(1). Thus $\mathfrak{p} \in \operatorname{Ass}(N)$. □

EXERCISE **(17.6)**. — Given modules $M_1, \dots, M_r$, set $M := M_1 \oplus \cdots \oplus M_r$. Prove

$$\operatorname{Ass}(M) = \operatorname{Ass}(M_1) \cup \cdots \cup \operatorname{Ass}(M_r).$$

EXERCISE **(17.7)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 2\rangle \oplus \mathbb{Z}$. Find $\operatorname{Ass}(M)$ and find two submodules L, $N \subset M$ with $L + N = M$ but $\operatorname{Ass}(L) \cup \operatorname{Ass}(N) \subsetneqq \operatorname{Ass}(M)$.

PROPOSITION **(17.8)**. — *Let M be a module, and Ψ a subset of $\operatorname{Ass}(M)$. Then there is a submodule N of M with $\operatorname{Ass}(M/N) = \Psi$ and $\operatorname{Ass}(N) = \operatorname{Ass}(M) - \Psi$.*

PROOF: Given submodules N_λ of M totally ordered by inclusion, set $N := \bigcup N_\lambda$. Given $\mathfrak{p} \in \operatorname{Ass}(N)$, say $\mathfrak{p} = \operatorname{Ann}(m)$. Then $m \in N_\lambda$ for some λ; so $\mathfrak{p} \in \operatorname{Ass}(N_\lambda)$. Conversely, $\operatorname{Ass}(N_\lambda) \subset \operatorname{Ass}(N)$ by **(17.5)**. Thus $\operatorname{Ass}(N) = \bigcup \operatorname{Ass}(N_\lambda)$.

So we may apply Zorn's Lemma to obtain a submodule N of M that is maximal with $\operatorname{Ass}(N) \subset \operatorname{Ass}(M) - \Psi$. By **(17.5)**, it suffices to show that $\operatorname{Ass}(M/N) \subset \Psi$.

Take $\mathfrak{p} \in \operatorname{Ass}(M/N)$. Then M/N has a submodule N'/N isomorphic to $R/\mathfrak{p}$ by **(17.2)**. So $\operatorname{Ass}(N') \subset \operatorname{Ass}(N) \cup \{\mathfrak{p}\}$ by **(17.5)** and **(17.4)**(2). Now, $N' \supsetneqq N$ and N is maximal with $\operatorname{Ass}(N) \subset \operatorname{Ass}(M) - \Psi$. Hence $\mathfrak{p} \in \operatorname{Ass}(N') \subset \operatorname{Ass}(M)$, but $\mathfrak{p} \notin \operatorname{Ass}(M) - \Psi$. Thus $\mathfrak{p} \in \Psi$. □

PROPOSITION **(17.9)**. — *Let R be a ring, S a multiplicative subset, M a module, and $\mathfrak{p}$ a prime ideal. If $\mathfrak{p} \cap S = \emptyset$ and $\mathfrak{p} \in \operatorname{Ass}(M)$, then $S^{-1}\mathfrak{p} \in \operatorname{Ass}(S^{-1}M)$; the converse holds if $\mathfrak{p}$ is finitely generated.*

PROOF: Assume $\mathfrak{p} \in \operatorname{Ass}(M)$. Then **(17.2)** yields an injection $R/\mathfrak{p} \hookrightarrow M$. It induces an injection $S^{-1}(R/\mathfrak{p}) \hookrightarrow S^{-1}M$ by **(12.16)**. But $S^{-1}(R/\mathfrak{p}) = S^{-1}R/S^{-1}\mathfrak{p}$ by **(12.18)**. Assume $\mathfrak{p} \cap S = \emptyset$ also. Then $\mathfrak{p}S^{-1}R$ is prime by **(11.15)**(3)(b). But $\mathfrak{p}S^{-1}R = S^{-1}\mathfrak{p}$ by **(12.2)**. Thus $S^{-1}\mathfrak{p} \in \operatorname{Ass}(S^{-1}M)$.

Conversely, assume $S^{-1}\mathfrak{p} \in \operatorname{Ass}(S^{-1}M)$. Then there are $m \in M$ and $t \in S$ with $S^{-1}\mathfrak{p} = \operatorname{Ann}(m/t)$. Say $\mathfrak{p} = \langle x_1, \dots, x_n\rangle$. Fix i. Then $x_i m/t = 0$. So there is $s_i \in S$ with $s_i x_i m = 0$. Set $s := \prod s_i$. Then $x_i \in \operatorname{Ann}(sm)$. Thus $\mathfrak{p} \subset \operatorname{Ann}(sm)$.

Take $b \in \operatorname{Ann}(sm)$. Then $bsm/st = 0$. So $b/1 \in S^{-1}\mathfrak{p}$. So $b \in \mathfrak{p}$ by **(11.15)**(1)(a) and **(11.15)**(3)(a). Thus $\mathfrak{p} \supset \operatorname{Ann}(sm)$. So $\mathfrak{p} = \operatorname{Ann}(sm)$. Thus $\mathfrak{p} \in \operatorname{Ass}(M)$.

Finally, $\mathfrak{p} \cap S = \emptyset$ by **(11.16)**(2), as $S^{-1}\mathfrak{p}$ is prime. □

EXERCISE **(17.10)**. — Let R be a ring, and suppose $R_\mathfrak{p}$ is a domain for every prime $\mathfrak{p}$. Prove every associated prime of R is minimal.

LEMMA **(17.11)**. — *Let R be a ring, M a module, and $\mathfrak{a}$ an ideal. Suppose $\mathfrak{a}$ is maximal in the set of annihilators of nonzero elements m of M. Then $\mathfrak{a} \in \operatorname{Ass}(M)$.*

PROOF: Say $\mathfrak{a} := \operatorname{Ann}(m)$ with $m \neq 0$. Then $1 \notin \mathfrak{a}$ as $m \neq 0$. Now, take $b, c \in R$ with $bc \in \mathfrak{a}$, but $c \notin \mathfrak{a}$. Then $bcm = 0$, but $cm \neq 0$. Plainly, $\mathfrak{a} \subset \operatorname{Ann}(cm)$. So $\mathfrak{a} = \operatorname{Ann}(cm)$ by maximality. But $b \in \operatorname{Ann}(cm)$, so $b \in \mathfrak{a}$. Thus $\mathfrak{a}$ is prime. □

PROPOSITION **(17.12)**. — *Let R be a Noetherian ring, M a module. Then $M = 0$ if and only if $\operatorname{Ass}(M) = \emptyset$.*

PROOF: Obviously, if $M = 0$, then $\operatorname{Ass}(M) = \emptyset$. Conversely, suppose $M \neq 0$. Let $\mathcal{S}$ be the set of annihilators of nonzero elements of M. Then $\mathcal{S}$ has a maximal element $\mathfrak{a}$ by **(16.5)**. By **(17.11)**, $\mathfrak{a} \in \operatorname{Ass}(M)$. Thus $\operatorname{Ass}(M) \neq \emptyset$. □

DEFINITION **(17.13)**. — Let R be a ring, M a module, $x \in R$. We say x is a **zerodivisor** on M if there is a nonzero $m \in M$ with $xm = 0$; otherwise, we say x is a **nonzerodivisor**. We denote the set of zerodivisors by $\operatorname{z.div}(M)$.

PROPOSITION **(17.14)**. — *Let R be a Noetherian ring, M a module. Then*

$$\mathrm{z.div}(M) = \bigcup_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p}.$$

PROOF: Given $x \in \mathrm{z.div}(M)$, say $xm = 0$ where $m \in M$ and $m \neq 0$. Then $x \in \mathrm{Ann}(m)$. But $\mathrm{Ann}(m)$ is contained in an ideal $\mathfrak{p}$ that is maximal among annihilators of nonzero elements because of **(16.5)**; hence, $\mathfrak{p} \in \mathrm{Ass}(M)$ by **(17.11)**. Thus $\mathrm{z.div}(M) \subset \bigcup \mathfrak{p}$. The opposite inclusion results from the definitions. □

EXERCISE **(17.15)**. — Let R be a Noetherian ring, M a module, N a submodule, $x \in R$. Show that, if $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Ass}(M/N)$, then $xM \cap N = xN$.

LEMMA **(17.16)**. — *Let R be a Noetherian ring, M a module. Then*

$$\mathrm{Supp}(M) = \bigcup_{\mathfrak{q}\in \mathrm{Ass}(M)} \boldsymbol{V}(\mathfrak{q}) \supset \mathrm{Ass}(M).$$

PROOF: Let $\mathfrak{p}$ be a prime. Then $R_\mathfrak{p}$ is Noetherian by **(16.7)** as R is. So $M_\mathfrak{p} \neq 0$ if and only if $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) \neq \emptyset$ by **(17.12)**. But R is Noetherian; so $\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) \neq \emptyset$ if and only if there is $\mathfrak{q} \in \mathrm{Ass}(M)$ with $\mathfrak{q} \cap (R - \mathfrak{p}) = \emptyset$, or $\mathfrak{q} \subset \mathfrak{p}$, owing to **(11.16)**(2) and **(17.9)**. Thus $\mathfrak{p} \in \mathrm{Supp}(M)$ if and only if $\mathfrak{p} \in \mathbf{V}(\mathfrak{q})$ for some $\mathfrak{q} \in \mathrm{Ass}(M)$. □

THEOREM **(17.17)**. — *Let R be a Noetherian ring, M a module, $\mathfrak{p} \in \mathrm{Supp}(M)$. Then $\mathfrak{p}$ contains some $\mathfrak{q} \in \mathrm{Ass}(M)$; if $\mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$, then $\mathfrak{p} \in \mathrm{Ass}(M)$.*

PROOF: By **(17.16)**, $\mathfrak{q}$ exists. Also, $\mathfrak{q} \in \mathrm{Supp}(M)$; so $\mathfrak{q} = \mathfrak{p}$ if $\mathfrak{p}$ is minimal. □

THEOREM **(17.18)**. — *Let R be a Noetherian ring, and M a finitely generated module. Then*

$$\mathrm{nil}(M) = \bigcap_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p}.$$

PROOF: Since M is finitely generated, $\mathrm{nil}(M) = \bigcap_{\mathfrak{p}\in \mathrm{Supp}(M)} \mathfrak{p}$ by **(13.8)**. Since R is Noetherian, given $\mathfrak{p} \in \mathrm{Supp}(M)$, there is $\mathfrak{q} \in \mathrm{Ass}(M)$ with $\mathfrak{q} \subset \mathfrak{p}$ by **(17.16)**. The assertion follows. □

LEMMA **(17.19)**. — *Let R be a Noetherian ring, M a finitely generated module. Then there exists a chain of submodules*

$$0 = M_0 \subset M_1 \subset \cdots M_{n-1} \subset M_n = M$$

with $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$ for $i = 1, \ldots, n$. For any such chain,

$$\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \mathrm{Supp}(M). \qquad \textbf{(17.19.1)}$$

PROOF: Among all submodules of M having such a chain, there is a maximal submodule N by **(16.18)** and **(16.12)**. Suppose $M/N \neq 0$. Then by **(17.12)**, the quotient M/N contains a submodule N'/N isomorphic to $R/\mathfrak{p}$ for some prime $\mathfrak{p}$. Then $N \subsetneqq N'$, contradicting maximality. Hence $N = M$. Thus a chain exists.

The first inclusion of **(17.19.1)** follows by induction from **(17.5)** and **(17.4)**(2). Now, $\mathfrak{p}_i \in \mathrm{Supp}(R/\mathfrak{p}_i)$ owing to **(12.19)**. Thus **(17.19.1)** follows from **(13.6)**(1). □

THEOREM **(17.20)**. — *Let R be a Noetherian ring, and M a finitely generated module. Then the set $\mathrm{Ass}(M)$ is finite.*

PROOF: The assertion follows directly from **(17.19)**. □

EXERCISE **(17.21)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Prove the primes minimal containing $\mathfrak{a}$ are associated to $\mathfrak{a}$. Prove such primes are finite in number.

EXERCISE **(17.22)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}$ in **(17.19)**. Determine when a chain $0 \subset M_1 \subsetneqq M$ is acceptable, and show that then $\mathfrak{p}_2 \notin \operatorname{Ass}(M)$.

EXERCISE **(17.23)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 12\rangle$ in **(17.19)**. Find all three acceptable chains, and show that, in each case, $\{\mathfrak{p}_i\} = \operatorname{Ass}(M)$.

PROPOSITION **(17.24)**. — *Let R be a Noetherian ring, and M and N finitely generated modules. Then*

$$\operatorname{Ass}(\operatorname{Hom}(M,N)) = \operatorname{Supp}(M) \bigcap \operatorname{Ass}(N).$$

PROOF: Take $\mathfrak{p} \in \operatorname{Ass}\big(\operatorname{Hom}(M,N)\big)$. Then **(17.2)** yields an injective R-map $R/\mathfrak{p} \hookrightarrow \operatorname{Hom}(M,N)$. Set $k(\mathfrak{p}) := \operatorname{Frac}(R/\mathfrak{p})$. Then $k(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ by **(12.19)**. Now, M is finitely presented by **(16.18)** as R is Noetherian; hence,

$$\operatorname{Hom}(M,N)_\mathfrak{p} = \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \qquad \textbf{(17.24.1)}$$

by **(12.21)**(2). Therefore, by exactness, localizing yields an injection

$$\varphi\colon k(\mathfrak{p}) \hookrightarrow \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}).$$

Hence $M_\mathfrak{p} \neq 0$; so $\mathfrak{p} \in \operatorname{Supp}(M)$. For any $m \in M_\mathfrak{p}$ with $\varphi(1)(m) \neq 0$, the map $k(\mathfrak{p}) \to N_\mathfrak{p}$ given by $x \mapsto \varphi(x)(m)$ is nonzero, so an injection. Hence by **(17.2)**, we have $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(N_\mathfrak{p})$. Therefore, also $\mathfrak{p} \in \operatorname{Ass}(N)$ by **(17.9)**.

Conversely, take $\mathfrak{p} \in \operatorname{Supp}(M) \cap \operatorname{Ass}(N)$. Then $M_\mathfrak{p} \neq 0$. So by Nakayama's Lemma, $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ is a nonzero vector space over $k(\mathfrak{p})$. Take any nonzero R-map $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \to k(\mathfrak{p})$, precede it by the canonical map $M_\mathfrak{p} \to M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$, and follow it by an R-injection $k(\mathfrak{p}) \hookrightarrow N_\mathfrak{p}$, which exists by **(17.2)** and **(17.9)**. We obtain a nonzero element of $\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$, annihilated by $\mathfrak{p}R_\mathfrak{p}$. But $\mathfrak{p}R_\mathfrak{p}$ is maximal, so is the entire annihilator. So $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}\big(\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})\big)$. Hence $\mathfrak{p} \in \operatorname{Ass}\big(\operatorname{Hom}(M,N)\big)$ by **(17.24.1)** and **(17.9)**. □

PROPOSITION **(17.25)**. — *Let R be a Noetherian ring, $\mathfrak{p}$ a prime, M a finitely generated module, and $x, y \in \mathfrak{p}$ nonzerodivisors on M. Then $\mathfrak{p} \in \operatorname{Ass}(M/xM)$ if and only if $\mathfrak{p} \in \operatorname{Ass}(M/yM)$.*

PROOF: Form the sequence $0 \to K \to M/xM \xrightarrow{\mu_y} M/xM$ with $K := \operatorname{Ker}(\mu_y)$. Apply the functor $\operatorname{Hom}(R/\mathfrak{p}, \bullet)$ to that sequence, and get this one:

$$0 \to \operatorname{Hom}(R/\mathfrak{p},\, K) \to \operatorname{Hom}(R/\mathfrak{p},\, M/xM) \xrightarrow{\mu_y} \operatorname{Hom}(R/\mathfrak{p},\, M/xM).$$

It is exact by **(5.17)**. But $y \in \mathfrak{p}$; so the right-hand map vanishes. Thus

$$\operatorname{Hom}(R/\mathfrak{p}, K) \xrightarrow{\sim} \operatorname{Hom}(R/\mathfrak{p},\, M/xM).$$

Form the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \to & M & \xrightarrow{\mu_x} & M & \to & M/xM \to 0 \\ & & \downarrow{\scriptstyle \mu_y} & & \downarrow{\scriptstyle \mu_y} & & \downarrow{\scriptstyle \mu_y} \\ 0 & \to & M & \xrightarrow{\mu_x} & M & \to & M/xM \to 0 \end{array}$$

The Snake Lemma **(5.12)** yields an exact sequence $0 \to K \to M/yM \xrightarrow{\mu_x} M/yM$. Hence, similarly, $\operatorname{Hom}(R/\mathfrak{p},\, K) \xrightarrow{\sim} \operatorname{Hom}(R/\mathfrak{p},\, M/yM)$. Therefore,

$$\operatorname{Hom}(R/\mathfrak{p},\, M/yM) = \operatorname{Hom}(R/\mathfrak{p},\, M/xM). \qquad \textbf{(17.25.1)}$$

Finally, $\mathfrak{p} \in \operatorname{Supp}(R/\mathfrak{p})$ by **(13.6)**(3). Hence **(17.24)** yields the assertion. □

18. Primary Decomposition

Primary decomposition of a submodule generalizes factorization of an integer into powers of primes. A submodule is called **primary** if the quotient module has only one associated prime. We characterize these submodules in various ways over a Noetherian ring, emphasizing the case of ideals. A primary decomposition is a representation of a submodule as a finite intersection of primary submodules. The decomposition is called **irredundant**, or **minimal**, if cannot be reduced. We consider several illustrative examples in a polynomial ring.

Then we prove existence and uniqueness theorems for a proper submodule of a finitely generated module over a Noetherian ring. The celebrated Lasker–Noether Theorem asserts the existence of an irredundant primary decomposition. The First Uniqueness Theorem asserts the uniqueness of the primes that arise; they are just the associated primes of the quotient. The Second Uniqueness Theorem asserts the uniqueness of the primary components whose primes are minimal among these associated primes; the other primary components may vary.

DEFINITION **(18.1)**. — Let R be a ring, M a module, Q a submodule. If $\operatorname{Ass}(M/Q)$ consists of a single prime $\mathfrak{p}$, we say Q is **primary** or **$\mathfrak{p}$-primary** in M.

EXAMPLE **(18.2)**. — *A prime $\mathfrak{p}$ is $\mathfrak{p}$-primary,* as $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by **(17.4)**(2).

PROPOSITION **(18.3)**. — *Let R be a Noetherian ring, M a finitely generated module, Q a submodule. If Q is $\mathfrak{p}$-primary, then $\mathfrak{p} = \operatorname{nil}(M/Q)$.*

PROOF: The assertion holds as $\operatorname{nil}(M/Q) = \bigcap_{\mathfrak{q}\in\operatorname{Ass}(M/Q)} \mathfrak{q}$ by **(17.18)**. □

THEOREM **(18.4)**. — *Let R be a Noetherian ring, M a nonzero finitely generated module, Q a submodule. Set $\mathfrak{p} := \operatorname{nil}(M/Q)$. Then these conditions are equivalent:*

(1) *$\mathfrak{p}$ is prime and Q is $\mathfrak{p}$-primary.* (2) $\mathfrak{p} = \operatorname{z.div}(M/Q)$.
(3) *Given $x \in R$ and $m \in M$ with $xm \in Q$ but $m \notin Q$, necessarily $x \in \mathfrak{p}$.*

PROOF: Recall $\mathfrak{p} = \bigcap_{\mathfrak{q}\in\operatorname{Ass}(M/Q)} \mathfrak{q}$ by **(17.18)**, and $\operatorname{z.div}(M/Q) = \bigcup_{\mathfrak{q}\in\operatorname{Ass}(M/Q)} \mathfrak{q}$ by **(17.14)**. Thus $\mathfrak{p} \subset \operatorname{z.div}(M/Q)$.

Further, (2) holds if $\operatorname{Ass}(M/Q) = \{\mathfrak{p}\}$, that is, if (1) holds.

Conversely, if $x \in \mathfrak{q} \in \operatorname{Ass}(M/Q)$, but $x \notin \mathfrak{q}' \in \operatorname{Ass}(M/Q)$, then $x \notin \mathfrak{p}$, but $x \in \operatorname{z.div}(M/Q)$; hence, (2) implies (1). Thus (1) and (2) are equivalent.

Clearly, (3) means every zerodivisor on M/Q is nilpotent, or $\mathfrak{p} \supset \operatorname{z.div}(M/Q)$. But the opposite inclusion always holds. Thus (2) and (3) are equivalent. □

COROLLARY **(18.5)**. — *Let R be a Noetherian ring, and $\mathfrak{q}$ a proper ideal. Set $\mathfrak{p} := \sqrt{\mathfrak{q}}$. Then $\mathfrak{q}$ is primary (in R) if and only if, given $x, y \in R$ with $xy \in \mathfrak{q}$ but $x \notin \mathfrak{q}$, necessarily $y \in \mathfrak{p}$; if so, then $\mathfrak{p}$ is prime and $\mathfrak{q}$ is $\mathfrak{p}$-primary.*

PROOF: Clearly $\mathfrak{q} = \operatorname{Ann}(R/\mathfrak{q})$, so $\mathfrak{p} = \operatorname{nil}(R/\mathfrak{q})$. So the assertions result directly from **(18.4)** and **(18.3)**. □

EXERCISE **(18.6)**. — Let R be a ring, and $\mathfrak{p} = \langle p \rangle$ a principal prime generated by a nonzerodivisor p. Show every positive power $\mathfrak{p}^n$ is $\mathfrak{p}$-primary. Show conversely, if R is Noetherian, then every $\mathfrak{p}$-primary ideal $\mathfrak{q}$ is equal to some power $\mathfrak{p}^n$.

EXERCISE **(18.7)**. — Let k be a field, and $k[X,Y]$ the polynomial ring. Let $\mathfrak{a}$ be the ideal $\langle X^2, XY\rangle$. Show $\mathfrak{a}$ is not primary, but $\sqrt{\mathfrak{a}}$ is prime. Show $\mathfrak{a}$ satisfies this condition: $ab \in \mathfrak{a}$ implies $a^2 \in \mathfrak{a}$ or $b^2 \in \mathfrak{a}$.

EXERCISE **(18.8)**. — Let $\varphi\colon R \to R'$ be a homomorphism of Noetherian rings, and $\mathfrak{q} \subset R'$ a $\mathfrak{p}$-primary ideal. Show that $\varphi^{-1}\mathfrak{q} \subset R$ is $\varphi^{-1}\mathfrak{p}$-primary. Show that the converse holds if φ is surjective.

PROPOSITION **(18.9)**. — *Let R be a Noetherian ring, M a finitely generated module, Q a submodule. Set $\mathfrak{p} := \operatorname{nil}(M/Q)$. If $\mathfrak{p}$ is maximal, then Q is $\mathfrak{p}$-primary.*

PROOF: Since $\mathfrak{p} = \bigcap_{\mathfrak{q}\in \operatorname{Ass}(M/Q)} \mathfrak{q}$ by **(17.18)**, if $\mathfrak{p}$ is maximal, then $\mathfrak{p} = \mathfrak{q}$ for any $\mathfrak{q} \in \operatorname{Ass}(M/Q)$, or $\{\mathfrak{p}\} = \operatorname{Ass}(M/Q)$, as desired. □

COROLLARY **(18.10)**. — *Let R be a Noetherian ring, $\mathfrak{q}$ an ideal. Set $\mathfrak{p} := \sqrt{\mathfrak{q}}$. If $\mathfrak{p}$ is maximal, then $\mathfrak{q}$ is $\mathfrak{p}$-primary.*

PROOF: Since $\mathfrak{p} = \operatorname{nil}(R/\mathfrak{q})$, the assertion is a special case of **(18.9)**. □

COROLLARY **(18.11)**. — *Let R be a Noetherian ring, $\mathfrak{m}$ a maximal ideal. An ideal $\mathfrak{q}$ is $\mathfrak{m}$-primary if and only if there exists $n \geq 1$ such that $\mathfrak{m}^n \subset \mathfrak{q} \subset \mathfrak{m}$.*

PROOF: The condition $\mathfrak{m}^n \subset \mathfrak{q} \subset \mathfrak{m}$ just means that $\mathfrak{m} := \sqrt{\mathfrak{q}}$ by **(3.20)**. So the assertion results from **(18.5)** and **(18.10)**. □

LEMMA **(18.12)**. — *Let R be a Noetherian ring, $\mathfrak{p}$ a prime ideal, M a module. Let Q_1 and Q_2 be $\mathfrak{p}$-primary submodules; set $Q := Q_1 \cap Q_2$. Then Q is $\mathfrak{p}$-primary.*

PROOF: Form the canonical map $M \to M/Q_1 \oplus M/Q_2$. Its kernel is Q, so it induces an injection $M/Q \hookrightarrow M/Q_1 \oplus M/Q_2$. Hence **(17.12)** and **(17.5)** yield

$$\emptyset \neq \operatorname{Ass}(M/Q) \subset \operatorname{Ass}(M/Q_1) \cup \operatorname{Ass}(M/Q_2).$$

Since the latter two sets are each equal to $\{\mathfrak{p}\}$, so is $\operatorname{Ass}(M/Q)$, as desired. □

(18.13) (*Primary decomposition*). — Let R be a ring, M a module, and N a submodule. A **primary decomposition** of N is a decomposition

$$N = Q_1 \cap \cdots \cap Q_r \quad \text{with the } Q_i \text{ primary.}$$

We call the decomposition **irredundant** or **minimal** if these conditions are satisfied:

(1) $N \neq \bigcap_{j\neq i} Q_j$, or equivalently, $\bigcap_{j\neq i} Q_j \not\subset Q_i$ for $i = 1, \ldots, r$.
(2) Say Q_i is $\mathfrak{p}_i$-primary for $i = 1, \ldots, r$. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct.

If R is Noetherian, then owing to **(18.12)**, any primary decomposition can be made irredundant by intersecting all the primary submodules with the same prime and then discarding those of them that are not needed.

EXAMPLE **(18.14)**. — Let k be a field, $R := k[X,Y]$ the polynomial ring, and $\mathfrak{a} := \langle X^2, XY\rangle$. Below, it is proved that

$$\mathfrak{a} = \langle X\rangle \cap \langle X,Y\rangle^2 = \langle X\rangle \cap \langle X^2, Y\rangle. \qquad \textbf{(18.14.1)}$$

Here $\langle X,Y\rangle^2$ and $\langle X^2,Y\rangle$ are $\langle X,Y\rangle$-primary by **(18.11)**. Thus **(18.14.1)** shows two distinct primary decompositions of $\mathfrak{a}$. They are clearly irredundant.

Note: *the $\langle X,Y\rangle$-primary component is not unique!*

Obviously, $\mathfrak{a} \subset \langle X\rangle \cap \langle X,Y\rangle^2$ and $\langle X,Y\rangle^2 \subset \langle X^2,Y\rangle$. To see $\mathfrak{a} \supset \langle X\rangle \cap \langle X^2,Y\rangle$,

take $F \in \langle X\rangle \cap \langle X^2, Y\rangle$. Then $F = GX = AX^2 + BY$ where $A, B, G \in R$. Then $X(G - AX) = BY$. So $X \mid B$. Say $B = B'X$. Then $F = AX^2 + B'XY \in \mathfrak{a}$.

EXAMPLE **(18.15)**. — Let k be a field, $P := k[X, Y, Z]$ the polynomial ring. Set $R := P/\langle XZ - Y^2\rangle$. Let x, y, z be the residues of X, Y, Z in R. Set $\mathfrak{p} := \langle x, y\rangle$. Clearly $\mathfrak{p}^2 = \langle x^2, xy, y^2\rangle = x\langle x, y, z\rangle$. Let's show that $\mathfrak{p}^2 = \langle x\rangle \cap \langle x^2, y, z\rangle$ is an irredundant primary decomposition.

First note the inclusions $x\langle x, y, z\rangle \subset \langle x\rangle \cap \langle x, y, z\rangle^2 \subset \langle x\rangle \cap \langle x^2, y, z\rangle$.

Conversely, given $f \in \langle x\rangle \cap \langle x^2, y, z\rangle$, represent f by GX with $G \in P$. Then

$$GX = AX^2 + BY + CZ + D(XZ - Y^2) \quad \text{with} \quad A, B, C, D \in P.$$

So $(G - AX)X = B'Y + C'Z$ with $B', C' \in P$. Say $G - AX = A'' + B''Y + C''Z$ with $A'' \in k[X]$ and $B'', C'' \in P$. Then

$$A''X = -B''XY - C''XZ + B'Y + C'Z = (B' - B''X)Y + (C' - C''X)Z;$$

whence, $A'' = 0$. Therefore, $GX \in X\langle X, Y, Z\rangle$. Thus $\mathfrak{p}^2 = \langle x\rangle \cap \langle x^2, y, z\rangle$.

The ideal $\langle x\rangle$ is $\langle x, y\rangle$-primary in R by **(18.8)**. Indeed, the preimage in P of $\langle x\rangle$ is $\langle X, Y^2\rangle$ and of $\langle x, y\rangle$ is $\langle X, Y\rangle$. Further, $\langle X, Y^2\rangle$ is $\langle X, Y\rangle$-primary, as under the map $\varphi\colon P \to k[Y, Z]$ with $\varphi(X) = 0$, clearly $\langle X, Y^2\rangle = \varphi^{-1}\langle Y^2\rangle$ and $\langle X, Y\rangle = \varphi^{-1}\langle Y\rangle$; moreover, $\langle Y^2\rangle$ is $\langle Y\rangle$-primary by **(18.5)**, or by **(18.6)**.

Finally $\langle x, y, z\rangle^2 \subset \langle x^2, y, z\rangle \subset \langle x, y, z\rangle$ and $\langle x, y, z\rangle$ is maximal. So $\langle x^2, y, z\rangle$ is $\langle x, y, z\rangle$-primary by **(18.11)**.

Thus $\mathfrak{p}^2 = \langle x\rangle \cap \langle x^2, y, z\rangle$ is a primary decomposition. It is clearly irredundant.

EXERCISE **(18.16)**. — Let k be a field, $R := k[X, Y, Z]$ be the polynomial ring. Set $\mathfrak{a} := \langle XY,\ X - YZ\rangle$, set $\mathfrak{q}_1 := \langle X, Z\rangle$ and set $\mathfrak{q}_2 := \langle Y^2, X - YZ\rangle$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ and that this expression is an irredundant primary decomposition.

EXERCISE **(18.17)**. — Let $R := R' \times R''$ be a product of two domains. Find an irredundant primary decomposition of $\langle 0\rangle$.

LEMMA **(18.18)**. — *Let R be a ring, M a module, $N = Q_1 \cap \cdots \cap Q_r$ a primary decomposition in M. Say Q_i is $\mathfrak{p}_i$-primary for $i = 1, \dots, r$. Then*

$$\operatorname{Ass}(M/N) \subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}. \tag{18.18.1}$$

If equality holds and if $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct, then the decomposition is irredundant; the converse holds if R is Noetherian.

PROOF: Since $N = \bigcap Q_i$, the canonical map is injective: $M/N \hookrightarrow \bigoplus M/Q_i$. So **(17.5)** and **(17.6)** yield $\operatorname{Ass}(M/N) \subseteq \bigcup \operatorname{Ass}(M/Q_i)$. Thus **(18.18.1)** holds.

If $N = Q_2 \cap \cdots \cap Q_r$, then $\operatorname{Ass}(M/N) \subseteq \{\mathfrak{p}_2, \dots, \mathfrak{p}_r\}$ too. Thus if equality holds in **(18.18.1)** and if $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct, then $N = Q_1 \cap \cdots \cap Q_r$ is irredundant.

Conversely, assume $N = Q_1 \cap \cdots \cap Q_r$ is irredundant. Given i, set $P_i := \bigcap_{j \neq i} Q_j$. Then $P_i \cap Q_i = N$ and $P_i/N \neq 0$. Consider these two canonical injections:

$$P_i/N \hookrightarrow M/Q_i \quad \text{and} \quad P_i/N \hookrightarrow M/N.$$

Assume R is Noetherian. Then $\operatorname{Ass}(P_i/N) \neq \emptyset$ by **(17.12)**. So the first injection yields $\operatorname{Ass}(P_i/N) = \{\mathfrak{p}_i\}$ by **(17.5)**; then the second yields $\mathfrak{p}_i \in \operatorname{Ass}(M/N)$. Thus $\operatorname{Ass}(M/N) \supseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$, and **(18.18.1)** yields equality, as desired. □

THEOREM **(18.19)** (First Uniqueness). — *Let R be a Noetherian ring, and M a module. Let $N = Q_1 \cap \cdots \cap Q_r$ be an irredundant primary decomposition in M; say Q_i is $\mathfrak{p}_i$-primary for $i = 1, \ldots, r$. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are uniquely determined; in fact, they are just the distinct associated primes of M/N.*

PROOF: The assertion is just part of **(18.18)**. □

THEOREM **(18.20)** (Lasker–Noether). — *Over a Noetherian ring, each proper submodule of a finitely generated module has an irredundant primary decomposition.*

PROOF: Let M be the module, N the submodule. By **(17.20)**, M/N has finitely many distinct associated primes, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Owing to **(17.8)**, for each i, there is a $\mathfrak{p}_i$-primary submodule Q_i of M with $\operatorname{Ass}(Q_i/N) = \operatorname{Ass}(M/N) - \{\mathfrak{p}_i\}$. Set $P := \bigcap Q_i$. Fix i. Then $P/N \subset Q_i/N$. So $\operatorname{Ass}(P/N) \subset \operatorname{Ass}(Q_i/N)$ by **(17.5)**. But i is arbitrary. Hence $\operatorname{Ass}(P/N) = \emptyset$. Therefore, $P/N = 0$ by **(17.12)**. Finally, the decomposition $N = \bigcap Q_i$ is irredundant by **(18.18)**. □

EXERCISE **(18.21)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Consider the following submodule of M:

$$\Gamma_{\mathfrak{a}}(M) := \textstyle\bigcup_{n\geq 1}\{m \in M \mid \mathfrak{a}^n m = 0 \text{ for some } n \geq 1\}.$$

(1) For any decomposition $0 = \bigcap Q_i$ with Q_i $\mathfrak{p}_i$-primary, show $\Gamma_{\mathfrak{a}}(M) = \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$.
(2) Show $\Gamma_{\mathfrak{a}}(M)$ is the set of all $m \in M$ such that $m/1 \in M_{\mathfrak{p}}$ vanishes for every prime $\mathfrak{p}$ with $\mathfrak{a} \not\subset \mathfrak{p}$. (Thus $\Gamma_{\mathfrak{a}}(M)$ is the set of all m whose support lies in $\mathbf{V}(\mathfrak{a})$.)

LEMMA **(18.22)**. — *Let R be a Noetherian ring, S a multiplicative set, $\mathfrak{p}$ a prime ideal, M a module, and Q a $\mathfrak{p}$-primary submodule. If $S\cap\mathfrak{p} \neq \emptyset$, then $S^{-1}Q = S^{-1}M$ and $Q^S = M$. If $S\cap\mathfrak{p} = \emptyset$, then $S^{-1}Q$ is $S^{-1}\mathfrak{p}$-primary and $Q^S = \varphi_S^{-1}(S^{-1}Q) = Q$.*

PROOF: Every prime of $S^{-1}R$ is of the form $S^{-1}\mathfrak{q}$ where $\mathfrak{q}$ is a prime of R with $S \cap \mathfrak{q} = \emptyset$ by **(11.16)**(2) and **(12.2)**. And $S^{-1}\mathfrak{q} \in \operatorname{Ass}(S^{-1}(M/Q))$ if and only if $\mathfrak{q} \in \operatorname{Ass}(M/Q)$, that is, $\mathfrak{q} = \mathfrak{p}$, by **(17.9)**.

However, $S^{-1}(M/Q) = S^{-1}M/S^{-1}Q$ by **(12.16)**. Therefore, if $S \cap \mathfrak{p} \neq \emptyset$, then $\operatorname{Ass}(S^{-1}M/S^{-1}Q) = \emptyset$; whence, **(17.12)** yields $S^{-1}M/S^{-1}Q = 0$. Otherwise, if $S \cap \mathfrak{p} = \emptyset$, then $\operatorname{Ass}(S^{-1}M/S^{-1}Q) = \{S^{-1}\mathfrak{p}\}$; whence, $S^{-1}Q$ is $S^{-1}\mathfrak{p}$-primary.

Finally, $Q^S = \varphi_S^{-1}(S^{-1}Q)$ by **(12.15)**(3). So if $S^{-1}Q = S^{-1}M$, then $Q^S = M$. Now, suppose $S \cap \mathfrak{p} = \emptyset$. Given $m \in Q^S$, there is $s \in S$ with $sm \in Q$. But $s \notin \mathfrak{p}$. Further, $\mathfrak{p} = \operatorname{z.div}(M/Q)$ owing to **(17.14)**. Therefore, $m \in Q$. Thus $Q^S \subset Q$. But $Q^S \supset Q$ as $1 \in S$. Thus $Q^S = Q$. □

PROPOSITION **(18.23)**. — *Let R be a Noetherian ring, S a multiplicative set, M a finitely generated module. Let $N = Q_1 \cap \cdots \cap Q_r \subset M$ be an irredundant primary decomposition. Say Q_i is $\mathfrak{p}_i$-primary for all i, and $S \cap \mathfrak{p}_i = \emptyset$ just for $i \leq h$. Then*

$$S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_h \subset S^{-1}M \quad \textit{and} \quad N^S = Q_1 \cap \cdots \cap Q_h \subset M$$

are irredundant primary decompositions.

PROOF: By **(12.15)**(4)(b), $S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_r$. Further, by **(18.22)**, $S^{-1}Q_i$ is $S^{-1}\mathfrak{p}_i$-primary for $i \leq h$, and $S^{-1}Q_i = S^{-1}M$ for $i > h$. Therefore, $S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_h$ is a primary decomposition.

It is irredundant by **(18.18)**. Indeed, $\operatorname{Ass}(S^{-1}M/S^{-1}N) = \{S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_h\}$ by an argument like that in the first part of **(18.22)**. Further, $S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_h$ are distinct by **(11.16)**(2) as the $\mathfrak{p}_i$ are distinct.

Apply φ_S^{-1} to $S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_h$. Owing to **(12.15)**(3), we get $N^S = Q_1^S \cap \cdots \cap Q_h^S$. But $Q_i^S = Q_i$ by **(18.22)**. So $N^S = Q_1 \cap \cdots \cap Q_h$ is a primary decomposition. It is irredundant as, clearly, **(18.13)**(1) and (2) hold for it, since they hold for $N = Q_1 \cap \cdots \cap Q_r$. □

THEOREM **(18.24)** (Second Uniqueness). — *Let R be a ring, M a module, N a submodule. Assume R is Noetherian and M is finitely generated. Let $\mathfrak{p}$ be a minimal prime of M/N. Then, in any irredundant primary decomposition of N in M, the $\mathfrak{p}$-primary component Q is uniquely determined; in fact, $Q = N^S$ where $S := R - \mathfrak{p}$.*

PROOF: In **(18.23)**, take $S := R - \mathfrak{p}$. Then $h = 1$ as $\mathfrak{p}$ is minimal. □

EXERCISE **(18.25)**. — Let R be a Noetherian ring, M a finitely generated module, N a submodule. Prove $N = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(M/N)} \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$.

THEOREM **(18.26)** (Krull Intersection). — *Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Set $N := \bigcap_{n \geq 0} \mathfrak{a}^n M$. Then there exists $x \in \mathfrak{a}$ such that $(1 + x)N = 0$.*

PROOF: By **(16.18)**, N is finitely generated. So the desired $x \in \mathfrak{a}$ exists by **(10.3)** provided $N = \mathfrak{a}N$. Clearly $N \supset \mathfrak{a}N$. To prove $N \subset \mathfrak{a}N$, use **(18.20)**: take a primary decomposition $\mathfrak{a}N = \bigcap Q_i$ with Q_i $\mathfrak{p}_i$-primary. Fix i. If there's $a \in \mathfrak{a} - \mathfrak{p}_i$, then $aN \subset Q_i$, and so **(18.4)** yields $N \subset Q_i$. If $\mathfrak{a} \subset \mathfrak{p}_i$, then there's n_i with $\mathfrak{a}^{n_i} M \subset Q_i$ by **(18.3)** and **(3.19)**, and so again $N \subset Q_i$. Thus $N \subset \bigcap Q_i = \mathfrak{a}N$, as desired. □

EXERCISE **(18.27)**. — Let R be a Noetherian ring, $\mathfrak{m} \subset \mathrm{rad}(R)$ an ideal, M a finitely generated module, and M' a submodule. Considering M/M', show that

$$M' = \textstyle\bigcap_{n \geq 0} (\mathfrak{m}^n M + M').$$

EXAMPLE **(18.28)** (*Another non-Noetherian ring*). — Let R denote the ring of C^∞ functions on the real line, $\mathfrak{m}$ the ideal of all $f \in R$ that vanish at the origin. Note that $\mathfrak{m}$ is maximal, as $f \mapsto f(0)$ defines an isomorphism $R/\mathfrak{m} \xrightarrow{\sim} \mathbb{R}$.

Let $f \in R$ and $n \geq 1$. Then, Taylor's Theorem yields

$$f(x) = f(0) + f'(0)x + \cdots + \tfrac{f^{(n-1)}(0)}{(n-1)!} x^{n-1} + x^n f_n(x)$$
$$\text{where} \quad f_n(x) := \textstyle\int_0^1 \frac{(1-t)^{n-1}}{(n-1)!} f^{(n)}(xt)\, dt.$$

Here f_n is C^∞ too, since we can differentiate under the integral sign by [5, (7.1), p. 276]. So, if $f \in \mathfrak{m}$, then $f(x) = x f_1(x)$. Thus $\mathfrak{m} \subset \langle x \rangle$. But, obviously, $\mathfrak{m} \supset \langle x \rangle$. Hence $\mathfrak{m} = \langle x \rangle$. Therefore, $\mathfrak{m}^n = \langle x^n \rangle$.

If the first $n - 1$ derivatives of f vanish at 0, then Taylor's Theorem yields $f \in \langle x^n \rangle$. Conversely, assume $f(x) = x^n g(x)$ for some $g \in R$. By Leibniz's Rule,

$$f^{(k)}(x) = \textstyle\sum_{j=0}^k \binom{k}{j} \frac{n!}{(n-j+1)!} x^{n-j+1} g^{(k-j)}(x).$$

Hence $f^{(k)}$ vanishes at 0 if $n > k$. Thus $\langle x^n \rangle$ consists of the $f \in R$ whose first $n-1$ derivatives vanish at 0. But $\langle x^n \rangle = \mathfrak{m}^n$. Thus $\bigcap_{n \geq 0} \mathfrak{m}^n$ consists of those $f \in R$ all of whose derivatives vanish at 0.

There is a well-known nonzero C^∞-function all of whose derivatives vanish at 0:

$$h(x) := \begin{cases} e^{-1/x^2} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0; \end{cases}$$

see [5, Ex. 7, p. 82]. Thus $\bigcap_{n\geq 0} \mathfrak{m}^n \neq 0$.

Given $g \in \mathfrak{m}$, let's show $(1+g)h \neq 0$. Since $g(0) = 0$ and g is continuous, there is $\delta > 0$ such that $|g(x)| < 1/2$ if $|x| < \delta$. Hence $1 + g(x) \geq 1/2$ if $|x| < \delta$. Hence $\big(1 + g(x)\big)h(x) > (1/2)h(x) > 0$ if $0 < |x| < \delta$. Thus $(1+g)(\bigcap \mathfrak{m}^n) \neq 0$. Thus the Krull Intersection Theorem **(18.26)** fails for R, and so R is non-Noetherian.

19. Length

The length of a module is a generalization of the dimension of a vector space. The length is the number of links in a composition series, which is a finite chain of submodules whose successive quotients are simple — that is, their only proper submodules are zero. Our main result is the Jordan–Hölder Theorem: any two composition series do have the same length and even the same successive quotients; further, their annihilators are just the primes in the support of the module, and the module is equal to the product of its localizations at these primes. Consequently, the length is finite if and only if the module is both Artinian and Noetherian. We also prove Akizuki's Theorem: a ring is Artinian if and only if it is Noetherian and every prime is maximal. Consequently, a ring is Artinian if and only if its length is finite; if so, then it is the product of Artinian local rings.

(19.1) (*Length*). — Let R be a ring, and M a module. We call M **simple** if it is nonzero and its only proper submodule is 0. We call a chain of submodules,

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = 0 \qquad \textbf{(19.1.1)}$$

a **composition series** of **length** m if each successive quotient M_{i-1}/M_i is simple.

Finally, we define the **length** $\ell(M)$ to be the infimum of all those lengths:

$$\ell(M) := \inf\{\, m \mid M \text{ has a composition series of length } m \,\}. \qquad \textbf{(19.1.2)}$$

By convention, if M has no composition series, then $\ell(M) := \infty$; further, $\ell(0) := 0$.

For example, if R is a field, then M is a vector space and $\ell(M) = \dim_R(M)$. Further, the chains in **(17.23)** are composition series, but those in **(17.22)** are not.

Exercise **(19.2)**. — Let R be a ring, M a module. Prove these statements:

(1) If M is simple, then any nonzero element $m \in M$ generates M.
(2) M is simple if and only if $M \simeq R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and if so, then $\mathfrak{m} = \operatorname{Ann}(M)$.
(3) If M has finite length, then M is finitely generated.

Theorem **(19.3)** (Jordan–Hölder). — *Let R be a ring, and M a module with a composition series* **(19.1.1)**. *Then any chain of submodules can be refined to a composition series, and every composition series is of the same length $\ell(M)$. Further,*

$$\operatorname{Supp}(M) = \{\, \mathfrak{m} \in \operatorname{Spec}(R) \mid \mathfrak{m} = \operatorname{Ann}(M_{i-1}/M_i) \text{ for some } i \,\};$$

the $\mathfrak{m} \in \operatorname{Supp}(M)$ are maximal; there is a canonical isomorphism

$$M \xrightarrow{\sim} \textstyle\prod_{\mathfrak{m}\in\operatorname{Supp}(M)} M_{\mathfrak{m}};$$

and $\ell(M_{\mathfrak{m}})$ is equal to the number of i with $\mathfrak{m} = \operatorname{Ann}(M_{i-1}/M_i)$.

Proof: First, let M' be a proper submodule of M. Let's show that

$$\ell(M') < \ell(M). \qquad \textbf{(19.3.1)}$$

To do so, set $M'_i := M_i \cap M'$. Then $M'_{i-1} \cap M_i = M'_i$. So

$$M'_{i-1}/M'_i = (M'_{i-1} + M_i)/M_i \subset M_{i-1}/M_i.$$

Since M_{i-1}/M_i is simple, either $M'_{i-1}/M'_i = 0$, or $M'_{i-1}/M'_i = M_{i-1}/M_i$ and so

$$M'_{i-1} + M_i = M_{i-1}. \tag{19.3.2}$$

If **(19.3.2)** holds and if $M_i \subset M'$, then $M_{i-1} \subset M'$. Hence, if **(19.3.2)** holds for all i, then $M \subset M'$, a contradiction. Therefore, there is an i with $M'_{i-1}/M'_i = 0$. Now, $M' = M'_0 \supset \cdots \supset M'_m = 0$. Omit M'_i if $M'_{i-1}/M'_i = 0$. Thus M' has a composition series of length strictly less than m. Therefore, $\ell(M') < m$ for any choice of **(19.1.1)**. Thus **(19.3.1)** holds.

Next, given a chain $N_0 \supsetneqq \cdots \supsetneqq N_n = 0$, let's prove $n \leq \ell(M)$ by induction on $\ell(M)$. If $\ell(M) = 0$, then $M = 0$; so also $n = 0$. Assume $\ell(M) \geq 1$. If $n = 0$, then we're done. If $n \geq 1$, then $\ell(N_1) < \ell(M)$ by **(19.3.1)**; so $n - 1 \leq \ell(N_1)$ by induction. Thus $n \leq \ell(M)$.

If N_{i-1}/N_i is not simple, then there is N' with $N_{i-1} \supsetneqq N' \supsetneqq N_i$. The new chain can have length at most $\ell(M)$ by the previous paragraph. Repeating, we can refine the given chain into a composition series in at most $\ell(M) - n$ steps.

Suppose the given chain is a composition series. Then $\ell(M) \leq n$ by **(19.1.2)**. But we proved $n \leq \ell(M)$ above. Thus $n = \ell(M)$, and the first assertion is proved.

To proceed, fix a prime $\mathfrak{p}$. Exactness of Localization, **(12.16)**, yields this chain:

$$M_\mathfrak{p} = (M_0)_\mathfrak{p} \supset (M_1)_\mathfrak{p} \supset \cdots \supset (M_m)_\mathfrak{p} = 0. \tag{19.3.3}$$

Now, consider a maximal ideal $\mathfrak{m}$. If $\mathfrak{p} = \mathfrak{m}$, then $(R/\mathfrak{m})_\mathfrak{p} \simeq R/\mathfrak{m}$ by **(12.4)**. If $\mathfrak{p} \neq \mathfrak{m}$, then there is $s \in \mathfrak{m} - \mathfrak{p}$; so $(R/\mathfrak{m})_\mathfrak{p} = 0$.

Set $\mathfrak{m}_i := \operatorname{Ann}(M_{i-1}/M_i)$. So $M_{i-1}/M_i \simeq R/\mathfrak{m}_i$ and $\mathfrak{m}_i$ is maximal by **(19.2)**(2). Then Exactness of Localization yields $(M_{i-1}/M_i)_\mathfrak{p} = (M_{i-1})_\mathfrak{p}/(M_i)_\mathfrak{p}$. Hence

$$(M_{i-1})_\mathfrak{p}/(M_i)_\mathfrak{p} = \begin{cases} 0, & \text{if } \mathfrak{p} \neq \mathfrak{m}_i; \\ M_{i-1}/M_i \simeq R/\mathfrak{m}_i, & \text{if } \mathfrak{p} = \mathfrak{m}_i. \end{cases}$$

Thus $\operatorname{Supp}(M) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_m\}$.

If we omit the duplicates from the chain **(19.3.3)**, then we get a composition series from the $(M_i)_\mathfrak{p}$ with $M_{i-1}/M_i \simeq R/\mathfrak{p}$. Thus the number of such i is $\ell(M_\mathfrak{p})$.

Finally, consider the canonical map $\varphi\colon M \to \prod_{\mathfrak{m}\in\operatorname{Supp}(M)} M_\mathfrak{m}$. To prove φ is an isomorphism, it suffices, by **(13.17)**, to prove $\varphi_\mathfrak{p}$ is for each maximal ideal $\mathfrak{p}$. Now, localization commutes with finite product by **(12.10)**. Therefore,

$$\varphi_\mathfrak{p}\colon M_\mathfrak{p} \to \left(\textstyle\prod_\mathfrak{m} M_\mathfrak{m}\right)_\mathfrak{p} = \prod_\mathfrak{m} (M_\mathfrak{m})_\mathfrak{p} = M_\mathfrak{p}$$

as $(M_\mathfrak{m})_\mathfrak{p} = 0$ if $\mathfrak{m} \neq \mathfrak{p}$ and $(M_\mathfrak{m})_\mathfrak{p} = M_\mathfrak{p}$ if $\mathfrak{m} = \mathfrak{p}$ by the above. Thus $\varphi_\mathfrak{p} = 1$. □

Exercise **(19.4)**. — Let R be a Noetherian ring, M a finitely generated module. Prove that the following conditions are equivalent:

(1) M has finite length.
(2) $\operatorname{Supp}(M)$ consists entirely of maximal ideals.
(3) $\operatorname{Ass}(M)$ consists entirely of maximal ideals.

Prove that, if the conditions hold, then $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ are equal and finite.

Corollary **(19.5)**. — *A module M is both Artinian and Noetherian if and only if M is of finite length.*

PROOF: Any chain $M \supset N_0 \supsetneqq \cdots \supsetneqq N_n = 0$ has $n < \ell(M)$ by the Jordan–Hölder Theorem, **(19.3)**. So if $\ell(M) < \infty$, then M satisfies both the dcc and the acc.

Conversely, assume M is both Artinian and Noetherian. Form a chain as follows. Set $M_0 := M$. For $i \geq 1$, if $M_{i-1} \neq 0$, take a maximal $M_i \subsetneqq M_{i-1}$ by the maxc. By the dcc, this recursion terminates. Then the chain is a composition series. □

EXAMPLE **(19.6)**. — Any simple $\mathbb{Z}$-module is finite owing to **(19.2)**(2). Hence, a $\mathbb{Z}$-module is of finite length if and only if it is finite. In particular, $\ell(\mathbb{Z}) = \infty$.

Of course, $\mathbb{Z}$ is Noetherian, but not Artinian.

Let $p \in \mathbb{Z}$ be a prime, and set $M := \mathbb{Z}[1/p]/\mathbb{Z}$. Then M is an Artinian $\mathbb{Z}$-module, but not Noetherian by **(16.25)**. Since M is infinite, $\ell(M) = \infty$.

EXERCISE **(19.7)**. — Let k be a field, and R a finitely generated k-algebra. Prove that R is Artinian if and only if R is a finite-dimensional k-vector space.

THEOREM **(19.8)** (Additivity of Length). — *Let M be a module, and M' a submodule. Then $\ell(M) = \ell(M') + \ell(M/M')$.*

PROOF: If M has a composition series, then the Jordan–Hölder Theorem yields another one of the form $M = M_0 \supset \cdots \supset M' \supset \cdots \supset M_m = 0$. The latter yields a pair of composition series: $M/M' = M_0/M' \supset \cdots \supset M'/M' = 0$ and $M' \supset \cdots \supset M_m = 0$. Conversely, every such pair arises from a unique composition series in M through M'. Therefore, $\ell(M) < \infty$ if and only if $\ell(M/M') < \infty$ and $\ell(M') < \infty$; furthermore, if so, then $\ell(M) = \ell(M') + \ell(M/M')$, as desired. □

EXERCISE **(19.9)**. — Let k be a field, R a local k-algebra. Assume the map from k to the residue field is bijective. Given an R-module M, prove $\ell(M) = \dim_k(M)$.

THEOREM **(19.10)** (Akizuki). — *A ring R is Artinian if and only if R is Noetherian and $\dim(R) = 0$. If so, then R has only finitely many primes.*

PROOF: If $\dim(R) = 0$, then every prime is maximal. If also R is Noetherian, then R has finite length by **(19.4)**. Thus R is Artinian by **(19.5)**.

Conversely, suppose R is Artinian. Let $\mathfrak{m}$ be a minimal product of maximal ideals of R. Then $\mathfrak{m}^2 = \mathfrak{m}$. Let $\mathcal{S}$ be the set of ideals $\mathfrak{a}$ contained in $\mathfrak{m}$ such that $\mathfrak{a}\mathfrak{m} \neq 0$. If $\mathcal{S} \neq \emptyset$, take $\mathfrak{a} \in \mathcal{S}$ minimal. Then $\mathfrak{a}\mathfrak{m}^2 = \mathfrak{a}\mathfrak{m} \neq 0$; hence, $\mathfrak{a}\mathfrak{m} = \mathfrak{a}$ by minimality of $\mathfrak{a}$. For any $x \in \mathfrak{a}$, if $x\mathfrak{m} \neq 0$, then $\mathfrak{a} = \langle x \rangle$ by minimality of $\mathfrak{a}$.

Let $\mathfrak{n}$ be any maximal ideal. Then $\mathfrak{n}\mathfrak{m} = \mathfrak{m}$ by minimality of $\mathfrak{m}$. But $\mathfrak{n}\mathfrak{m} \subset \mathfrak{n}$. Thus $\mathfrak{m} \subset \operatorname{rad}(R)$. But $\mathfrak{a} = \langle x \rangle$. So Nakayama's Lemma yields $\mathfrak{a} = 0$, a contradiction. So $x\mathfrak{m} = 0$ for any $x \in \mathfrak{a}$. Thus $\mathfrak{a}\mathfrak{m} = 0$, a contradiction. Hence $\mathcal{S} = \emptyset$. Therefore, $\mathfrak{m}^2 = 0$. But $\mathfrak{m}^2 = \mathfrak{m}$. Thus $\mathfrak{m} = 0$. Say $\mathfrak{m} = \mathfrak{m}_1 \cdots \mathfrak{m}_r$ with $\mathfrak{m}_i$ maximal.

Set $\mathfrak{a}_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$ for $1 \leq i \leq r$. Consider the chain

$$R =: \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_r = 0.$$

Fix i. Set $V_i := \mathfrak{a}_{i-1}/\mathfrak{a}_i$. Then V_i is a vector space over $R/\mathfrak{m}_i$. Given linearly independent elements $x_1, x_2, \ldots \in V_i$, let $W_j \subset V_i$ be the subspace spanned by $x_j, x_{j+1}, \ldots$. The W_j form a descending chain. It must stabilize as R is Artinian. Thus $\dim(V_i) < \infty$. Hence $\ell(R) < \infty$ by **(19.8)**. So R is Noetherian by **(19.5)**. So, by **(19.4)**, every prime is maximal, and there are only finitely many primes. □

COROLLARY **(19.11)**. — *Let R be an Artinian ring, and M a finitely generated module. Then M has finite length, and $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ are equal and finite.*

PROOF: By **(19.10)** every prime is maximal, so $\mathrm{Supp}(M)$ consists of maximal ideals. Also R is Noetherian by **(19.10)**. Hence **(19.4)** yields the assertions. □

COROLLARY **(19.12)**. — *A ring R is Artinian if and only if $\ell(R) < \infty$.*

PROOF: By **(19.11)**, $\ell(R) < \infty$ if R is Artinian. The converse holds by **(19.5)**. □

EXERCISE **(19.13)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal, and R' a module-finite R-algebra. Show that R' has only finitely many primes $\mathfrak{p}'$ over $\mathfrak{p}$, as follows: reduce to the case that R is a field by localizing at $\mathfrak{p}$ and passing to the residue rings.

COROLLARY **(19.14)**. — *A ring R is Artinian if and only if R is a finite product of Artinian local rings; if so, then $R = \prod_{\mathfrak{m}\in\mathrm{Spec}(R)} R_{\mathfrak{m}}$.*

PROOF: A finite product of rings is Artinian if and only if each factor is Artinian by **(16.23)**(3). If R is Artinian, then $\ell(R) < \infty$ by **(19.12)**; whence, $R = \prod R_{\mathfrak{m}}$ by the Jordan–Hölder Theorem. Thus the assertion holds. □

EXERCISE **(19.15)**. — Let R be a Noetherian ring, and M a finitely generated module. Prove the equivalence of the following four conditions:

(1) M has finite length.
(2) M is annihilated by some finite product of maximal ideals $\prod \mathfrak{m}_i$.
(3) Every prime $\mathfrak{p}$ containing $\mathrm{Ann}(M)$ is maximal.
(4) $R/\mathrm{Ann}(M)$ is Artinian.

20. Hilbert Functions

The **Hilbert Function** of a graded module lists the lengths of its components. The corresponding generating function is called the **Hilbert Series**. This series is, under suitable hypotheses, a rational function, according to the Hilbert–Serre Theorem, which we prove. Passing to an arbitrary module, we study its **Hilbert–Samuel Series**, namely, the generating function of the colengths of the submodules in a filtration. We prove Samuel's Theorem: if the ring is Noetherian, if the module is finitely generated, and if the filtration is stable, then the Hilbert–Samuel Series is a rational function with poles just at 0 and 1. In the same setup, we prove the Artin–Rees Lemma: given any submodule, its induced filtration is stable.

In a brief appendix, we study further one notion that arose: homogeneity.

(20.1) (*Graded rings and modules*). — We call a ring R **graded** if there are additive subgroups R_n for $n \geq 0$ with $R = \bigoplus R_n$ and $R_m R_n \subset R_{m+n}$ for all m, n.

For example, a polynomial ring R with coefficient ring R_0 is graded if R_n is the R_0-submodule generated by the monomials of (total) degree n.

In general, R_0 is a *subring*. Obviously, R_0 is closed under addition and under multiplication, but we must check $1 \in R_0$. So say $1 = \sum x_m$ with $x_m \in R_m$. Given $z \in R$, say $z = \sum z_n$ with $z_n \in R_n$. Fix n. Then $z_n = 1 \cdot z_n = \sum x_m z_n$ with $x_m z_n \in R_{m+n}$. So $\sum_{m>0} x_m z_n = z_n - x_0 z_n \in R_n$. Hence $x_m z_n = 0$ for $m > 0$. But n is arbitrary. So $x_m z = 0$ for $m > 0$. But z is arbitrary. Taking $z := 1$ yields $x_m = x_m \cdot 1 = 0$ for $m > 0$. Thus $1 = x_0 \in R_0$.

We call an R-module M (compatibly) **graded** if there are additive subgroups M_n for $n \in \mathbb{Z}$ with $M = \bigoplus M_n$ and $R_m M_n \subset M_{m+n}$ for all m, n. We call M_n the nth **homogeneous component**; we say its elements are **homogeneous**. Obviously, M_n is an R_0-module.

Given $m \in \mathbb{Z}$, set $M(m) := \bigoplus M_{m+n}$. Then $M(m)$ is another graded module; its nth graded component $M(m)_n$ is M_{m+n}. Thus $M(m)$ is obtained from M by **shifting** m places to the left.

Lemma **(20.2)**. — *Let $R = \bigoplus R_n$ be a graded ring, and $M = \bigoplus M_n$ a graded R-module. If R is a finitely generated R_0-algebra and if M is a finitely generated R-module, then each M_n is a finitely generated R_0-module.*

Proof: Say $R = R_0[x_1, \dots, x_r]$. If $x_i = \sum_j x_{ij}$ with $x_{ij} \in R_j$, then replace the x_i by the nonzero x_{ij}. Similarly, say M is generated over R by $m_1, \dots, m_s$ with $m_i \in M_{l_i}$. Then any $m \in M_n$ is a sum $m = \sum f_i m_i$ where $f_i \in R$. Say $f_i = \sum f_{ij}$ with $f_{ij} \in R_j$, and replace f_i by f_{ik} with $k := n - l_i$ or by 0 if $n < l_i$. Then f_i is an R_0-linear combination of monomials $x_1^{i_1} \cdots x_r^{i_r} \in R_k$; hence, m is one of the products $x_1^{i_1} \cdots x_r^{i_r} m_i \in M_n$. Thus M_n is a finitely generated R_0-module. □

(20.3) (*Hilbert functions*). — Let $R = \bigoplus R_n$ be a graded ring, and $M = \bigoplus M_n$ a graded R-module. Assume R_0 is Artinian, R is a finitely generated R_0-algebra, and M is a finitely generated R-module. Then each M_n is a finitely generated R_0-module by **(20.2)**, so is of finite length $\ell(M_n)$ by **(19.11)**. We call $n \mapsto \ell(M_n)$ the **Hilbert Function** of M and its generating function

$$H(M, t) := \sum_{n \in \mathbb{Z}} \ell(M_n) t^n$$

the **Hilbert Series** of M. This series is a rational function by **(20.7)** below.

If $R = R_0[x_1, \dots, x_r]$ with $x_i \in R_1$, then by **(20.8)** below, the Hilbert Function is, for $n \gg 0$, a polynomial $h(M, n)$, which we call the **Hilbert Polynomial** of M.

EXAMPLE **(20.4)**. — Let $R := R_0[X_1, \dots, X_r]$ be the polynomial ring, graded by degree. Then R_n is free over R_0 on the monomials of degree n, so of rank $\binom{r-1+n}{r-1}$.

Assume R_0 is Artinian. Then $\ell(R_n) = \ell(R_0)\binom{r-1+n}{r-1}$ by Additivity of Length, **(19.8)**. Thus the Hilbert Function is, for $n \geq 0$, a polynomial of degree $r-1$.

Formal manipulation yields $\binom{r-1+n}{r-1} = (-1)^n\binom{-r}{n}$. Therefore, Newton's binomial theorem for negative exponents yields this computation for the Hilbert Series:

$$H(R, t) = \textstyle\sum_{n\geq 0} \ell(R_0)\binom{r-1+n}{r-1}t^n = \sum_{n\geq 0} \ell(R_0)\binom{-r}{n}(-t)^n = \ell(R_0)/(1-t)^r.$$

EXERCISE **(20.5)**. — Let k be a field, $k[X, Y]$ the polynomial ring. Show $\langle X, Y^2\rangle$ and $\langle X^2, Y^2\rangle$ have different Hilbert Series, but the same Hilbert Polynomial.

EXERCISE **(20.6)**. — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded R-module. Let $N = \bigoplus N_n$ be a **homogeneous submodule**; that is, $N_n = N \cap M_n$. Assume R_0 is Artinian, R is a finitely generated R_0-algebra, and M is a finitely generated R-module. Set

$$N' := \{\, m \in M \mid \text{there is } k_0 \text{ such that } R_k m \in N \text{ for all } k \geq k_0 \,\}.$$

(1) Prove that N' is a homogeneous submodule of M with the same Hilbert Polynomial as N, and that N' is the largest such submodule.

(2) Let $N = \bigcap Q_i$ be a decomposition with Q_i $\mathfrak{p}_i$-primary. Set $R_+ := \bigoplus_{n>0} R_n$. Prove that $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$.

THEOREM **(20.7)** (Hilbert–Serre). — *Let $R = \bigoplus R_n$ be a graded ring, and let $M = \bigoplus M_n$ be a graded R-module. Assume R_0 is Artinian, R is a finitely generated R_0-algebra, and M is a finitely generated R-module. Then*

$$H(M, t) = e(t)/t^l(1-t^{k_1})\cdots(1-t^{k_r})$$

with $e(t) \in \mathbb{Z}[t]$, with $l \geq 0$, and with $k_1, \dots, k_r \geq 1$.

PROOF: Say $R = R_0[x_1, \dots, x_r]$ with $x_i \in R_{k_i}$. First, assume $r = 0$. Say M is generated over R by $m_1, \dots, m_s$ with $m_i \in M_{l_i}$. Then $R = R_0$. So $M_n = 0$ for $n < l_0 := \min\{l_i\}$ and for $n > \max\{l_i\}$. Hence $t^{-l_0}H(M, t)$ is a polynomial.

Next, assume $r \geq 1$ and form the exact sequence

$$0 \to K \to M(-k_1) \xrightarrow{\mu_{x_1}} M \to L \to 0$$

where μ_{x_1} is the map of multiplication by x_1. Since $x_1 \in R_{k_1}$, the grading on M induces a grading on K and on L. Further, μ_{x_1} acts as 0 on both K and L.

Since R_0 is Artinian, R_0 is Noetherian by Akizuki's Theorem, **(19.10)**. So, since R is a finitely generated R_0-algebra, R is Noetherian by **(16.11)**. Since M is a finitely generated R-module, obviously so is $M(-k_1)$. Hence, so are both K and L by **(16.15)**(2). Set $R' := R_0[x_2, \dots, x_r]$. Since x_1 acts as 0 on K and L, they are finitely generated R'-modules. Therefore, $H(K, t)$ and $H(L, t)$ are defined, and they may be written in the desired form by induction on r.

By definition, $M(-k_1)_n := M_{n-k_1}$; hence, $H(M(-k_1), t) = t^{k_1}H(M, t)$. Therefore, Additivity of Length, **(19.8)**, and the previous paragraph yield

$$(1-t^{k_1})H(M, t) = H(L, t) - H(K, t) = e(t)/t^l(1-t^{k_2})\cdots(1-t^{k_r}).$$

Thus the assertion holds. □

COROLLARY **(20.8)**. — *Under the conditions of* **(20.7)**, *assume that* $M \neq 0$ *and* $R = R_0[x_1, \dots, x_r]$ *with* $x_i \in R_1$. *Then* $H(M, t)$ *can be written uniquely in the form* $e(t)/t^l(1-t)^d$ *where* $e(t) \in \mathbb{Z}[t]$ *with* $e(0) \neq 0$ *and* $e(1) \neq 0$ *and where* $l \in \mathbb{Z}$ *and* $r \geq d \geq 0$; *further, there is a polynomial* $h(M, n) \in \mathbb{Q}[n]$ *with degree* $d-1$ *and leading coefficient* $e(1)/(d-1)!$ *such that* $\ell(M_n) = h(M, n)$ *for* $n \geq \deg(e(t)) - l$.

PROOF: We may take $k_i = 1$ for all i in the proof of **(20.7)**. Hence $H(M, t)$ is of the form $e(t)(1-t)^s/t^l(1-t)^r$ with $e(0) \neq 0$ and $e(1) \neq 0$ and $l \in \mathbb{Z}$. Set $d := r - s$. Then $d \geq 0$ since $H(M, 1) > 0$ as $M \neq 0$. Thus $H(M, t)$ is of the asserted form. This form is unique owing to the uniqueness of factorization of polynomials.

Say $e(t) = \sum_{i=0}^{N} e_i t^i$. Now, $(1-t)^{-d} = \sum \binom{-d}{n}(-t)^n = \sum \binom{d-1+n}{d-1} t^n$. Hence $\ell(M_n) = \sum_{i=0}^{N} e_i \binom{d-1+n+l-i}{d-1}$ for $n + l \geq N$. But $\binom{d-1+n-i}{d-1} = n^{d-1}/(d-1)! + \cdots$. Therefore, $\ell(M_n) = e(1)n^{d-1}/(d-1)! + \cdots$, as asserted. □

EXERCISE **(20.9)**. — Let k be a field, $P := k[X, Y, Z]$ the polynomial ring in three variables, $f \in P$ a homogeneous polynomial of degree $d \geq 1$. Set $R := P/\langle f \rangle$. Find the coefficients of the Hilbert Polynomial $h(R, n)$ explicitly in terms of d.

EXERCISE **(20.10)**. — Under the conditions of **(20.8)**, assume there is a homogeneous nonzerodivisor $f \in R$ with $M_f = 0$. Prove $\deg\big(h(R, n)\big) > \deg\big(h(M, n)\big)$; start with the case $M := R/\langle f^k \rangle$.

(20.11) (*Filtrations*). — Let R be an arbitrary ring, $\mathfrak{q}$ an ideal, and M a module. A **filtration** of M is an infinite descending chain of submodules:

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots . \tag{20.11.1}$$

We call it a **$\mathfrak{q}$-filtration** if $\mathfrak{q}M_n \subset M_{n+1}$ for all n, and a **stable $\mathfrak{q}$-filtration** if also $\mathfrak{q}M_n = M_{n+1}$ for $n \gg 0$, or equivalently, if also there is an m with $\mathfrak{q}^n M_m = M_{n+m}$ for $n \geq 0$. For example, setting $M_n := \mathfrak{q}^n M$, we get a stable $\mathfrak{q}$-filtration; we call it the **$\mathfrak{q}$-adic filtration**.

The $\mathfrak{q}$-adic filtration of R yields a graded ring $G_{\mathfrak{q}}(R)$ or $G(R)$, defined by

$$G(R) := \textstyle\bigoplus_{n \geq 0} G(R)_n \quad \text{where} \quad G(R)_n := \mathfrak{q}^n/\mathfrak{q}^{n+1}.$$

We obtain the product of an element in $\mathfrak{q}^i/\mathfrak{q}^{i+1}$ and one in $\mathfrak{q}^j/\mathfrak{q}^{j+1}$ by choosing a representative of each, forming their product, and taking its residue in $\mathfrak{q}^{i+j}/\mathfrak{q}^{i+j+1}$. We call $G(R)$ the **associated graded ring**.

Similarly, if **(20.11.1)** is a $\mathfrak{q}$-filtration, then we obtain a graded $G(R)$-module

$$G_{\mathfrak{q}}(M) := G(M) := \textstyle\bigoplus_{n \geq 0} G(M)_n \quad \text{where} \quad G(M)_n := M_n/M_{n+1}.$$

If all the quotients M/M_n of the filtration **(20.11.1)** are of finite length, then we call $n \mapsto \ell(M/M_n)$ the **Hilbert–Samuel Function**, and the generating function

$$P(M_\bullet, t) := \textstyle\sum_{n \geq 0} \ell(M/M_n) t^n$$

the **Hilbert–Samuel Series**. If the function $n \mapsto \ell(M/M_n)$ is, for $n \gg 0$, a polynomial $p(M_\bullet, n)$, then we call it the **Hilbert–Samuel Polynomial.** If the filtration is the $\mathfrak{q}$-adic filtration, we also denote $P(M_\bullet, t)$ and $p(M_\bullet, n)$ by $P_{\mathfrak{q}}(M, t)$ and $p_{\mathfrak{q}}(M, n)$.

LEMMA **(20.12)**. — *Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, M a finitely generated module with a stable $\mathfrak{q}$-filtration. Then $G(R)$ is generated as an $R/\mathfrak{q}$-algebra by finitely many elements of $\mathfrak{q}/\mathfrak{q}^2$, and $G(M)$ is a finitely generated $G(R)$-module.*

PROOF: Since R is Noetherian, $\mathfrak{q}$ is a finitely generated ideal, say by $x_1, \dots, x_r$. Then, clearly, the residues of the x_i in $\mathfrak{q}/\mathfrak{q}^2$ generate $G(R)$ as a $R/\mathfrak{q}$-algebra.

Say the filtration is $M = M_0 \supset M_1 \supset \cdots$. Since it is stable, there is an m with $\mathfrak{q}^n M_m = M_{n+m}$ for $n \geq 0$. Hence $G(M)$ is generated by M_0/M_1, ..., M_m/M_{m+1} over $G(R)$. But R is Noetherian and M is finitely generated over R; hence, every M_i is finitely generated over R. Therefore, every M_n/M_{n+1} is finitely generated over $R/\mathfrak{q}$. Thus $G(M)$ is a finitely generated $G(R)$-module. □

THEOREM **(20.13)** (Samuel). — *Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, M a finitely generated module with a stable $\mathfrak{q}$-filtration $M = M_0 \supset M_1 \supset \cdots$. Assume $\ell(M/\mathfrak{q}M) < \infty$. Then $\ell(M_n/M_{n+1}) < \infty$ and $\ell(M/M_n) < \infty$ for every n; further,*

$$P(M_\bullet, t) = H(G(M), t)\, t/(1-t).$$

PROOF: Set $\mathfrak{a} := \operatorname{Ann}(M)$. Set $R' := R/\mathfrak{a}$ and $\mathfrak{q}' := (\mathfrak{a} + \mathfrak{q})/\mathfrak{a}$. Then $R'/\mathfrak{q}'$ is Noetherian as R is. Further, M can be viewed as a finitely generated R'-module, and $M = M_0 \supset M_1 \supset \cdots$ as a stable $\mathfrak{q}'$-filtration. So $G(R')$ is generated as a $R'/\mathfrak{q}'$-algebra by finitely many elements of degree 1, and $G(M)$ is a finitely generated $G(R')$-module by **(20.12)**. Therefore, each M_n/M_{n+1} is a finitely generated $R'/\mathfrak{q}'$-module by **(20.2)** or by the proof of **(20.12)**.

On the other hand, **(13.1)** and **(13.6)**(3) and **(13.10)** yield, respectively,

$$\mathbf{V}(\mathfrak{a} + \mathfrak{q}) = \mathbf{V}(\mathfrak{a}) \bigcap \mathbf{V}(\mathfrak{q}) = \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q}) = \operatorname{Supp}(M/\mathfrak{q}M).$$

Hence $\mathbf{V}(\mathfrak{a} + \mathfrak{q})$ consists entirely of maximal ideals, because $\operatorname{Supp}(M/\mathfrak{q}M)$ does by **(19.4)** as $\ell(M/\mathfrak{q}M) < \infty$. Thus $\dim(R'/\mathfrak{q}') = 0$. But $R'/\mathfrak{q}'$ is Noetherian. Therefore, $R'/\mathfrak{q}'$ is Artinian by Akizuki's Theorem, **(19.10)**.

Therefore, $\ell(M_n/M_{n+1}) < \infty$ for every n by **(19.11)**. Form the exact sequence

$$0 \to M_n/M_{n+1} \to M/M_{n+1} \to M/M_n \to 0.$$

Then Additivity of Length, **(19.8)**, yields

$$\ell(M_n/M_{n+1}) = \ell(M/M_{n+1}) - \ell(M/M_n).$$

So induction on n yields $\ell(M/M_{n+1}) < \infty$ for every n. Further, multiplying that equation by t^n and summing over n yields the desired expression in another form:

$$H(G(M), t) = (t^{-1} - 1)P(M_\bullet, t) = P(M_\bullet, t)\,(1-t)/t. \qquad \square$$

COROLLARY **(20.14)**. — *Under the conditions of* **(20.13)**, *assume $\mathfrak{q}$ is generated by r elements and $M \neq 0$. Then $P(M_\bullet, t)$ can be written uniquely in the form $e(t)/t^{l-1}(1-t)^{d+1}$ where $e(t) \in \mathbb{Z}[t]$ with $e(0) \neq 0$ and $e(1) \neq 0$ and where $l \in \mathbb{Z}$ and $r \geq d \geq 0$; further, there is a polynomial $p(M_\bullet, n) \in \mathbb{Q}[n]$ with degree d and leading coefficient $e(1)/d!$ such that $\ell(M/M_n) = p(M_\bullet, n)$ for $n \geq \deg(e(t)) - l$.*

Finally, $p_{\mathfrak{q}}(M, n) - p(M_\bullet, n)$ is a polynomial with degree at most $d-1$ and nonnegative leading coefficient; further, d and $e(1)$ are the same for every stable $\mathfrak{q}$-filtration.

PROOF: The proof of **(20.13)** shows that $G(R')$ and $G(M)$ satisfy the hypotheses of **(20.8)**. So **(20.8)** yields a certain form for $H(G(M), t)$. Then **(20.13)** yields the asserted form for $P(M_\bullet, t)$. In turn, that form yields the asserted polynomial $p(M_\bullet, n)$ by the argument in the second paragraph of the proof of **(20.8)**.

Finally, as $M = M_0 \supset M_1 \supset \cdots$ is a stable $\mathfrak{q}$-filtration, there's an m such that

$$M_n \supset \mathfrak{q}^n M \supset \mathfrak{q}^n M_m = M_{n+m}$$

for all $n \geq 0$. Dividing into M and extracting lengths yields

$$\ell(M/M_n) \leq \ell(M/\mathfrak{q}^n M) \leq \ell(M/M_{n+m}).$$

Therefore, for large n, we get

$$p(M_\bullet, n) \leq p_{\mathfrak{q}}(M, n) \leq p(M_\bullet, n+m).$$

The two extremes are polynomials in n with the same degree and leading coefficient, say d and c. Dividing by n^d and letting $n \to \infty$, we conclude that the polynomial $p_{\mathfrak{q}}(M, n)$ also has degree d and leading coefficient c.

Thus the degree and leading coefficient are the same for every stable $\mathfrak{q}$-filtration. Further $p_{\mathfrak{q}}(M, n) - p(M_\bullet, n)$ has degree at most $d-1$ and positive leading coefficient, owing to cancellation of the two leading terms and to the first inequality. □

Exercise **(20.15)**. — Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, and M a finitely generated module. Assume $\ell(M/\mathfrak{q}M) < \infty$. Set $\mathfrak{m} := \sqrt{\mathfrak{q}}$. Show

$$\deg p_{\mathfrak{m}}(M, n) = \deg p_{\mathfrak{q}}(M, n).$$

(20.16) (*Rees Algebras*). — Let R be an arbitrary ring, $\mathfrak{q}$ an ideal. The sum

$$\mathcal{R}(\mathfrak{q}) := \textstyle\bigoplus_{n \geq 0} \mathfrak{q}^n$$

is, canonically, a graded ring, with R as zeroth graded component and $\mathfrak{q}$ as first. We call $\mathcal{R}(\mathfrak{q})$ the **Rees Algebra** of $\mathfrak{q}$.

Let M be a module with a $\mathfrak{q}$-filtration $M = M_0 \supset M_1 \supset \cdots$. Then the sum

$$\mathcal{R}(M_\bullet) := \textstyle\bigoplus_{n \geq 0} M_n$$

is canonically a module over the Rees Algebra $\mathcal{R}(\mathfrak{q})$.

Lemma **(20.17)**. — *Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, and M a finitely generated module with a $\mathfrak{q}$-filtration. Then $\mathcal{R}(\mathfrak{q})$ is generated as an R-algebra by finitely many elements of $\mathfrak{q}$, and $\mathcal{R}(M_\bullet)$ is a finitely generated $\mathcal{R}(\mathfrak{q})$-module if and only if the filtration is stable.*

Proof: Say the filtration is $M = M_0 \supset M_1 \supset \cdots$. Suppose $\mathcal{R}(M_\bullet)$ is generated over $\mathcal{R}(\mathfrak{q})$ by $m_1, \ldots, m_s$. Say $m_i = \sum_{j=0}^{\mu} m_{ij}$ with $m_{ij} \in M_j$. Then for any $n \geq 0$, any $m \in M_{n+\mu}$ is a sum $m = \sum f_{ij} m_{ij}$ where $f_{ij} \in \mathfrak{q}^{n+\mu-j}$. But $\mathfrak{q}^{n+\mu-j} = \mathfrak{q}^n \mathfrak{q}^{\mu-j}$. Thus $M_{n+\mu} = \mathfrak{q}^n M_\mu$; that is, the filtration is stable.

The rest of the proof is similar to that of **(20.12)**, but simpler. □

Lemma **(20.18)** (Artin–Rees). — *Let R be a Noetherian ring, M a finitely generated module, N a submodule, $\mathfrak{q}$ an ideal, $M = M_0 \supset M_1 \supset \cdots$ a stable $\mathfrak{q}$-filtration. For $n \geq 0$, set $N_n := N \cap M_n$. Then $N = N_0 \supset N_1 \supset \cdots$ is a stable $\mathfrak{q}$-filtration.*

Proof: By **(20.17)**, the Rees Algebra $\mathcal{R}(\mathfrak{q})$ is finitely generated over R, so Noetherian by **(16.11)**. By **(20.17)**, the module $\mathcal{R}(M_\bullet)$ is finitely generated over $\mathcal{R}(\mathfrak{q})$, so Noetherian by **(16.18)**. Clearly, $N = N_0 \supset N_1 \supset \cdots$ is a $\mathfrak{q}$-filtration; hence, $\mathcal{R}(N_\bullet)$ is a submodule of $\mathcal{R}(M_\bullet)$, so Noetherian by **(16.15)**(2), so finitely generated by **(16.18)**. Hence, $N = N_0 \supset N_1 \supset \cdots$ is stable by **(20.17)**, as desired. □

EXERCISE **(20.19)**. — Derive the Krull Intersection Theorem, **(18.26)**, from the Artin–Rees Lemma, **(20.18)**.

PROPOSITION **(20.20)**. — *Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, and*

$$0 \to M' \to M \to M'' \to 0$$

an exact sequence of finitely generated modules. Then $M/\mathfrak{q}M$ has finite length if and only if $M'/\mathfrak{q}M'$ and $M''/\mathfrak{q}M''$ do. If so, then the polynomial

$$p_{\mathfrak{q}}(M', n) - p_{\mathfrak{q}}(M, n) + p_{\mathfrak{q}}(M'', n)$$

has degree at most $\deg\bigl(p_{\mathfrak{q}}(M', n)\bigr) - 1$ and has positive leading coefficient; also then

$$\deg p_{\mathfrak{q}}(M, n) = \max\{\, \deg p_{\mathfrak{q}}(M', n),\, \deg p_{\mathfrak{q}}(M'', n)\,\}.$$

PROOF: First off, **(13.10)** and **(13.6)**(1) and **(13.10)** again yield

$$\begin{aligned}\operatorname{Supp}(M/\mathfrak{q}M) &= \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q}) = \bigl(\operatorname{Supp}(M') \bigcup \operatorname{Supp}(M'')\bigr) \bigcap \mathbf{V}(\mathfrak{q}) \\ &= \bigl(\operatorname{Supp}(M') \bigcap \mathbf{V}(\mathfrak{q})\bigr) \bigcup \bigl(\operatorname{Supp}(M'') \bigcap \mathbf{V}(\mathfrak{q})\bigr) \\ &= \operatorname{Supp}(M'/\mathfrak{q}M') \bigcup \operatorname{Supp}(M''/\mathfrak{q}M'').\end{aligned}$$

Hence $M/\mathfrak{q}M$ has finite length if and only if $M'/\mathfrak{q}M'$ and $M''/\mathfrak{q}M''$ do by **(19.4)**.

For $n \geq 0$, set $M'_n := M' \bigcap \mathfrak{q}^n M$. Then $M' = M'_0 \supset M'_1 \supset \cdots$ is a stable $\mathfrak{q}$-filtration by the Artin–Rees Lemma. Form this canonical commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & M'_n & \to & \mathfrak{q}^n M & \to & \mathfrak{q}^n M'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

Its rows are exact. So the Nine Lemma yields this exact sequence:

$$0 \to M'/M'_n \to M/\mathfrak{q}^n M \to M''/\mathfrak{q}^n M'' \to 0.$$

Assume $M/\mathfrak{q}M$ has finite length. Then Additivity of Length and **(20.14)** yield

$$p(M'_\bullet, n) - p_{\mathfrak{q}}(M, n) + p_{\mathfrak{q}}(M'', n) = 0. \qquad \textbf{(20.20.1)}$$

Hence $p_{\mathfrak{q}}(M', n) - p_{\mathfrak{q}}(M, n) + p_{\mathfrak{q}}(M'', n)$ is equal to $p_{\mathfrak{q}}(M', n) - p(M'_\bullet, n)$. But by **(20.14)** again, the latter is a polynomial with degree at most $\deg\bigl(p_{\mathfrak{q}}(M', n)\bigr) - 1$ and positive leading coefficient.

Finally, $\deg p_{\mathfrak{q}}(M, n) = \max\{\deg p(M'_\bullet, n), \deg p_{\mathfrak{q}}(M'', n)\}$ owing to **(20.20.1)**, as the leading coefficients of $p(M'_\bullet, n)$ and $p_{\mathfrak{q}}(M'', n)$ are both positive, so cannot cancel. But $\deg p(M'_\bullet, n) = \deg p_{\mathfrak{q}}(M', n)$ by **(20.14)**, completing the proof. □

20. Appendix: Homogeneity

(20.21) (*Homogeneity*). — Let R be a graded ring, and $M = \bigoplus M_n$ a graded module. We call the M_n the **homogeneous components** of M.

Given $m \in M$, write $m = \sum m_n$ with $m_n \in M_n$. Call the finitely many nonzero m_n the **homogeneous components** of m. Say that a component m_n is **homogeneous of degree** n. If n is lowest, call m_n the **initial component** of m.

Call a submodule $N \subset M$ **homogeneous** if, whenever $m \in N$, also $m_n \in N$, or equivalently, $N = \bigoplus(M_n \cap N)$.

Call a map $\alpha\colon M' \to M$ of graded modules with components M'_n and M_n **homogeneous of degree** r if $\alpha(M'_n) \subset M_{n+r}$ for all n. If so, then clearly $\mathrm{Ker}(\alpha)$ is a homogeneous submodule of M. Further, $\mathrm{Coker}(\alpha)$ is canonically graded, and the quotient map $M \to \mathrm{Coker}(\alpha)$ is homogeneous of degree 0.

Exercise **(20.22)**. — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded R-module, and $N = \bigoplus N_n$ a homogeneous submodule. Assume R_0 is Artinian, R is a finitely generated R_0-algebra, and M is a finitely generated R-module. Set

$$N' := \{\, m \in M \mid \text{there is } n_0 \text{ such that } R_n m \in N \text{ for all } n \geq n_0 \,\}.$$

Prove that N' is a homogeneous submodule of M with the same Hilbert polynomial as N, and that N' is the largest such submodule.

Proposition **(20.23)**. — *Let R be a Noetherian graded ring, M a nonzero finitely generated graded module, Q a homogeneous submodule. Suppose Q possesses this property: given any homogeneous $x \in R$ and homogeneous $m \in M$ with $xm \in Q$ but $m \notin Q$, necessarily $x \in \mathfrak{p} := \mathrm{nil}(M/Q)$. Then $\mathfrak{p}$ is prime, and Q is $\mathfrak{p}$-primary.*

Proof: Given $x \in R$ and $m \in M$, decompose them into their homogeneous components: $x = \sum_{i \geq r} x_i$ and $m = \sum_{j \geq s} m_j$. Suppose $xm \in Q$, but $m \notin Q$. Then $m_t \notin Q$ for some t; take t minimal. Set $m' := \sum_{j<t} m_j$. Then $m' \in Q$. Set $m'' := m - m'$. Then $xm'' \in Q$.

Either $x_s m_t$ vanishes or it's the initial component of xm''. But Q is homogeneous. So $x_s m_t \in Q$. But $m_t \notin Q$. Hence $x_s \in \mathfrak{p}$ by the hypothesis. Say $x_s, \ldots, x_u \in \mathfrak{p}$ with u maximal. Set $x' := \sum_{i=s}^{u} x_i$. Then $x' \in \mathfrak{p}$. So $x'^k \in \mathrm{Ann}(M/Q)$ for some $k \geq 1$. So $x'^k m'' \in Q$. Set $x'' := x - x'$. Since $xm'' \in Q$, also $x''^k m'' \in Q$.

Suppose $x \notin \mathfrak{p}$. Then $x'' \neq 0$. And its initial component is x_v with $v > u$. Either $x''_v m''_t$ vanishes or it is the initial component of xm. But Q is homogeneous. So $x_v m_t \in Q$. But $m_t \notin Q$. Hence $x_v \in \mathfrak{p}$ by the hypothesis, contradicting $v > u$. Thus $x \in \mathfrak{p}$. Thus Q is $\mathfrak{p}$-primary by **(18.4)**. □

Exercise **(20.24)**. — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, and M a graded module. Prove that $\sqrt{\mathfrak{a}}$ and $\mathrm{Ann}(M)$ and $\mathrm{nil}(M)$ are homogeneous.

Exercise **(20.25)**. — Let R be a graded ring, M a graded module, and Q a primary submodule. Let $Q^* \subset Q$ be the submodule generated by the homogeneous elements of Q. Then Q^* is primary.

THEOREM **(20.26)**. — *Let R be a Noetherian graded ring, M a finitely generated graded module, N a homogeneous submodule. Then all the associated primes of M/N are homogeneous, and N admits an irredundant primary decomposition in which all the primary submodules are homogeneous.*

PROOF: Let $N = \bigcap Q_j$ be any primary decomposition; one exists by **(18.20)**. Let $Q_j^* \subset Q_j$ be the submodule generated by the homogeneous elements of Q_j. Trivially, $\bigcap Q_j^* \subset \bigcap Q_j = N \subset \bigcap Q_j^*$. Further, each Q_j^* is clearly homogeneous, and is primary by **(20.25)**. Thus $N = \bigcap Q_j^*$ is a primary decomposition into homogeneous primary submodules. And, owing to **(18.18)**, it is irredundant if $N = \bigcap Q_j$ is, as both decompositions have minimal length. Finally, M/Q_j^* is graded by **(20.21)**; so each associated prime is homogeneous by **(18.19)** and **(20.24)**. □

(20.27) (*Graded Domains*). — Let $R = \bigoplus_{n\geq 0} R_n$ be a graded domain, and set $K := \mathrm{Frac}(R)$. We call $z \in K$ **homogeneous of degree** $n \in \mathbb{Z}$ if $z = x/y$ with $x \in R_m$ and $y \in R_{m-n}$. Clearly, n is well defined.

Let K_n be the set of all such z, plus 0. Then $K_m K_n \subset K_{m+n}$. Clearly, the canonical map $\bigoplus_{n\in\mathbb{Z}} K_n \to K$ is injective. Thus $\bigoplus_{n\geq 0} K_n$ is a graded subring of K. Further, K_0 is a field.

The n with $K_n \neq 0$ form a subgroup of $\mathbb{Z}$. So by renumbering, we may assume $K_1 \neq 0$. Fix any nonzero $x \in K_1$. Clearly, x is transcendental over K_0. If $z \in K_n$, then $z/x^n \in K_0$. Hence $R \subset K_0[x]$. So **(2.3)** yields $K = K_0(x)$.

Any $w \in \bigoplus K_n$ can be written $w = a/b$ with $a, b \in R$ and b homogeneous: say $w = \sum(a_n/b_n)$ with $a_n, b_n \in R$ homogeneous; set $b := \prod b_n$ and $a := \sum(a_n b/b_n)$.

THEOREM **(20.28)**. — *Let R be a Noetherian graded domain, $K := \mathrm{Frac}(R)$, and $\overline{R}$ the integral closure of R in K. Then $\overline{R}$ is a graded subring of K.*

PROOF: Use the setup of **(20.27)**. Since $K_0[x]$ is a polynomial ring over a field, it is normal by **(10.26)**. Hence $\overline{R} \subset K_0[x]$. So every $y \in R$ can be written as $y = \sum_{i=r}^{r+n} y_i$, with y_i homogeneous and nonzero. Let's show $y_i \in \overline{R}$ for all i.

Since y is integral over R, the R-algebra $R[y]$ is module finite by **(10.15)**. So **(20.27)** yields a homogeneous $b \in R$ with $bR[y] \subset R$. Hence $by^j \in R$ for all $j \geq 0$. But R is graded. Hence $by_r^j \in R$. Set $z := 1/b$. Then $y_r^j \in Rz$. Since R is Noetherian, the R-algebra $R[y_r]$ is module finite. Hence $y_r \in \overline{R}$. Then $y - y_r \in \overline{R}$. Thus $y_i \in \overline{R}$ for all i by induction on n. Thus $\overline{R}$ is graded. □

EXERCISE **(20.29)**. — Under the conditions of **(20.8)**, assume that R is a domain and that its integral closure $\overline{R}$ in $\mathrm{Frac}(R)$ is a finitely generated R-module.

(1) Prove that there is a homogeneous $f \in R$ with $R_f = \overline{R}_f$.

(2) Prove that the Hilbert Polynomials of R and $\overline{R}$ have the same degree and same leading coefficient.

21. Dimension

The dimension of a module is defined as the sup of the lengths of the chains of primes in its support. The Dimension Theorem, which we prove, characterizes the dimension of a nonzero finitely generated semilocal module over a Noetherian ring in two ways. First, the dimension is the degree of the Hilbert–Samuel Polynomial formed with the radical of the ring. Second, the dimension is the smallest number of elements in the radical that span a submodule of finite colength.

Next, in an arbitrary Noetherian ring, we study the height of a prime: the length of the longest chain of subprimes. We bound the height by the minimal number of generators of an ideal over which the prime is minimal. In particular, when this number is 1, we obtain Krull's Principal Ideal Theorem. Finally, we study regular local rings: Noetherian local rings whose maximal ideal has the minimum number of generators, namely, the dimension.

(21.1) (*Dimension of a module*). — Let R be a ring, and M a nonzero module. The **dimension** of M, denoted $\dim(M)$, is defined by this formula:

$$\dim(M) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \text{ in } \operatorname{Supp}(M)\,\}.$$

Assume R is Noetherian, and M is finitely generated. Then M has finitely many minimal (associated) primes by **(17.19)**. They are also the minimal primes $\mathfrak{p}_0 \in \operatorname{Supp}(M)$ by **(17.16)**. Thus **(1.7)** yields

$$\dim(M) = \max\{\, \dim(R/\mathfrak{p}_0) \mid \mathfrak{p}_0 \in \operatorname{Supp}(M) \text{ is minimal}\,\}. \qquad \textbf{(21.1.1)}$$

(21.2) (*Parameters*). — Let R be a ring, M a nonzero module. Denote the intersection of the maximal ideals in $\operatorname{Supp}(M)$ by $\operatorname{rad}(M)$, and call it the **radical** of M. If there are only finitely many such maximal ideals, call M **semilocal**.Call an ideal $\mathfrak{q}$ a **parameter ideal of** M if $\mathfrak{q} \subset \operatorname{rad}(M)$ and $M/\mathfrak{q}M$ is Artinian.

Assume M is finitely generated. Then $\operatorname{Supp}(M) = \mathbf{V}(\operatorname{Ann}(M))$ by **(13.6)**(3). Hence M is semilocal if and only if $R/\operatorname{Ann}(M)$ is a semilocal ring.

Assume, in addition, R is Noetherian; so M is Noetherian by **(16.18)**. Fix an ideal $\mathfrak{q}$. Then **(19.5)** yields that $M/\mathfrak{q}M$ is Artinian if and only if $\ell(M/\mathfrak{q}M) < \infty$.

However, $\ell(M/\mathfrak{q}M) < \infty$ if and only if $\operatorname{Supp}(M/\mathfrak{q}M)$ consists of finitely many maximal ideals by **(19.4)** and **(17.20)**. Further, **(13.10)**, **(13.6)**(3), and **(13.1)** yield

$$\operatorname{Supp}(M/\mathfrak{q}M) = \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q}) = \mathbf{V}(\operatorname{Ann}(M)) \bigcap \mathbf{V}(\mathfrak{q}) = \mathbf{V}(\operatorname{Ann}(M) + \mathfrak{q}).$$

Set $\mathfrak{q}' := \operatorname{Ann}(M) + \mathfrak{q}$. Thus $M/\mathfrak{q}M$ is Artinian if and only if $\mathbf{V}(\mathfrak{q}')$ consists of finitely many maximal ideals; so by **(19.10)**, if and only if $R/\mathfrak{q}'$ is Artinian. But **(19.15)** implies that $R/\mathfrak{q}'$ is Artinian if and only if $\mathfrak{q}'$ contains a product of maximal ideals each of which contains $\mathfrak{q}'$. Then each lies in $\operatorname{Supp}(M)$, so contains $\operatorname{rad}(M)$.

Set $\mathfrak{m} := \operatorname{rad}(M)$. Thus if $R/\mathfrak{q}'$ is Artinian, then $\mathfrak{q}' \supset \mathfrak{m}^n$ for some $n > 0$.

Assume, in addition, M is semilocal, so that $\operatorname{Supp}(M)$ contains only finitely many maximal ideals. Then their product is contained in $\mathfrak{m}$. Thus, conversely, if $\mathfrak{q}' \supset \mathfrak{m}^n$ for some $n > 0$, then $R/\mathfrak{q}'$ is Artinian. Thus $\mathfrak{q}$ *is a parameter ideal if and only if*

$$\mathfrak{m} \supset \mathfrak{q}' \supset \mathfrak{m}^n \quad \textit{for some } n, \qquad \textbf{(21.2.1)}$$

or by **(3.20)** *if and only if* $\mathfrak{m} = \sqrt{\mathfrak{q}'}$, or by **(13.1)** *if and only if* $\mathbf{V}(\mathfrak{m}) = \mathbf{V}(\mathfrak{q}')$. In particular, $\mathfrak{m}^n$ *is a parameter ideal for any* n.

Assume $\mathfrak{q}$ is a parameter ideal. Then the Hilbert–Samuel polynomial $p_{\mathfrak{q}}(M, n)$ exists by **(20.14)**. Similarly, $p_{\mathfrak{m}}(M, n)$ exists, and the two polynomials have the same degree by **(20.15)** since $\mathfrak{m} = \sqrt{\mathfrak{q}'}$ and $p_{\mathfrak{q}'}(M, n) = p_{\mathfrak{q}}(M, n)$. Thus the degree is the same for every parameter ideal. Denote this common degree by $d(M)$.

Alternatively, $d(M)$ can be viewed as the order of pole at 1 of the Hilbert series $H(G_{\mathfrak{q}}(M), t)$. Indeed, that order is 1 less than the order of pole at 1 of the Hilbert–Samuel series $P_{\mathfrak{q}}(M, t)$ by **(20.13)**. In turn, the latter order is $d(M)+1$ by **(20.14)**.

Denote by $s(M)$ the smallest s such that there are $x_1, \dots, x_s \in \mathfrak{m}$ with

$$\ell(M/\langle x_1, \dots, x_s\rangle M) < \infty. \tag{21.2.2}$$

By convention, if $\ell(M) < \infty$, then $s(M) = 0$. We say that $x_1, \dots, x_s \in \mathfrak{m}$ form a **system of parameters** (sop) for M if $s = s(M)$ and **(21.2.2)** holds. Note that a sop generates a parameter ideal.

LEMMA **(21.3)**. — *Let R be a Noetherian ring, M a nonzero Noetherian semilocal module, $\mathfrak{q}$ a parameter ideal of M, and $x \in \operatorname{rad}(M)$. Set $K := \operatorname{Ker}(M \xrightarrow{\mu_x} M)$.*

1. *Then $s(M) \le s(M/xM) + 1$.*
2. *Then $\dim(M/xM) \le \dim(M) - 1$ if $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$.*
3. *Then $\deg\big(p_{\mathfrak{q}}(K, n) - p_{\mathfrak{q}}(M/xM, n)\big) \le d(M) - 1$.*

PROOF: For (1), set $s := s(M/xM)$. There are $x_1, \dots, x_s \in \operatorname{rad}(M/xM)$ with

$$\ell(M/\langle x, x_1, \dots, x_s\rangle M) < \infty.$$

Now, $\operatorname{Supp}(M/xM) = \operatorname{Supp}(M) \cap \mathbf{V}(\langle x\rangle)$ by **(13.10)**. However, $x \in \operatorname{rad}(M)$. Hence, $\operatorname{Supp}(M/xM)$ and $\operatorname{Supp}(M)$ have the same maximal ideals. Therefore, $\operatorname{rad}(M/xM) = \operatorname{rad}(M)$. Hence $s(M) \le s + 1$. Thus (1) holds.

To prove (2), take a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in $\operatorname{Supp}(M/xM)$. Now, $\operatorname{Supp}(M/xM) = \operatorname{Supp}(M) \cap \mathbf{V}(\langle x\rangle)$ by **(13.10)**. So $x \in \mathfrak{p}_0 \in \operatorname{Supp}(M)$. So, by hypothesis, $\dim(R/\mathfrak{p}_0) < \dim(M)$. Hence $r \le \dim(M) - 1$. Thus (2) holds.

To prove (3), set $xM := \operatorname{Im}(\mu_x)$, and form these two exact sequences:

$$0 \to K \to M \to xM \to 0, \quad \text{and} \quad 0 \to xM \to M \to M/xM \to 0.$$

Then **(20.20)** yields $d(K) \le d(M)$ and $d(xM) \le d(M)$. So by **(20.20)** again, both $p_{\mathfrak{q}}(K, n) + p_{\mathfrak{q}}(xM, n) - p_{\mathfrak{q}}(M, n)$ and $p_{\mathfrak{q}}(xM, n) + p_{\mathfrak{q}}(M/xM, n) - p_{\mathfrak{q}}(M, n)$ are of degree at most $d(M) - 1$. So their difference is too. Thus (3) holds. □

THEOREM **(21.4)** (Dimension). — *Let R be a Noetherian ring, M a nonzero finitely generated semilocal module. Then*

$$\dim(M) = d(M) = s(M) < \infty.$$

PROOF: Let's prove a cycle of inequalities. Set $\mathfrak{m} := \operatorname{rad}(M)$. First, let's prove $\dim(M) \le d(M)$. We proceed by induction on $d(M)$. Suppose $d(M) = 0$. Then $\ell(M/\mathfrak{m}^n M)$ stabilizes. So $\mathfrak{m}^n M = \mathfrak{m}^{n+1} M$ for some n. Hence $\mathfrak{m}^n M = 0$ by Nakayama's Lemma applied over the semilocal ring $R/\operatorname{Ann}(M)$. Hence $\ell(M) < \infty$. So $\dim(M) = 0$ by **(19.4)**.

Suppose $d(M) \ge 1$. Take $\mathfrak{p}_0 \in \operatorname{Ass}(M)$ with $\dim(R/\mathfrak{p}_0) = \dim(M)$. Then M has a submodule N isomorphic to $R/\mathfrak{p}_0$ by **(17.2)**. Further, $d(N) \le d(M)$ by **(20.20)**.

Take a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in $\operatorname{Supp}(N)$. If $r = 0$, then $r \le d(M)$.

Suppose $r \geq 1$. Then there's an $x_1 \in \mathfrak{p}_1 - \mathfrak{p}_0$. Further, since $\mathfrak{p}_0$ is not maximal, for each maximal ideal $\mathfrak{n}$ in $\operatorname{Supp}(M)$, there is an $x_\mathfrak{n} \in \mathfrak{n} - \mathfrak{p}_0$. Set $x := x_1 \prod x_\mathfrak{n}$. Then $x \in (\mathfrak{p}_1 \cap \mathfrak{m}) - \mathfrak{p}_0$. Then $\mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ lies in $\operatorname{Supp}(N) \bigcap \mathbf{V}(\langle x \rangle)$. But the latter is equal to $\operatorname{Supp}(N/xN)$ by **(13.10)**. So $r - 1 \leq \dim(N/xN)$.

However, μ_x is injective on N as $N \simeq R/\mathfrak{p}_0$ and $x \notin \mathfrak{p}_0$. So **(21.3)**(3) yields $d(N/xN) \leq d(N) - 1$. But $d(N) \leq d(M)$. So $\dim(N/xN) \leq d(N/xN)$ by the induction hypothesis. Therefore, $r \leq d(M)$. Thus $\dim(M) \leq d(M)$.

Second, let's prove $d(M) \leq s(M)$. Let $\mathfrak{q}$ be a parameter ideal of M with $s(M)$ generators. Then $d(M) := \deg p_\mathfrak{q}(M, n)$. But $\deg p_\mathfrak{q}(M, n) \leq s(M)$ owing to **(20.14)**. Thus $d(M) \leq s(M)$.

Finally, let's prove $s(M) \leq \dim(M)$. Set $r := \dim(M)$, which is finite since $r \leq d(M)$ by the first step. The proof proceeds by induction on r. If $r = 0$, then M has finite length by **(19.4)**; so $s(M) = 0$.

Suppose $r \geq 1$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the primes of $\operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}_i) = r$. No $\mathfrak{p}_i$ is maximal as $r \geq 1$. So $\mathfrak{m}$ lies in no $\mathfrak{p}_i$. Hence, by Prime Avoidance **(3.12)**, there is an $x \in \mathfrak{m}$ such that $x \notin \mathfrak{p}_i$ for all i. So **(21.3)**(1), (2) yield $s(M) \leq s(M/xM) + 1$ and $\dim(M/xM) + 1 \leq r$. By the induction hypothesis, $s(M/xM) \leq \dim(M/xM)$. Hence $s(M) \leq r$, as desired. □

Corollary **(21.5)**. — *Let R be a Noetherian ring, M a nonzero Noetherian semi-local module, $x \in \operatorname{rad}(M)$. Then $\dim(M/xM) \geq \dim(M) - 1$, with equality if $x \notin \mathfrak{p}$ for $\mathfrak{p} \in \operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$; equality holds if $x \notin \operatorname{z.div}(M)$.*

Proof: By **(21.3)**(1), we have $s(M/xM) \geq s(M) - 1$. So the asserted inequality holds by **(21.4)**. If $x \notin \mathfrak{p} \in \operatorname{Supp}(M)$ when $\dim(R/\mathfrak{p}) = \dim(M)$, then **(21.3)**(2) yields the opposite inequality, so equality. Finally, if $x \notin \operatorname{z.div}(M)$, then $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$ owing to **(17.17)** and **(17.14)**. □

(21.6) (*Height*). — Let R be a ring, and $\mathfrak{p}$ a prime. The **height** of $\mathfrak{p}$, denoted $\operatorname{ht}(\mathfrak{p})$, is defined by this formula:

$$\operatorname{ht}(\mathfrak{p}) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{p} \,\}.$$

The bijective correspondence $\mathfrak{p} \mapsto \mathfrak{p}R_\mathfrak{p}$ of **(11.16)**(2) yields this formula:

$$\operatorname{ht}(\mathfrak{p}) = \dim(R_\mathfrak{p}). \tag{21.6.1}$$

Corollary **(21.7)**. — *Let R be a Noetherian ring, $\mathfrak{p}$ a prime. Then $\operatorname{ht}(\mathfrak{p}) \leq r$ if and only if $\mathfrak{p}$ is minimal containing an ideal generated by r elements.*

Proof: Assume $\mathfrak{p}$ is minimal containing an ideal $\mathfrak{a}$ generated by r elements. Now, any prime of $R_\mathfrak{p}$ containing $\mathfrak{a}R_\mathfrak{p}$ is of the form $\mathfrak{q}R_\mathfrak{p}$ where $\mathfrak{q}$ is a prime of R with $\mathfrak{a} \subset \mathfrak{q} \subset \mathfrak{p}$ by **(11.16)**. So $\mathfrak{q} = \mathfrak{p}$. Hence $\mathfrak{p}R_\mathfrak{p} = \sqrt{\mathfrak{a}R_\mathfrak{p}}$ by the Scheinnullstellensatz. Hence $r \geq s(R_\mathfrak{p})$ by **(21.2)**. But $s(R_\mathfrak{p}) = \dim(R_\mathfrak{p})$ by **(21.4)**, and $\dim(R_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p})$ by **(21.6.1)**. Thus $\operatorname{ht}(\mathfrak{p}) \leq r$.

Conversely, assume $\operatorname{ht}(\mathfrak{p}) \leq r$. Then $R_\mathfrak{p}$ has a parameter ideal $\mathfrak{b}$ generated by r elements, say $y_1, \ldots, y_r$ by **(21.6.1)** and **(21.4)**. Say $y_i = x_i/s_i$ with $s_i \notin \mathfrak{p}$. Set $\mathfrak{a} := \langle x_1, \ldots, x_r \rangle$. Then $\mathfrak{a}R_\mathfrak{p} = \mathfrak{b}$.

Suppose there is a prime $\mathfrak{q}$ with $\mathfrak{a} \subset \mathfrak{q} \subset \mathfrak{p}$. Then $\mathfrak{b} = \mathfrak{a}R_\mathfrak{p} \subset \mathfrak{q}R_\mathfrak{p} \subset \mathfrak{p}R_\mathfrak{p}$, and $\mathfrak{q}R_\mathfrak{p}$ is prime by **(11.16)**(2). But $\sqrt{\mathfrak{b}} = \mathfrak{p}R_\mathfrak{p}$. So $\mathfrak{q}R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$. Hence $\mathfrak{q} = \mathfrak{p}$ by **(11.16)**(2). Thus $\mathfrak{p}$ is minimal containing $\mathfrak{a}$, which is generated by r elements. □

EXERCISE **(21.8)**. — Let R be a Noetherian ring, and $\mathfrak{p}$ be a prime minimal containing $x_1, \dots, x_r$. Given r' with $1 \le r' \le r$, set $R' := R/\langle x_1, \dots, x_{r'}\rangle$ and $\mathfrak{p}' := \mathfrak{p}/\langle x_1, \dots, x_{r'}\rangle$. Assume $\operatorname{ht}(\mathfrak{p}) = r$. Prove $\operatorname{ht}(\mathfrak{p}') = r - r'$.

THEOREM **(21.9)** (Krull Principal Ideal). — *Let R be a Noetherian ring, $x \in R$, and $\mathfrak{p}$ a prime minimal containing x. If $x \notin \text{z.div}(R)$, then $\operatorname{ht}(\mathfrak{p}) = 1$.*

PROOF: We have $\operatorname{ht}(\mathfrak{p}) \le 1$ by **(21.7)**. But if $\operatorname{ht}(\mathfrak{p}) = 0$, then $\mathfrak{p} \in \operatorname{Ass}(R)$ by **(17.17)**, and so $x \in \text{z.div}(R)$ by **(17.14)**. □

EXERCISE **(21.10)**. — Let R be a domain. Prove that, if R is a UFD, then every height-1 prime is principal, and that the converse holds if R is Noetherian.

EXERCISE **(21.11)**. — (1) Let A be a Noetherian local ring, and $\mathfrak{p}$ a principal prime of height at least 1. Prove that A is a domain.

(2) Let k be a field, $P := k[[X]]$ the formal power series ring in one variable. Set $R := P \times P$. Prove that P is Noetherian and semilocal, and that P contains a principal prime $\mathfrak{p}$ of height 1, but that P is not a domain.

EXERCISE **(21.12)**. — Let R be a finitely generated algebra over a field. Assume R is a domain of dimension r. Let $x \in R$ be neither 0 nor a unit. Set $R' := R/\langle x\rangle$. Prove that $r - 1$ is the length of any chain of primes in R' of maximal length.

COROLLARY **(21.13)**. — *Let A and B be Noetherian local rings, $\mathfrak{m}$ and $\mathfrak{n}$ their maximal ideals. Let $\varphi\colon A \to B$ be a* ***local homomorphism****; that is, $\varphi(\mathfrak{m}) \subset \mathfrak{n}$. Then*

$$\dim(B) \le \dim(A) + \dim(B/\mathfrak{m}B),$$

with equality if B is flat over A.

PROOF: Set $s := \dim(A)$. By **(21.4)**, there is a parameter ideal $\mathfrak{q}$ generated by s elements. Then $\mathfrak{m}/\mathfrak{q}$ is nilpotent by **(21.2.1)**. Hence $\mathfrak{m}B/\mathfrak{q}B$ is nilpotent. It follows that $\dim(B/\mathfrak{m}B) = \dim(B/\mathfrak{q}B)$. But **(21.5)** yields $\dim(B/\mathfrak{q}B) \ge \dim(B) - s$. Thus the inequality holds.

Assume B is flat over A. Let $\mathfrak{p} \supset \mathfrak{m}B$ be a prime with $\dim(B/\mathfrak{p}) = \dim(B/\mathfrak{m}B)$. Then $\dim(B) \ge \dim(B/\mathfrak{p}) + \operatorname{ht}(\mathfrak{p})$ because the concatenation of a chain of primes containing $\mathfrak{p}$ of length $\dim(B/\mathfrak{p})$ with a chain of primes contained in $\mathfrak{p}$ of length $\operatorname{ht}(\mathfrak{p})$ is a chain of primes of B of length $\operatorname{ht}(\mathfrak{p}) + \dim(B/\mathfrak{p})$. Hence it suffices to show that $\operatorname{ht}(\mathfrak{p}) \ge \dim(A)$.

As $\mathfrak{n} \supset \mathfrak{p} \supset \mathfrak{m}B$ and as φ is local, $\varphi^{-1}(\mathfrak{p}) = \mathfrak{m}$. Since B is flat over A, **(14.11)** and induction yield a chain of primes of B descending from $\mathfrak{p}$ and lying over any given chain in A. Thus $\operatorname{ht}(\mathfrak{p}) \ge \dim(A)$, as desired. □

EXERCISE **(21.14)**. — Let A be a Noetherian local ring of dimension r. Let $\mathfrak{m}$ be the maximal ideal, and $k := A/\mathfrak{m}$ the residue class field. Prove that

$$r \le \dim_k(\mathfrak{m}/\mathfrak{m}^2),$$

with equality if and only if $\mathfrak{m}$ is generated by r elements.

(21.15) (*Regular local rings*). — Let A be a Noetherian local ring of dimension r. We say A is **regular** if its maximal ideal is generated by r elements. Then any r generators are said to form a **regular** system of parameters.

By **(21.14)**, A is regular if and only if $r = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

For example, a field is a regular local ring of dimension 0, and is the only one.

LEMMA **(21.16)**. — *Let A be a Noetherian semilocal ring of dimension r, and $\mathfrak{q}$ a parameter ideal. Then* $\deg h(G_{\mathfrak{q}}(R), n) = r - 1$.

PROOF: By **(20.8)**, $\deg h(G_{\mathfrak{q}}(A), r)$ is equal to 1 less than the order of pole at 1 of the Hilbert series $H(G_{\mathfrak{q}}(A), t)$. But that order is equal to $d(A)$ by **(21.2)**. Further, $d(A) = r$ by the Dimension Theorem, **(21.4)**. Thus the assertion holds. □

PROPOSITION **(21.17)**. — *Let A be a Noetherian local ring of dimension r, and $\mathfrak{m}$ its maximal ideal. Then A is regular if and only if its associated graded ring $G_{\mathfrak{m}}(A)$ is a polynomial ring; if so, then the number of variables is r.*

PROOF: Assume $G(A)$ is a polynomial ring in s variables. Then $\dim(\mathfrak{m}/\mathfrak{m}^2) = s$. By **(20.4)**, $\deg h(G_{\mathfrak{m}}(A), n) = s - 1$. So $s = r$ by **(21.16)**. So A is regular by **(21.15)**.

Conversely, assume A is regular. Let $x_1, \dots, x_r$ be a regular sop, and $x_i' \in \mathfrak{m}/\mathfrak{m}^2$ the residue of x_i. Set $k := A/\mathfrak{m}$, and let $P := k[X_1, \dots, X_r]$ be the polynomial ring. Form the k-algebra homomorphism $\varphi\colon P \to G(A)$ with $\varphi(X_i) = x_i'$.

Then φ is surjective as the x_i generate $G(A)$. Set $\mathfrak{a} := \operatorname{Ker}\varphi$. Let $P = \bigoplus P_n$ be the grading by total degree. Then φ preserves the gradings of P and $G(A)$. So $\mathfrak{a}$ inherits a grading: $\mathfrak{a} = \bigoplus \mathfrak{a}_n$. So for $n \geq 0$, there's this canonical exact sequence:

$$0 \to \mathfrak{a}_n \to P_n \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to 0. \qquad \textbf{(21.17.1)}$$

Suppose $\mathfrak{a} \neq 0$. Then there's a nonzero $f \in \mathfrak{a}_m$ for some m. Take $n \geq m$. Then $P_{n-m}f \subset \mathfrak{a}_n$. Since P is a domain, $P_{n-m} \xrightarrow{\sim} P_{n-m}f$. Therefore, **(21.17.1)** yields

$$\begin{aligned}\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) &= \dim_k(P_n) - \dim_k(\mathfrak{a}_n)\\ &\leq \dim_k(P_n) - \dim_k(P_{n-m}) = \tbinom{r-1+n}{r-1} - \tbinom{r-1+n-m}{r-1}.\end{aligned}$$

The expression on the right is a polynomial in n of degree $r - 2$.

On the other hand, $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = h(G(A), n)$ for $n \gg 0$ by **(20.8)**. Further, $\deg h(G(A), n) = r - 1$ by **(21.16)**. However, it follows from the conclusion of the preceding paragraph that $\deg h(G(A), n) \leq r - 2$. We have a contradiction! Hence $\mathfrak{a} = 0$. Thus φ is injective, so bijective, as desired. □

EXERCISE **(21.18)**. — Let A be a Noetherian local ring of dimension r, and let $x_1, \dots, x_s \in A$ with $s \leq r$. Set $\mathfrak{a} := \langle x_1, \dots, x_s\rangle$ and $B := A/\mathfrak{a}$. Prove equivalent:

(1) A is regular, and there are $x_{s+1}, \dots, x_r \in A$ with $x_1, \dots, x_r$ a regular sop.

(2) B is regular of dimension $r - s$.

THEOREM **(21.19)**. — *A regular local ring A is a domain.*

PROOF: Use induction on $r := \dim(A)$. If $r = 0$, then A is a field, so a domain.

Assume $r \geq 1$. Let x be a member of a regular sop. Then $A/\langle x\rangle$ is regular of dimension $r - 1$ by **(21.18)**. By induction, $A/\langle x\rangle$ is a domain. So $\langle x\rangle$ is prime. Thus A is a domain by **(21.11)**. □

LEMMA **(21.20)**. — *Let A be a local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{a}$ a proper ideal. Set $\mathfrak{n} := \mathfrak{m}/\mathfrak{a}$ and $k := A/\mathfrak{m}$. Then this sequence of k-vector spaces is exact:*

$$0 \to (\mathfrak{m}^2 + \mathfrak{a})/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2 \to 0.$$

PROOF: The assertion is very easy to check. □

PROPOSITION **(21.21)**. — *Let A be a regular local ring of dimension r, and $\mathfrak{a}$ an ideal. Set $B := A/\mathfrak{a}$, and assume B is regular of dimension $r - s$. Then $\mathfrak{a}$ is generated by s elements, and any such s elements form part of a regular sop.*

PROOF: In its notation, **(21.20)** yields $\dim((\mathfrak{m}^2 + \mathfrak{a})/\mathfrak{m}^2) = s$. Hence, any set of generators of $\mathfrak{a}$ includes s members of a regular sop of A. Let $\mathfrak{b}$ be the ideal the s generate. Then $A/\mathfrak{b}$ is regular of dimension $r - s$ by **(21.18)**. By **(21.19)**, both $A/\mathfrak{b}$ and B are domains of dimension $r - s$; whence, **(15.10)** implies $\mathfrak{a} = \mathfrak{b}$. □

22. Completion

Completion is used to simplify a ring and its modules beyond localization. First, we discuss the topology of a filtration, and use Cauchy sequences to construct the completion. Then we discuss the inverse limit, the dual notion of the direct limit; thus we obtain an alternative construction. We conclude that, if we use the adic filtration of an ideal, then the functor of completion is exact on finitely generated modules over a Noetherian ring. Further, then the completion of a Noetherian ring is Noetherian; if the ideal is maximal, then the completion is local. We end with a useful version of the Cohen Structure Theorem for complete Noetherian local rings.

(22.1) (*Topology and completion*). — Let R be a ring, M a module equipped with a filtration $M = M_0 \supset M_1 \supset \cdots$. Then M has a *topology*: the open sets are the arbitrary unions of the sets $m + M_n$. Indeed, the intersection of two open sets is open, because the intersection of two unions is the union of the pairwise intersections; further, if the intersection U of $m + M_n$ and $m' + M_{n'}$ is nonempty and if $n \geq n'$, then $U = m + M_n$, because, if say $m'' \in U$, then

$$m + M_n = m'' + M_n \subset m'' + M_{n'} = m' + M_{n'}. \qquad \textbf{(22.1.1)}$$

The addition map $M \times M \to M$, given by $(m, m') \mapsto m + m'$, *is continuous,* as

$$(m + M_n) + (m' + M_n) \subset (m + m') + M_n.$$

So, with m' fixed, *the translation* $m \mapsto m + m'$ *is a homeomorphism* $M \to M$. (Similarly, inversion $m \mapsto -m$ is a homeomorphism; so M is a topological group.)

Let $\mathfrak{a}$ be an ideal, and give R the $\mathfrak{a}$-adic filtration. If the filtration on M is an $\mathfrak{a}$-filtration, then scalar multiplication $(x, m) \mapsto xm$ too is continuous, because

$$(x + \mathfrak{a}^n)(m + M_n) \subset xm + M_n.$$

Further, if the filtration is $\mathfrak{a}$-stable, then it yields the same topology as the $\mathfrak{a}$-adic filtration, because

$$M_n \supset \mathfrak{a}^n M \supset \mathfrak{a}^n M_{n'} = M_{n+n'}.$$

Thus *any two stable* $\mathfrak{a}$*-filtrations give the same topology,* called the **$\mathfrak{a}$-adic topology**.

When $\mathfrak{a}$ is given, it is conventional to use the $\mathfrak{a}$-adic filtration and $\mathfrak{a}$-adic topology unless there's explicit mention to the contrary. Further, if R is semi-local, then it is conventional to take $\mathfrak{a} := \operatorname{rad}(R)$.

Let N be a submodule of M. Then *the closure* $\overline{N}$ *of* N *is equal to* $\bigcap_{n\geq 0}(N + M_n)$, because $m \notin \overline{N}$ means there's $n \geq 0$ with $(m + M_n) \cap N = \emptyset$, or $m \notin (N + M_n)$. In particular, each M_n is closed, and $\{0\}$ is closed if and only if $\bigcap M_n = \{0\}$.

Further, M *is* **separated** — that is, **Hausdorff** — *if and only if* $\{0\}$ *is closed.* For, if $\{0\}$ is closed, then so is each $\{m\}$. Hence, given $m' \neq m$, there's n' so that $m \notin (m' + M_{n'})$. Take $n \geq n'$. Then $(m + M_n) \cap (m' + M_{n'}) = \emptyset$ owing to **(22.1.1)**.

Finally, M is **discrete** — that is, every $\{m\}$ is both open and closed — *if and only if* $\{0\}$ *is open.*

A sequence $(m_n)_{n\geq 0}$ in M is called **Cauchy** if, given n_0, there's n_1 with

$$m_n - m_{n'} \in M_{n_0}, \quad \text{or simply } m_n - m_{n+1} \in M_{n_0}, \quad \text{for all } n, n' \geq n_1;$$

the two conditions are equivalent because M_{n_0} is a subgroup and

$$m_n - m_{n'} = (m_n - m_{n+1}) + (m_{n+1} - m_{n+2}) + \cdots + (m_{n'-1} - m_{n'}).$$

An $m \in M$ is called a **limit** of (m_n) if, given n_0, there's n_1 with $m - m_n \in M_{n_0}$ for all $n \geq n_1$. If every Cauchy sequence has a limit, then M is called **complete.**

The Cauchy sequences form a module under termwise addition and termwise scalar multiplication. The sequences with 0 as a limit form a submodule. The quotient module is denoted $\widehat{M}$ and is called the **completion**. There is a canonical homomorphism, which carries $m \in M$ to the class of the constant sequence (m):

$$\kappa\colon M \to \widehat{M} \quad \text{by} \quad \kappa(m) := (m).$$

It is straightforward to check that the notions of Cauchy sequence and limit depend only on the topology. Similarly, $\widehat{M}$ is separated and complete with respect to the filtration $\widehat{M} = \widehat{M}_0 \supset \widehat{M}_1 \supset \cdots$, and κ is the universal example of a continuous homomorphism from M into a separated and complete, filtered module.

Again, let $\mathfrak{a}$ be an ideal. Under termwise multiplication of Cauchy sequences, $\widehat{R}$ *is a ring,* $\kappa\colon R \to \widehat{R}$ *is a ring homomorphism, and* $\widehat{M}$ *is an* $\widehat{R}$*-module.* Further, $M \mapsto \widehat{M}$ *is a linear functor* from $((R\text{-mod}))$ to $((\widehat{R}\text{-mod}))$.

For example, let k be a ring, and $R := k[X_1, \ldots, X_r]$ the polynomial ring in r variables. Set $\mathfrak{a} := \langle X_1, \ldots, X_r \rangle$. Then a sequence $(m_n)_{n\geq 0}$ of polynomials is Cauchy if and only if, given n_0, there's n_1 such that, for all $n \geq n_1$, the m_n agree in degree less than n_0. Thus $\widehat{R}$ is just the power series ring $k[[X_1, \ldots, X_r]]$.

For another example, take a prime integer p, and set $\mathfrak{a} := \langle p \rangle$. Then a sequence $(m_n)_{n\geq 0}$ of integers is Cauchy if and only if, given n_0, there's n_1 such that, for all $n, n' \geq n_1$, the difference $m_n - m_{n'}$ is a multiple of p^{n_0}. The completion of $\mathbb{Z}$ is called the p**-adic integers**, and consists of the sums $\sum_{i=0}^{\infty} z_i p^i$ with $0 \leq z_i < p$.

PROPOSITION **(22.2)**. — *Let R be a ring, and $\mathfrak{a}$ an ideal. Then $\widehat{\mathfrak{a}} \subset \operatorname{rad}(\widehat{R})$.*

PROOF: Recall from **(22.1)** that $\widehat{R}$ is complete in the $\widehat{\mathfrak{a}}$-adic topology. Hence for $x \in \widehat{\mathfrak{a}}$, we have $1/(1-x) = 1 + x + x^2 + \cdots$ in $\widehat{R}$. Thus $\widehat{\mathfrak{a}} \subset \operatorname{rad}(\widehat{R})$ by **(3.2)**. □

EXERCISE **(22.3)**. — In the 2-adic integers, evaluate the sum $1 + 2 + 4 + 8 + \cdots$.

EXERCISE **(22.4)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Prove the following three conditions are equivalent:

(1) $\kappa\colon M \to \widehat{M}$ is injective; (2) $\bigcap \mathfrak{a}^n M = \langle 0 \rangle$; (3) M is separated.

COROLLARY **(22.5)**. — *Let R be a Noetherian ring, $\mathfrak{a} \subset \operatorname{rad}(R)$ an ideal, and M a finitely generated module. Then $M \subset \widehat{M}$.*

PROOF: The assertion results from **(22.4)**, **(18.26)** or **(20.19)**, and **(3.2)**. □

(22.6) (*Inverse limits*). — Let R be a ring. Given modules Q_n equipped with homomorphisms $\alpha_n^{n+1}\colon Q_{n+1} \to Q_n$ for $n \geq 0$, their **inverse limit** $\varprojlim Q_n$ is the submodule of $\prod Q_n$ of all vectors (q_n) with $\alpha_n^{n+1}(q_{n+1}) = q_n$ for all n. Note that

$$\varprojlim Q_n = \operatorname{Ker}(\theta) \qquad \textbf{(22.6.1)}$$

where $\theta\colon \prod Q_n \to \prod Q_n$ is the map defined by $\theta(q_n) := (q_n - \alpha_n^{n+1} q_{n+1})$.

Clearly, $\varprojlim Q_n$ *has this UMP: given maps $\beta_n\colon P \to Q_n$ with $\alpha_n^{n+1}\beta_{n+1} = \beta_n$, there's a unique map $\beta\colon P \to \varprojlim Q_n$ with $\pi_n\beta = \beta_n$ for all n.*

Further, the UMP yields these two natural module isomorphisms:

$$\varprojlim \operatorname{Hom}(P,\, Q_n) = \operatorname{Hom}(P,\, \varprojlim Q_n),$$
$$\varprojlim \operatorname{Hom}(Q_n,\, N) = \operatorname{Hom}(\varinjlim Q_n,\, N).$$

(The notion of inverse limit is formally dual to that of direct limit.)

For example, let k be a ring, and $R := k[X_1, \dots, X_r]$ the polynomial ring in r variables. Set $\mathfrak{m} := \langle X_1, \dots, X_r \rangle$ and $R_n := R/\mathfrak{m}^{n+1}$. Then R_n is just the R-algebra of polynomials of degree at most n, and the canonical map $\alpha_n^{n+1}\colon R_{n+1} \to R_n$ is just truncation. Thus $\varprojlim R_n$ is equal to the power series ring $k[[X_1, \dots, X_r]]$.

For another example, take a prime integer p, and set $\mathbb{Z}_n := \mathbb{Z}/\langle p^{n+1} \rangle$. Then $\mathbb{Z}_n$ is just the ring of sums $\sum_{i=0}^{n} z_i p^i$ with $0 \le z_i < p$, and the canonical map $\alpha_n^{n+1}\colon \mathbb{Z}_{n+1} \to \mathbb{Z}_n$ is just truncation. Thus $\varprojlim \mathbb{Z}_n$ is just the ring of p-adic integers.

In general, *consider exact sequences of modules*

$$0 \to Q'_n \xrightarrow{\beta_n} Q_n \xrightarrow{\gamma_n} Q''_n \to 0$$

and commutative diagrams

$$\begin{array}{ccccccccc} 0 & \to & Q'_{n+1} & \xrightarrow{\beta_{n+1}} & Q_{n+1} & \xrightarrow{\gamma_{n+1}} & Q''_{n+1} & \to & 0 \\ & & \alpha_n'^{n+1}\downarrow & & \alpha_n^{n+1}\downarrow & & \alpha_n''^{n+1}\downarrow & & \\ 0 & \longrightarrow & Q'_n & \xrightarrow{\beta_n} & Q_n & \xrightarrow{\gamma_n} & Q''_n & \longrightarrow & 0 \end{array}$$

Then the induced sequence

$$0 \to \varprojlim Q'_n \xrightarrow{\widehat{\beta}} \varprojlim Q_n \xrightarrow{\widehat{\gamma}} \varprojlim Q''_n \tag{22.6.2}$$

is exact; further, $\widehat{\gamma}$ is surjective if all the $\alpha_n'^{n+1}$ are surjective.

Indeed, the above commutative diagrams yield the following one:

$$\begin{array}{ccccccccc} 0 & \to & \prod Q'_n & \xrightarrow{\prod \beta_n} & \prod Q_n & \xrightarrow{\prod \gamma_n} & \prod Q''_n & \to & 0 \\ & & {\scriptstyle\theta'}\downarrow & & {\scriptstyle\theta}\downarrow & & {\scriptstyle\theta''}\downarrow & & \\ 0 & \to & \prod Q'_n & \xrightarrow{\prod \beta_n} & \prod Q_n & \xrightarrow{\prod \gamma_n} & \prod Q''_n & \to & 0 \end{array}$$

Owing to **(22.6.1)**, the Snake Lemma **(5.12)** yields the exact sequence **(22.6.2)** and an injection $\operatorname{Coker}(\widehat{\gamma}) \hookrightarrow \operatorname{Coker}(\theta')$. Also, $\operatorname{Coker}(\theta') = 0$ if the $\alpha_n'^{n+1}$ are surjective, because given $(q'_n) \in \prod Q'_n$, we can solve the equations $p'_n - \alpha_n'^{n+1}(p'_{n+1}) = q'_n$ recursively to get $(p'_n) \in \prod Q'_n$ with $\theta'(p'_n) = (q'_n)$. Thus $\widehat{\gamma}$ is surjective.

Proposition **(22.7)**. — *Let R be a ring, M a module, $M = M_0 \supset M_1 \supset \cdots$ a filtration. Then $\widehat{M} \xrightarrow{\sim} \varprojlim(M/M_n)$.*

Proof: First, let's define a map $\alpha\colon \widehat{M} \to \varprojlim(M/M_n)$. Given a Cauchy sequence (m_ν), let q_n be the image of m_ν in M/M_n for $\nu \gg 0$. Then q_n is independent of ν, because the sequence is Cauchy. Clearly, q_n is the residue of q_{n+1} in M/M_n. Also, (m_ν) has 0 as a limit if and only if $q_n = 0$ for all n. Define α by $\alpha(m_\nu) := (q_n)$. Clearly, α is well defined, linear, and injective.

As to surjectivity, given $(q_n) \in \varprojlim(M/M_n)$, let $m_\nu \in M$ represent $q_\nu \in M/M_\nu$ for each ν. Then $m_\mu - m_\nu \in M_\nu$ for $\mu \ge \nu$ because the residue of q_n in M/M_ν is q_ν. Hence (m_ν) is Cauchy. Thus α is surjective, so an isomorphism. □

EXERCISE **(22.8)**. — Let A be a Noetherian semilocal ring, and $\mathfrak{m}_1, \dots, \mathfrak{m}_m$ all its maximal ideals. Prove that $\widehat{A} = \prod \widehat{A}_{\mathfrak{m}_i}$.

EXERCISE **(22.9)**. — Let R be a ring, M a module, $M = M_0 \supset M_1 \supset \cdots$ a filtration, and $N \subset M$ a submodule. Filter N by $N_n := N \cap M_n$. Assume $N \supset M_n$ for $n \geq n_0$ for some n_0. Prove $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = M/N$ and $G(\widehat{M}) = G(M)$.

EXERCISE **(22.10)**. — (1) Let R be a ring, $\mathfrak{a}$ an ideal. If $G_{\mathfrak{a}}(R)$ is a domain, show $\widehat{R}$ is an domain. If also $\bigcap_{n\geq 0} \mathfrak{a}^n = 0$, show R is a domain.

(2) Use (1) to give an alternative proof that a regular local ring is a domain.

PROPOSITION **(22.11)**. — *Let A be a ring, $\mathfrak{m}$ a maximal ideal. Then $\widehat{A}$ is a local ring with maximal ideal $\widehat{\mathfrak{m}}$.*

PROOF: First, $\widehat{A}/\widehat{\mathfrak{m}} = A/\mathfrak{m}$ by **(22.9)**; so $\widehat{\mathfrak{m}}$ is maximal. Next, $\operatorname{rad}(\widehat{A}) \supset \widehat{\mathfrak{m}}$ by **(22.2)**. Finally, let $\mathfrak{m}'$ be any maximal ideal of $\widehat{A}$. Then $\mathfrak{m}' \supset \operatorname{rad}(\widehat{A})$. Hence $\mathfrak{m}' = \widehat{\mathfrak{m}}$. Thus $\widehat{\mathfrak{m}}$ is the only maximal ideal. □

EXERCISE **(22.12)**. — Let A be a semilocal ring, $\mathfrak{m}_1, \dots, \mathfrak{m}_m$ all its maximal ideals, and set $\mathfrak{m} := \operatorname{rad}(A)$. Prove that $\widehat{A}$ is a semilocal ring, that $\widehat{\mathfrak{m}}_1, \dots, \widehat{\mathfrak{m}}_m$ are all its maximal ideals, and that $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{A})$.

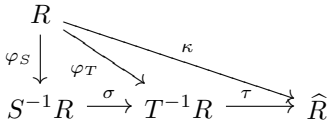
(22.13) (*Completion, units, and localization*). — Let R be a ring, $\mathfrak{a}$ an ideal, and $\kappa\colon R \to \widehat{R}$ the canonical map. Given $t \in R$, for each n denote by $t_n \in R/\mathfrak{a}^n$ the residue of t. Let's show that $\kappa(t)$ *is a unit if and only if each t_n is.*

Indeed, by **(22.7)**, we may regard $\widehat{R}$ as a submodule of $\prod R/\mathfrak{a}^n$. Then each t_n is equal to the projection of $\kappa(t)$. Hence t_n is a unit if $\kappa(t)$ is. Conversely, assume t_n is a unit for each n. Then there are $u_n \in R$ with $u_n t \equiv 1 \pmod{\mathfrak{a}^n}$. By the uniqueness of inverses, $u_{n+1} \equiv u_n$ in $R/\mathfrak{a}^n$ for each n. Set $u := (u_n) \in \prod R/\mathfrak{a}^n$. Then $u \in \widehat{R}$, and $u\kappa(t) = 1$. Thus $\kappa(t)$ is a unit.

Set $T := \kappa^{-1}(\widehat{R}^\times)$. Then by the above, T consists of the $t \in R$ whose residue $t_n \in R/\mathfrak{a}^n$ is a unit for each n. So **(2.26)** and **(1.7)** yield

$$T = \{\, t \in R \mid t \text{ lies in no maximal ideal containing } \mathfrak{a} \,\}. \qquad \textbf{(22.13.1)}$$

Set $S := 1 + \mathfrak{a}$. Then $S \subset T$ owing to **(22.13.1)** as no maximal ideal can contain both x and $1 + x$. Hence the UMP of localization **(11.5)** yields this diagram:



Further, S and T map into $(R/\mathfrak{a}^n)^\times$; hence, **(11.6)**, **(11.19)**, and **(12.18)** yield:

$$R/\mathfrak{a}^n = S^{-1}R/\mathfrak{a}^n S^{-1}R = T^{-1}R/\mathfrak{a}^n T^{-1}R.$$

Therefore, $\widehat{R}$ is, by **(22.7)**, equal to the completion of each of $S^{-1}R$ and $T^{-1}R$ in their $\mathfrak{a}S^{-1}R$-adic and $\mathfrak{a}T^{-1}R$-adic topologies.

For example, take $\mathfrak{a}$ to be a maximal ideal $\mathfrak{m}$. Then $T = R - \mathfrak{m}$ by **(22.13.1)**. Thus $\widehat{R}$ is equal to the completion of the localization $R_{\mathfrak{m}}$.

Finally, assume R is Noetherian. Let's prove that σ *and* τ *are injective.* Indeed, say $\tau\sigma(x/s) = 0$. Then $\kappa(x) = 0$ as $\kappa(s)$ is a unit. So $x \in \bigcap \mathfrak{a}^n$. Hence the Krull Intersection Theorem, **(18.26)** or **(20.19)**, yields an $s' \in S$ with $s'x = 0$. So $x/s = 0$ in $S^{-1}R$. Thus σ is injective. Similarly, τ is injective.

THEOREM **(22.14)** (Exactness of Completion). — *Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Then on the finitely generated modules M, the functor $M \mapsto \widehat{M}$ is exact.*

PROOF: Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of modules. Set $M'_n := M' \cap \mathfrak{a}^n M$. Then we obtain these exact sequences:

$$0 \to M'/M'_n \to M/\mathfrak{a}^n M \to M''/\mathfrak{a}^n M'' \to 0.$$

The maps $M'/M'_{n+1} \to M'/M'_n$ are surjective. So **(22.6)** yields this exact sequence:

$$0 \to \varprojlim M'/M'_n \to \varprojlim M/\mathfrak{a}^n M \to \varprojlim M''/\mathfrak{a}^n M'' \to 0.$$

Assume R is Noetherian and M is finitely generated. Then $M' = M'_0 \supset M'_1 \supset \cdots$ is an $\mathfrak{a}$-stable filtration by the Artin–Rees Lemma **(20.18)**. Hence, **(22.1)** and **(22.7)** yield the desired exactness of

$$0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0. \qquad \square$$

EXERCISE **(22.15)**. — Let A be a Noetherian semilocal ring. Prove that an element $x \in A$ is a nonzerodivisor if and only if its image $\widehat{x} \in \widehat{A}$ is also.

COROLLARY **(22.16)**. — *Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Then the natural map is an isomorphism:*

$$\widehat{R} \otimes M \xrightarrow{\sim} \widehat{M}.$$

PROOF: By **(22.14)**, the functor $M \mapsto \widehat{M}$ is exact on the category of finitely generated modules, and so **(8.16)** yields the conclusion. $\square$

EXERCISE **(22.17)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Show that $M \mapsto \widehat{M}$ preserves surjections, and that $\widehat{R} \otimes M \to \widehat{M}$ is surjective if M is finitely generated.

COROLLARY **(22.18)**. — *Let R be a Noetherian ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, M a finitely generated module. Then, using the $\mathfrak{a}$-adic topology, we have*

(1) $(\mathfrak{b}M)\widehat{\ } = \mathfrak{b}\widehat{M} = \widehat{\mathfrak{b}}\,\widehat{M}$ *and* (2) $(\mathfrak{b}^n)\widehat{\ } = \mathfrak{b}^n\widehat{R} = (\mathfrak{b}\widehat{R})^n = (\widehat{\mathfrak{b}})^n$ *for any $n \geq 0$.*

PROOF: In general, the inclusion $\mathfrak{b}M \to M$ induces a commutative square

$$\begin{array}{ccc} \widehat{R} \otimes (\mathfrak{b}M) & \to & \widehat{R} \otimes M \\ \downarrow & & \downarrow \\ (\mathfrak{b}M)\widehat{\ } & \longrightarrow & \widehat{M} \end{array}$$

It is not hard to see that top map's image is $\mathfrak{b}(\widehat{R} \otimes M)$.

In the present case, the two vertical maps are isomorphisms by **(22.16)**, and the bottom map is injective by **(22.14)**. Thus $(\mathfrak{b}M)\widehat{\ } = \mathfrak{b}\widehat{M}$.

Taking R for M yields $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$. Hence $\mathfrak{b}\widehat{M} = \mathfrak{b}\widehat{R}\,\widehat{M} = \widehat{\mathfrak{b}}\,\widehat{M}$. Thus (1) holds.

In (1), taking $\mathfrak{b}^n$ for $\mathfrak{b}$ and R for M yields $(\mathfrak{b}^n)\widehat{\ } = \mathfrak{b}^n\widehat{R}$. In particular, $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$; so $(\mathfrak{b}\widehat{R})^n = (\widehat{\mathfrak{b}})^n$. But $\mathfrak{b}^n R' = (\mathfrak{b}R')^n$ for any R-algebra R'. Thus (2) holds. $\square$

COROLLARY **(22.19)**. — *Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Then $\widehat{R}$ is flat.*

PROOF: Let $\mathfrak{b}$ be any ideal. Then $\widehat{R} \otimes \mathfrak{b} = \widehat{\mathfrak{b}}$ by **(22.16)**, and $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$ by **(22.18)**(2). Thus $\widehat{R}$ is flat by the Ideal Criterion **(9.18)**. $\square$

EXERCISE **(22.20)**. — Let R be a Noetherian ring, and $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Assume $\mathfrak{a} \subset \operatorname{rad}(R)$, and use the $\mathfrak{a}$-adic topology. Prove $\mathfrak{b}$ is principal if $\mathfrak{b}\widehat{R}$ is.

LEMMA **(22.21)**. — *Let R be a ring, $\beta\colon M \to N$ a map of filtered modules (so β preserves the filtration). If $G(\beta)$ is injective or surjective, then so is $\widehat{\beta}$.*

PROOF: Consider the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_n/M_{n+1} & \longrightarrow & M/M_{n+1} & \longrightarrow & M/M_n & \longrightarrow & 0 \\ & & {\scriptstyle G_n(\beta)}\downarrow & & {\scriptstyle \beta_{n+1}}\downarrow & & {\scriptstyle \beta_n}\downarrow & & \\ 0 & \longrightarrow & N_n/N_{n+1} & \longrightarrow & N/N_{n+1} & \longrightarrow & N/N_n & \longrightarrow & 0 \end{array}$$

Apply the Snake Lemma **(5.12)**. It yields the following exact sequence:

$$\operatorname{Ker} G_n(\beta) \to \operatorname{Ker} \beta_{n+1} \to \operatorname{Ker} \beta_n \to \operatorname{Coker} G_n(\beta) \to \operatorname{Coker} \beta_{n+1} \to \operatorname{Coker} \beta_n.$$

Assume $G(\beta)$ is injective. Then $\operatorname{Ker} G_n(\beta) = 0$. Hence induction on n yields $\operatorname{Ker} \beta_n = 0$ for all n. Thus $\widehat{\beta}$ is injective by **(22.6)**.

Assume $G(\beta)$ is surjective. Then $\operatorname{Coker} G_n(\beta) = 0$. So $\operatorname{Ker} \beta_{n+1} \to \operatorname{Ker} \beta_n$ is surjective for all n. Also, induction on n yields $\operatorname{Coker} \beta_n = 0$ for all n; that is,

$$0 \to \operatorname{Ker} \beta_n \to M/M_n \xrightarrow{\beta_n} N/N_n \to 0$$

is exact. Thus $\widehat{\beta}$ is surjective by **(22.6)**. □

LEMMA **(22.22)**. — *Let R be a complete ring, M a separated module. If $G(M)$ is finitely generated over $G(R)$, then M is finitely generated over R and complete.*

PROOF: Take finitely many homogeneous generators of $G(M)$. Lift them to M. The lifts define a map $\alpha\colon R^n \to M$, and $G(\alpha)$ is surjective. So $\widehat{\alpha}$ is surjective by **(22.21)**. Now, form this canonical commutative diagram:

$$\begin{array}{ccc} R^n & \xrightarrow{\kappa_{R^n}} & \widehat{R}^n \\ {\scriptstyle \alpha}\downarrow & & {\scriptstyle \widehat{\alpha}}\downarrow \\ M & \xrightarrow{\kappa_M} & \widehat{M} \end{array}$$

Since R is complete, κ_{R^n} is surjective by **(22.1)**. Since M is separated, κ_M is injective by **(22.4)**. Hence κ_M is an isomorphism and α is surjective, as desired. □

EXERCISE **(22.23)** (*Nakayama's Lemma for a complete ring*). — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Assume R is complete, and M separated. Show $m_1, \dots, m_n \in M$ generate if their images in $M/\mathfrak{a}M$ generate.

PROPOSITION **(22.24)**. — *Let R be a complete ring, M a separated module. If $G(M)$ is a Noetherian $G(R)$-module, then M is a complete Noetherian R-module.*

PROOF: Given a submodule $N \subset M$, set $N_n := M_n \cap N$. Then $G(N) \subset G(M)$. As $G(M)$ is Noetherian, $G(N)$ is finitely generated. Hence N is finitely generated and complete by **(22.22)**. Thus M is Noetherian and complete. □

THEOREM **(22.25)**. — *Let R be a ring, $\mathfrak{a}$ an ideal. If R is Noetherian, so is $\widehat{R}$.*

PROOF: Assume R is Noetherian. Then $G(R)$ is finitely generated as an $(R/\mathfrak{a})$-algebra by **(20.12)**. So $G(R)$ is Noetherian by the Hilbert Basis Theorem, **(16.11)**. But $G(R) = G(\widehat{R})$ by **(22.9)**. Hence $\widehat{R}$ is Noetherian by **(22.24)** with $\widehat{R}$ for R and for M. □

EXAMPLE **(22.26)**. — Let k be a Noetherian ring, $P := k[X_1, \dots, X_r]$ the polynomial ring, and $A := k[[X_1, \dots, X_r]]$ the formal power series ring. Then A is the completion of P in the $\langle X_1, \dots, X_r\rangle$-adic topology by **(22.1)**. Further, P is Noetherian by the Hilbert Basis Theorem, **(20.12)**. Thus A *is Noetherian* by **(22.25)**.

Assume k is a domain. Then A is a domain. Indeed, A is one if $r = 1$, because

$$(a_m X_1^m + \cdots)(b_n X_1^n + \cdots) = a_m b_n X_1^{m+n} + \cdots .$$

If $r > 1$, then $A = k[[X_1, \dots, X_i]]\,[[X_{i+1}, \dots, X_r]]$; so A is a domain by induction.

Set $\mathfrak{p}_i := \langle X_{i+1}, \dots, X_r\rangle$. Then $A/\mathfrak{p}_i = k[[X_1, \dots, X_i]]$ by **(3.7)**. Hence $\mathfrak{p}_i$ is prime. So $0 = \mathfrak{p}_r \subsetneqq \cdots \subsetneqq \mathfrak{p}_0$ is a chain of primes of length r. Thus $\dim(A) \geq r$.

Assume k is a field. Then A is local with maximal ideal $\langle X_1, \dots, X_r\rangle$ and with residue field k by the above and either by **(22.11)** or again by **(3.7)**. Therefore, $\dim(A) \leq r$ by **(21.14)**. Thus A *is regular of dimension r.*

EXERCISE **(22.27)**. — Let A be a Noetherian local ring, $\mathfrak{m}$ the maximal ideal. Prove (1) that $\widehat{A}$ is a Noetherian local ring with $\widehat{\mathfrak{m}}$ as maximal ideal, (2) that $\dim(A) = \dim(\widehat{A}\,)$, and (3) that A is regular if and only if $\widehat{A}$ is regular.

THEOREM **(22.28)** (UMP of Formal Power Series). — *Let R be a ring, R' an R-algebra, $\mathfrak{b}$ an ideal of R', and $x_1, \dots, x_n \in \mathfrak{b}$. Let $P := R[[X_1, \dots, X_n]]$ be the formal power series ring. If R' is separated and complete, then there is a unique R-algebra map $\pi\colon P \to R'$ with $\pi(X_i) = x_i$ for $1 \leq i \leq n$.*

PROOF: For each m, there's a unique R-algebra map $R[X_1, \dots, X_n] \to R'/\mathfrak{b}^m$ sending X_i to the residue of x_i. This map induces a map

$$P/\langle X_1, \dots X_n\rangle^m = R[X_1, \dots, X_n]/\langle X_1, \dots X_n\rangle^m \longrightarrow R'/\mathfrak{b}^m.$$

Taking inverse limits yields π owing to **(22.6)** and **(22.7)**. □

THEOREM **(22.29)** (Cohen Structure). — *Let A be a complete Noetherian local ring with maximal ideal $\mathfrak{m}$. Assume that A contains a field k such that $k \xrightarrow{\sim} A/\mathfrak{m}$. Then $A \simeq k[[X_1, \dots, X_n]]/\mathfrak{a}$ for some variables X_i and ideal $\mathfrak{a}$. Further, if A is regular of dimension r, then $A \simeq k[[X_1, \dots, X_r]]$.*

PROOF: Take generators $x_1, \dots, x_n \in \mathfrak{m}$. Let $\pi\colon k[[X_1, \dots, X_n]] \to A$ be the map with $\pi(X_i) = x_i$ of **(22.28)**. Then $G(\pi)$ is surjective. Hence, π is surjective by **(22.21)**. Set $\mathfrak{a} := \operatorname{Ker}(\pi)$. Then $k[[X_1, \dots, X_n]]/\mathfrak{a} \xrightarrow{\sim} A$.

Assume A is regular of dimension r. Take $n = r$. Then $G(A)$ is a polynomial ring in r variables over k by **(21.17)**. And $G\big(k[[X_1, \dots, X_r]]\big)$ is too by **(22.6)**. Since $G(\pi)$ is surjective, its kernel is a minimal prime, so equal to $\langle 0\rangle$. Hence $G(\pi)$ is bijective. So π is bijective by **(22.21)**. Thus $k[[X_1, \dots, X_r]] \xrightarrow{\sim} A$. □

23. Discrete Valuation Rings

A discrete valuation is a homomorphism from the multiplicative group of a field to the additive group integers such that the value of a sum is at least the minimum value of the summands. The corresponding discrete valuation ring consists of the elements whose values are nonnegative, plus 0. We characterize these rings in various ways; notably, we prove they are the normal Noetherian local domains of dimension 1. Then we prove that any normal Noetherian domain is the intersection of all the discrete valuation rings obtained by localizing at its height-1 primes. Finally, we prove Serre's Criterion for normality of Noetherian domains.

(23.1) (*Discrete Valuations*). — Let K be a field. We define a **discrete valuation** of K to be a surjective function $v\colon K^\times \to \mathbb{Z}$ such that, for every $x, y \in K^\times$,

$$(1)\ \ v(x\cdot y) = v(x) + v(y), \quad (2)\ \ v(x+y) \geq \min\{v(x), v(y)\} \text{ if } x \neq -y. \tag{23.1.1}$$

Condition (1) just means v is a group homomorphism. Hence, for any $x \in K^\times$,

$$(1)\ \ v(1) = 0 \quad \text{and} \quad (2)\ \ v(x^{-1}) = -v(x). \tag{23.1.2}$$

As a convention, we define $v(0) := \infty$. Consider the sets

$$A := \{x \in K \mid v(x) \geq 0\} \quad \text{and} \quad \mathfrak{m} := \{x \in K \mid v(x) > 0\}.$$

Clearly, A is a subring, so a domain, and $\mathfrak{m}$ is an ideal. Further, $\mathfrak{m}$ is nonzero as v is surjective. We call A the **discrete valuation ring** (DVR) of v.

Notice that, if $x \in K$, but $x \notin A$, then $x^{-1} \in \mathfrak{m}$; indeed, $v(x) < 0$, and so $v(x^{-1}) = -v(x) > 0$. Hence, $\operatorname{Frac}(A) = K$. Further,

$$A^\times = \{x \in K \mid v(x) = 0\} = A - \mathfrak{m}.$$

Indeed, if $x \in A^\times$, then $v(x) \geq 0$ and $-v(x) = v(x^{-1}) \geq 0$; so $v(x) = 0$. Conversely, if $v(x) = 0$, then $v(x^{-1}) = -v(x) = 0$; so $x^{-1} \in A$, and so $x \in A^\times$. Therefore, by the nonunit criterion, *A is a local domain, not a field, and $\mathfrak{m}$ is its maximal ideal.*

An element $t \in \mathfrak{m}$ with $v(t) = 1$ is called a (local) **uniformizing parameter**. Such a t is irreducible, as $t = ab$ with $v(a) \geq 0$ and $v(b) \geq 0$ implies $v(a) = 0$ or $v(b) = 0$ since $1 = v(a) + v(b)$. Further, any $x \in K^\times$ has the unique factorization $x = ut^n$ where $u \in A^\times$ and $n := v(x)$; indeed, $v(u) = 0$ as $u = xt^{-n}$. In particular, t_1 is uniformizing parameter if and only if $t_1 = ut$ with $u \in A^\times$; further, A is a UFD.

Moreover, *A is a* PID; *in fact, any nonzero ideal $\mathfrak{a}$ of A has the form*

$$\mathfrak{a} = \langle t^m \rangle \quad \text{where} \quad m := \min\{\, v(x) \mid x \in \mathfrak{a}\,\}. \tag{23.1.3}$$

Indeed, given a nonzero $x \in \mathfrak{a}$, say $x = ut^n$ where $u \in A^\times$. Then $t^n \in \mathfrak{a}$. So $n \geq m$. Set $y := ut^{n-m}$. Then $y \in A$ and $x = yt^m$, as desired.

In particular, $\mathfrak{m} = \langle t \rangle$ and $\dim(A) = 1$. Thus A is regular local of dimension 1.

The prototype is this. Let k be a field, t a variable, and $K := k((t))$ the field of formal Laurent series $x := \sum_{i \geq n} a_i t^i$ with $n \in \mathbb{Z}$ and with $a_i \in k$ and $a_n \neq 0$. Set $v(x) := n$, the "order of vanishing" of x. Clearly, v is a discrete valuation, the formal power series ring $k[[t]]$ is its DVR, and $\mathfrak{m} := \langle t \rangle$ is its maximal ideal.

The preceding example can be extended to cover any DVR A that contains a field k with $k \xrightarrow{\sim} A/\langle t \rangle$ where t is a uniformizing power. Indeed, A is a subring

of its completion $\widehat{A}$ by **(22.5)**, and $\widehat{A} = k[[t]]$ by the proof of the Cohen Structure Theorem **(22.29)**. Further, clearly, the valuation on $\widehat{A}$ restricts to that on A.

A second old example is this. Let $p \in \mathbb{Z}$ be prime. Given $x \in \mathbb{Q}$, write $x = ap^n/b$ with $a, b \in \mathbb{Z}$ relatively prime and prime to p. Set $v(x) := n$. Clearly, v is a discrete valuation, the localization $\mathbb{Z}_{\langle p \rangle}$ is its DVR, and $p\mathbb{Z}_{\langle p \rangle}$ is its maximal ideal. We call v the **p-adic valuation** of $\mathbb{Q}$.

LEMMA **(23.2)**. — *Let A be a local domain, $\mathfrak{m}$ its maximal ideal. Assume that $\mathfrak{m}$ is nonzero and principal and that $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$. Then A is a DVR.*

PROOF: Given a nonzero $x \in A$, there is an $n \geq 0$ such that $x \in \mathfrak{m}^n - \mathfrak{m}^{n+1}$. Say $\mathfrak{m} = \langle t \rangle$. Then $x = ut^n$, and $u \notin \mathfrak{m}$, so $u \in A^\times$. Set $K := \operatorname{Frac}(A)$. Given $x \in K^\times$, write $x = y/z$ where $y = bt^m$ and $z = ct^k$ with $b, c \in A^\times$. Then $x = ut^n$ with $u := b/c \in A^\times$ and $n := m - k \in \mathbb{Z}$. Define $v\colon K^\times \to \mathbb{Z}$ by $v(x) := n$. If $ut^n = wt^h$ with $n \geq h$, then $(u/w)t^{n-h} = 1$, and so $n = h$. Thus v is well defined.

Since $v(t) = 1$, clearly v is surjective. To verify **(23.1.1)**, take $x = ut^n$ and $y = wt^h$ with $u, w \in A^\times$. Then $xy = (uw)t^{n+h}$. Thus (1) holds. To verify (2), we may assume $n \geq h$. Then $x + y = t^h(ut^{n-h} + w)$. Hence

$$v(x + y) \geq h = \min\{n, h\} = \min\{v(x),\, v(y)\}.$$

Thus (2) holds. So $v\colon K^\times \to \mathbb{Z}$ is a valuation. Clearly, A is the DVR of v. □

(23.3) (*Depth*). — Let R be a ring, M a nonzero module, and $x_1, \dots, x_n \in R$. Set $M_i := M/\langle x_1, \dots, x_i \rangle$. We say the sequence $x_1, \dots, x_n$ is **regular** on M, or is an **M-sequence**, and call n its **length** if $M_n \neq 0$ and $x_i \notin \operatorname{z.div}(M_{i-1})$ for all i.

We call the supremum of the lengths n of the M-sequences found in an ideal $\mathfrak{a}$ the **depth** of $\mathfrak{a}$ on M, and denote it by $\operatorname{depth}(\mathfrak{a}, M)$. By convention, $\operatorname{depth}(\mathfrak{a}, M) = 0$ means $\mathfrak{a}$ contains no nonzerodivisor on M.

When M is semilocal, we call the depth of $\operatorname{rad}(M)$ on M simply the **depth** of M and denote it by $\operatorname{depth}(M)$. If $\operatorname{depth}(M) = \dim(M)$, we call M **Cohen–Macaulay**.

LEMMA **(23.4)**. — *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, and M a nonzero finitely generated module.*

(1) *Then* $\operatorname{depth}(M) = 0$ *if and only if* $\mathfrak{m} \in \operatorname{Ass}(M)$.

(2) *Then* $\operatorname{depth}(M) = 1$ *if and only if there is an* $x \in \mathfrak{m}$ *with* $x \notin \operatorname{z.div}(M)$ *and* $\mathfrak{m} \in \operatorname{Ass}(M/xM)$.

(3) *Then* $\operatorname{depth}(M) \leq \dim(M)$.

PROOF: Consider (1). If $\mathfrak{m} \in \operatorname{Ass}(M)$, then it is immediate from the definitions that $\mathfrak{m} \subset \operatorname{z.div}(M)$ and so $\operatorname{depth}(M) = 0$.

'1Conversely, assume $\operatorname{depth}(M) = 0$. Then $\mathfrak{m} \subset \operatorname{z.div}(M)$. Since A is Noetherian, $\operatorname{z.div}(M) = \bigcup_{\mathfrak{p}\in\operatorname{Ass}(M)} \mathfrak{p}$ by **(17.14)**. Since M is also finitely generated, $\operatorname{Ass}(M)$ is finite by **(17.20)**. Hence $\mathfrak{m} = \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M)$ by Prime Avoidance, **(3.12)**.

Consider (2). Assume $\operatorname{depth}(M) = 1$. Then there is an M-sequence of length 1, but none longer. So there is an $x \in \mathfrak{m}$ with $x \notin \operatorname{z.div}(M)$ and $\operatorname{depth}(M/xM) = 0$. Then $\mathfrak{m} \in \operatorname{Ass}(M/xM)$ by (1).

Conversely, assume there is $x \in \mathfrak{m}$ with $x \notin \operatorname{z.div}(M)$. Then $\operatorname{depth}(M) \geq 1$ by definition. Assume $\mathfrak{m} \in \operatorname{Ass}(M/xM)$. Then given any $y \in \mathfrak{m}$ with $y \notin \operatorname{z.div}(M)$, also $\mathfrak{m} \in \operatorname{Ass}(M/yM)$ by **(17.25)**. So $\operatorname{depth}(M/yM) = 0$ by (1). So there is no $z \in \mathfrak{m}$ such that y, z is an M-sequence. Thus $\operatorname{depth}(M) \leq 1$. Thus $\operatorname{depth}(M) = 1$.

Consider (3). Given any M-sequence $x_1, \dots, x_n$, set $M_i := M/\langle x_1, \dots, x_i\rangle$. Then $\dim(M_{i+1}) = \dim(M_i) - 1$ by **(21.5)**. Hence $\dim(M) - n = \dim(M_n) \geq 0$. But $\operatorname{depth}(M) := \sup\{n\}$. Thus (3) holds. □

Exercise **(23.5)**. — Let R be a ring, M a module, and $x, y \in R$.

(1) Prove that, if x, y form an M-sequence, then, given any $m, n \in M$ such that $xm = yn$, there exists $p \in M$ such that $m = yp$ and $n = xp$.

(2) Prove the converse of (1) if R is local, and x, y lie in its maximal ideal $\mathfrak{m}$, and M is Noetherian.

Exercise **(23.6)**. — Let R be a local ring, $\mathfrak{m}$ its maximal ideal, M a Noetherian module, $x_1, \dots, x_n \in \mathfrak{m}$, and σ a permutation of $1, \dots, n$. Assume $x_1, \dots, x_n$ form an M-sequence, and prove $x_{\sigma 1}, \dots, x_{\sigma n}$ do too; first, say σ transposes i and $i+1$.

Exercise **(23.7)**. — Prove that a Noetherian local ring A of dimension $r \geq 1$ is regular if and only if its maximal ideal $\mathfrak{m}$ is generated by an A-sequence.

Theorem **(23.8)** (Characterization of DVRs). — *Let A be a local ring, $\mathfrak{m}$ its maximal ideal. Assume A is Noetherian. Then these five conditions are equivalent:*

(1) *A is a* DVR.
(2) *A is a normal domain of dimension* 1.
(3) *A is a normal domain of depth* 1.
(4) *A is a regular local ring of dimension* 1.
(5) *$\mathfrak{m}$ is principal and of height at least* 1.

Proof: Assume (1). Then A is UFD by **(23.1)**; so A is normal by **(10.25)**. Further, A has just two primes, $\langle 0\rangle$ and $\mathfrak{m}$; so $\dim(A) = 1$. Thus (2) holds. Further, (4) holds by **(23.1)**. Clearly, (4) implies (5).

Assume (2). Take a nonzero $x \in \mathfrak{m}$. Then $A/\langle x\rangle \neq 0$, so $\operatorname{Ass}\big(A/\langle x\rangle\big) \neq \emptyset$ by **(17.12)**. Now, A is a local domain of dimension 1, so A has just two primes, $\langle 0\rangle$ and $\mathfrak{m}$. Clearly, $\langle 0\rangle \notin \operatorname{Ass}(A/\langle x\rangle)$. Hence, $\mathfrak{m} \in \operatorname{Ass}(A/\langle x\rangle)$. Thus (3) holds.

Assume (3). By **(23.4)**(2), there are $x, y \in \mathfrak{m}$ such that x is nonzero and y has residue $\overline{y} \in A/\langle x\rangle$ with $\mathfrak{m} = \operatorname{Ann}(\overline{y})$. So $y\mathfrak{m} \subset \langle x\rangle$. Set $z := y/x \in \operatorname{Frac}(A)$. Then $z\mathfrak{m} = (y\mathfrak{m})/x \subset A$. Suppose $z\mathfrak{m} \subset \mathfrak{m}$. Then z is integral over A by **(10.15)**. But A is normal, so $z \in A$. So $y = zx \in \langle x\rangle$, a contradiction. Hence, $1 \in z\mathfrak{m}$; so there is $t \in \mathfrak{m}$ with $zt = 1$. Given $w \in \mathfrak{m}$, therefore $w = (wz)t$ with $wz \in A$. Thus $\mathfrak{m}$ is principal. Finally, $\operatorname{ht}(\mathfrak{m}) \geq 1$ because $x \in \mathfrak{m}$ and $x \neq 0$. Thus (5) holds.

Assume (5). The Krull Intersection Theorem **(18.26)** yields an $x \in \mathfrak{m}$ with $(1+x)\bigcap \mathfrak{m}^n = 0$. Then $1 + x \in A^\times$. So $\bigcap \mathfrak{m}^n = 0$. Further, A is a domain by **(21.11)**(1). Hence (1) holds by **(23.2)**. □

Exercise **(23.9)**. — Let A be a DVR with fraction field K, and $f \in A$ a nonzero nonunit. Prove A is a maximal proper subring of K. Prove $\dim(A) \neq \dim(A_f)$.

Exercise **(23.10)**. — Let k be a field, $P := k[X, Y]$ the polynomial ring in two variables, $f \in P$ an irreducible polynomial. Say $f = \ell(X, Y) + g(X, Y)$ with $\ell(X, Y) = aX + bY$ for $a, b \in k$ and with $g \in \langle X, Y\rangle^2$. Set $R := P/\langle f\rangle$ and $\mathfrak{p} := \langle X, Y\rangle/\langle f\rangle$. Prove that $R_{\mathfrak{p}}$ is a DVR if and only if $\ell \neq 0$. (Thus $R_{\mathfrak{p}}$ is a DVR if and only if the plane curve $C : f = 0 \subset k^2$ is nonsingular at $(0, 0)$.)

EXERCISE **(23.11)**. — Let k be a field, A a ring intermediate between the polynomial ring and the formal power series ring in one variable: $k[X] \subset A \subset k[[X]]$. Suppose that A is local with maximal ideal $\langle X \rangle$. Prove that A is a DVR. (Such local rings arise as rings of power series with curious convergence conditions.)

EXERCISE **(23.12)**. — Let L/K be an algebraic extension of fields, $X_1, \dots, X_n$ variables, P and Q the polynomial rings over K and L in $X_1, \dots, X_n$.

(1) Let $\mathfrak{q}$ be a prime of Q, and $\mathfrak{p}$ its contraction in P. Prove $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q})$.
(2) Let $f, g \in P$ be two polynomials with no common prime factor in P. Prove that f and g have no common prime factor $q \in Q$.

(23.13) (*Serre's Conditions*). — Let R be a Noetherian ring. We say **Serre's Condition** (R_n) holds if, for any prime $\mathfrak{p}$ of height $m \leq n$, the localization $R_{\mathfrak{p}}$ is regular of dimension m. We say **Serre's Condition** (S_n) holds if, for any prime $\mathfrak{p}$ of any height m, the depth of $\mathfrak{p}$ on $R_{\mathfrak{p}}$ is at least $\min\{m, n\}$, or equivalently, if

$$\operatorname{depth}(R_{\mathfrak{p}}) \geq \min\{\dim(R_{\mathfrak{p}}), n\}$$

as $x_1, \dots, x_r \in \mathfrak{p}$ is an $R_{\mathfrak{p}}$-sequence if and only if $x_1/t_i, \dots, x_r/t_r$ is for any $t_i \notin \mathfrak{p}$.

For example, (R_0) holds if and only if $R_{\mathfrak{p}}$ is a field for any minimal prime $\mathfrak{p}$. Also, (R_1) holds if and only if (R_0) does and $R_{\mathfrak{p}}$ is a DVR for any $\mathfrak{p}$ of height-1.

Note $\operatorname{depth}(R_{\mathfrak{p}}) \leq \dim(R_{\mathfrak{p}})$ by **(23.4)**(3). Hence (S_n) holds if and only if $R_{\mathfrak{p}}$ is Cohen–Macaulay when $\operatorname{depth}(R_{\mathfrak{p}}) < n$. In particular, ($\mathrm{S}_1$) holds if and only if $\mathfrak{p}$ is minimal when $\mathfrak{p} \in \operatorname{Ass}(R)$ by **(17.14)**; that is, there are no embedded primes.

EXERCISE **(23.14)**. — Let R be a Noetherian ring. Show that R is reduced if and only if (R_0) and (S_1) hold.

LEMMA **(23.15)**. — *Let R be a Noetherian domain. Set*

$$\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\} \quad \text{and} \quad \Sigma := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{depth}(R_{\mathfrak{p}}) = 1 \,\}.$$

Then $\Phi \subset \Sigma$, and $\Phi = \Sigma$ if and only if (S_2) *holds. Further, $R = \bigcap_{\mathfrak{p} \in \Sigma} R_{\mathfrak{p}}$.*

PROOF: Given $\mathfrak{p} \in \Phi$, set $\mathfrak{q} := \mathfrak{p}R_{\mathfrak{p}}$. Take $0 \neq x \in \mathfrak{q}$. Then $\mathfrak{q}$ is minimal over $\langle x \rangle$. So $\mathfrak{q} \in \operatorname{Ass}(R_{\mathfrak{p}}/\langle x \rangle)$ by **(17.17)**. Hence $\operatorname{depth}(R_{\mathfrak{p}}) = 1$ by **(23.4)**(2). Thus $\Phi \subset \Sigma$.

However, (S_1) holds by **(23.14)**. Hence (S_2) holds if and only if $\Phi \supset \Sigma$. Thus $\Phi = \Sigma$ if and only if R satisfies (S_2).

Further, $R \subset R_{\mathfrak{p}}$ for any prime $\mathfrak{p}$ by **(11.3)**; so $R \subset \bigcap_{\mathfrak{p} \in \Sigma} R_{\mathfrak{p}}$. As to the opposite inclusion, take an $x \in \bigcap_{\mathfrak{p} \in \Sigma} R_{\mathfrak{p}}$. Say $x = a/b$ with $a, b \in R$ and $b \neq 0$. Then $a \in bR_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Sigma$. But $\mathfrak{p} \in \Sigma$ if $\mathfrak{p} \in \operatorname{Ass}(R_{\mathfrak{p}}/bR_{\mathfrak{p}})$ by **(23.4)**(2). So $a \in bR$ by **(18.25)**. Thus $x \in R$, as desired. □

THEOREM **(23.16)**. — *Let R be a normal Noetherian domain. Then*

$$R = \textstyle\bigcap_{\mathfrak{p} \in \Phi} R_{\mathfrak{p}} \quad \text{where} \quad \Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\}.$$

PROOF: As R is normal, so is $R_{\mathfrak{p}}$ for any prime $\mathfrak{p}$ by **(11.28)**. So $\operatorname{depth}(R_{\mathfrak{p}}) = 1$ if and only if $\dim(R_{\mathfrak{p}}) = 1$ by **(23.8)**. Thus **(23.15)** yields the assertion. □

THEOREM **(23.17)** (Serre's Criterion). — *Let R be a Noetherian domain. Then R is normal if and only if* (R_1) *and* (S_2) *hold.*

PROOF: As R is a domain, (R_0) and (S_1) hold by **(23.14)**. If R is normal, then so is $R_{\mathfrak{p}}$ for any prime $\mathfrak{p}$ by **(11.28)**; whence, (R_1) and (S_2) hold by **(23.8)**.

Conversely, assume R satisfies (R_1) and (S_2). Let x be integral over R. Then x is integral over $R_{\mathfrak{p}}$ for any prime $\mathfrak{p}$. Now, $R_{\mathfrak{p}}$ is a DVR for all $\mathfrak{p}$ of height 1 as R satisfies (R_1). Hence, $x \in R_{\mathfrak{p}}$ for all $\mathfrak{p}$ of height 1, so for all $\mathfrak{p}$ of depth 1 as R satisfies (S_2). So $x \in R$ owing to **(23.15)**. Thus R is normal. □

EXAMPLE **(23.18)**. — Let k be an algebraically closed field, $P := k[X, Y]$ the polynomial ring in two variables, $f \in P$ irreducible. Then $\dim(P) = 2$ by **(15.12)**. Set $R := P/\langle f \rangle$. Then R is a domain.

Let $\mathfrak{p} \subset R$ be a nonzero prime. Say $\mathfrak{p} = \mathfrak{m}/\langle f \rangle$. Then $0 \subsetneqq \langle f \rangle \subsetneqq \mathfrak{m}$ is a chain of primes of length 2, the maximum. Thus $\mathfrak{m}$ is maximal, and $\dim(R) = 1$.

Hence $\mathfrak{m} = \langle X - a, Y - b \rangle$ for some $a, b \in k$ by **(15.5)**. Write

$$f(X, Y) = \partial f/\partial X(a, b)(X - a) + \partial f/\partial Y(a, b)(Y - b) + g$$

where $g \in \mathfrak{m}^2$. Then $R_{\mathfrak{p}}$ is a DVR if and only if $\partial f/\partial X(a, b)$ and $\partial f/\partial Y(a, b)$ are not both equal to zero owing to **(23.10)** applied after making the change of variables $X' := X - a$ and $Y' := Y - b$.

Clearly, R satisfies (S_2). Further, R satisfies (R_1) if and only if $R_{\mathfrak{p}}$ is a DVR for every nonzero prime $\mathfrak{p}$. Hence, by Serre's Criterion, R is normal if and only if $\partial f/\partial X$ and $\partial f/\partial Y$ do not both belong to any maximal ideal $\mathfrak{m}$ of P containing f. (Put geometrically, R is normal if and only if the plane curve $C : f = 0 \subset k^2$ is nonsingular everywhere.) Thus R is normal if and only if $\langle f, \partial f/\partial X, \partial f/\partial Y \rangle = 1$.

EXERCISE **(23.19)**. — Prove that a Noetherian domain R is normal if and only if, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_{\mathfrak{p}}$ is principal.

EXERCISE **(23.20)**. — Let R be a Noetherian ring, K its total quotient ring,

$$\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\} \quad \text{and} \quad \Sigma := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{depth}(R_{\mathfrak{p}}) = 1 \,\}.$$

Assuming (S_1) holds in R, prove $\Phi \subset \Sigma$, and prove $\Phi = \Sigma$ if and only if (S_2) holds.

Further, without assuming (S_1) holds, prove this canonical sequence is exact:

$$R \to K \to \textstyle\prod_{\mathfrak{p} \in \Sigma} K_{\mathfrak{p}}/R_{\mathfrak{p}}. \qquad \textbf{(23.20.1)}$$

EXERCISE **(23.21)**. — Let R be a Noetherian ring, and K its total quotient ring. Set $\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\}$. Prove these three conditions are equivalent:

(1) R is normal.
(2) (R_1) and (S_2) hold.
(3) (R_1) and (S_1) hold, and $R \to K \to \prod_{\mathfrak{p} \in \Phi} K_{\mathfrak{p}}/R_{\mathfrak{p}}$ is exact.

24. Dedekind Domains

Dedekind domains are defined as the normal Noetherian domains of dimension 1. We prove they are the Noetherian domains whose localizations at nonzero primes are discrete valuation rings. Next we prove the Main Theorem of Classical Ideal Theory: in a Dedekind domain, every nonzero ideal factors uniquely into primes. Then we prove that a normal domain has a module-finite integral closure in any finite separable extension of its fraction field by means of Artin's Character Theorem and the trace pairing of a separable extension. We conclude that a ring of algebraic integers is a Dedekind domain and that, if a domain is a finitely generated algebra over a field of characteristic 0, then in any algebraic extension of its fraction field — in particular, in the fraction field itself — the integral closure is a finitely generated module over the domain and is a finitely generated algebra over the field.

Definition **(24.1)**. — A domain R is said to be **Dedekind** if it is Noetherian, normal, and of dimension 1.

Example **(24.2)**. — Examples of Dedekind domains include the integers $\mathbb{Z}$, the Gaussian integers $\mathbb{Z}\big[\sqrt{-1}\,\big]$, the polynomial ring $k[X]$ in one variable over a field, and any DVR. Indeed, those rings are PIDs, and every PID R is a Dedekind domain: R is Noetherian by definition; R is a UFD, so normal by Gauss's Theorem, **(10.25)**; and R is of dimension 1 since every nonzero prime is maximal by **(2.20)**.

On the other hand, any local Dedekind domain is a DVR by **(23.8)**.

Example **(24.3)**. — Let $d \in \mathbb{Z}$ be a square-free integer. Set $R := \mathbb{Z} + \mathbb{Z}\eta$ where

$$\eta := \begin{cases} (1+\sqrt{d})/2 & \text{if } d \equiv 1 \pmod 4; \\ \sqrt{d} & \text{if not.} \end{cases}$$

Then R is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ by [1, Prp. (6.14), p. 412]; so R is normal. Also, $\dim(R) = \dim(\mathbb{Z})$ by **(15.11)**; so $\dim(R) = 1$. Finally, R is Noetherian by **(16.11)** as $\mathbb{Z}$ is so and as $R := \mathbb{Z} + \mathbb{Z}\eta$. Thus R is Dedekind.

Example **(24.4)**. — Let k be an algebraically closed field, $P := k[X, Y]$ the polynomial ring in two variables, $f \in P$ irreducible. By **(23.18)**, R is a Noetherian domain of dimension 1, and R is Dedekind if and only if $\langle f, \partial f/\partial X, \partial f/\partial Y\rangle = 1$.

Exercise **(24.5)**. — Let R be a domain, S a multiplicative set.

(1) Assume $\dim(R) = 1$. Prove $\dim(S^{-1}R) = 1$ if and only if there is a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

(2) Assume $\dim(R) \geq 1$. Prove $\dim(R) = 1$ if and only if $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero prime $\mathfrak{p}$.

Exercise **(24.6)**. — Let R be a Dedekind domain, S a multiplicative set. Prove $S^{-1}R$ is a Dedekind domain if and only if there's a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

Proposition **(24.7)**. — *Let R be a Noetherian domain, not a field. Then R is a Dedekind domain if and only if $R_{\mathfrak{p}}$ is a DVR for every nonzero prime $\mathfrak{p}$.*

PROOF: If R is Dedekind, then $R_\mathfrak{p}$ is too by **(24.6)**; so $R_\mathfrak{p}$ is a DVR by **(23.8)**.

Conversely, suppose $R_\mathfrak{p}$ is a DVR for every nonzero prime $\mathfrak{p}$. Then, trivially, R satisfies (R_1) and (S_2); so R is normal by Serre's Criterion. Since R is not a field, $\dim(R) \geq 1$; whence, $\dim(R) = 1$ by **(24.5)**(2). Thus R is Dedekind. □

EXERCISE **(24.8)**. — Let R be a Dedekind domain, and $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ideals. By first reducing to the case that R is local, prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}),$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

PROPOSITION **(24.9)**. — *In a Noetherian domain R of dimension 1, every ideal $\mathfrak{a} \neq 0$ has a unique factorization $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ with the $\mathfrak{q}_i$ primary and their primes $\mathfrak{p}_i$ distinct; further, $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \operatorname{Ass}(R/\mathfrak{a})$ and $\mathfrak{q}_i = \mathfrak{a}R_{\mathfrak{p}_i} \cap R$ for each i.*

PROOF: The Lasker–Noether Theorem, **(18.20)**, yields an irredundant primary decomposition $\mathfrak{a} = \bigcap \mathfrak{q}_i$. Say $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Then by **(18.18)** the $\mathfrak{p}_i$ are distinct and $\{\mathfrak{p}_i\} = \operatorname{Ass}(R/\mathfrak{a})$.

The $\mathfrak{q}_i$ are pairwise comaximal for the following reason. Suppose $\mathfrak{q}_i + \mathfrak{q}_j$ lies in a maximal ideal $\mathfrak{m}$. Now, $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ by **(18.5)**; so $\mathfrak{p}_i^{n_i} \subset \mathfrak{q}_i$ for some n_i by **(3.19)**. Hence $\mathfrak{p}_i^{n_i} \subset \mathfrak{m}$. So $\mathfrak{p}_i \subset \mathfrak{m}$ by **(2.2)**. But $0 \neq \mathfrak{a} \subset \mathfrak{p}_i$; hence, $\mathfrak{p}_i$ is maximal since $\dim(R) = 1$. Therefore, $\mathfrak{p}_i = \mathfrak{m}$. Similarly, $\mathfrak{p}_j = \mathfrak{m}$. Hence $i = j$. Thus the $\mathfrak{q}_i$ are pairwise comaximal. So the Chinese Remainder Theorem, **(1.12)**, yields $\mathfrak{a} = \prod_i \mathfrak{q}_i$.

As to uniqueness, let $\mathfrak{a} = \prod \mathfrak{q}_i$ be any factorization with the $\mathfrak{q}_i$ primary and their primes $\mathfrak{p}_i$ distinct. The $\mathfrak{p}_i$ are minimal containing $\mathfrak{a}$ as $\dim(R) = 1$; so the $\mathfrak{p}_i$ are associated primes by **(17.17)**. By the above reasoning, the $\mathfrak{q}_i$ are pairwise comaximal and so $\prod \mathfrak{q}_i = \bigcap \mathfrak{q}_i$. Hence $\mathfrak{a} = \bigcap \mathfrak{q}_i$ is an irredundant primary decomposition by **(18.18)**. So the $\mathfrak{p}_i$ are unique by the First Uniqueness Theorem, **(18.19)**, and $\mathfrak{q}_i = \mathfrak{a}R_{\mathfrak{p}_i} \cap R$ by the Second Uniqueness Theorem, **(18.24)**, and by **(12.15)**(3). □

THEOREM **(24.10)** (Main Theorem of Classical Ideal Theory). — *Let R be a domain. Assume R is Dedekind. Then every nonzero ideal $\mathfrak{a}$ has a unique factorization into primes $\mathfrak{p}$. In fact, if $v_\mathfrak{p}$ denotes the valuation of $R_\mathfrak{p}$, then*

$$\mathfrak{a} = \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \quad \textit{where} \quad v_\mathfrak{p}(\mathfrak{a}) := \min\{\, v_\mathfrak{p}(a) \mid a \in \mathfrak{a} \,\}.$$

PROOF: Using **(24.9)**, write $\mathfrak{a} = \prod \mathfrak{q}_i$ with the $\mathfrak{q}_i$ primary, their primes $\mathfrak{p}_i$ distinct and unique, and $\mathfrak{q}_i = \mathfrak{a}R_{\mathfrak{p}_i} \cap R$. Then $R_{\mathfrak{p}_i}$ is a DVR by **(24.7)**. So **(23.1.3)** yields $\mathfrak{a}R_{\mathfrak{p}_i} = \mathfrak{p}_i^{m_i} R_{\mathfrak{p}_i}$ with $m_i := \min\{\, v_{\mathfrak{p}_i}(a/s) \mid a \in \mathfrak{a} \text{ and } s \in R - \mathfrak{p}_i \,\}$. But $v_{\mathfrak{p}_i}(1/s) = 0$. So $v_{\mathfrak{p}_i}(a/s) = v_{\mathfrak{p}_i}(a)$. Hence $m_i := \min\{\, v_{\mathfrak{p}_i}(a) \mid a \in \mathfrak{a} \,\}$. Now, $\mathfrak{p}_i^{m_i}$ is primary by **(18.10)** as $\mathfrak{p}_i$ is maximal; so $\mathfrak{p}_i^{m_i} R_{\mathfrak{p}_i} \cap R = \mathfrak{p}_i^{m_i}$ by **(18.22)**. Thus $\mathfrak{q}_i = \mathfrak{p}_i^{m_i}$. □

COROLLARY **(24.11)**. — *A Noetherian domain R of dimension 1 is Dedekind if and only if every primary ideal is a power of its radical.*

PROOF: If R is Dedekind, every primary ideal is a power of its radical by **(24.10)**.

Conversely, given a nonzero prime $\mathfrak{p}$, set $\mathfrak{m} := \mathfrak{p}R_\mathfrak{p}$. Then $\mathfrak{m} \neq 0$. So $\mathfrak{m} \neq \mathfrak{m}^2$ by Nakayama's Lemma. Take $t \in \mathfrak{m} - \mathfrak{m}^2$. Then $\mathfrak{m}$ is the only prime containing t, as $\dim(R_\mathfrak{p}) = 1$ by **(24.5)**(2). So $tR_\mathfrak{p}$ is $\mathfrak{m}$-primary by **(18.10)**. Set $\mathfrak{q} := tR_\mathfrak{p} \cap R$. Then $\mathfrak{q}$ is $\mathfrak{p}$-primary by **(18.8)**. So $\mathfrak{q} = \mathfrak{p}^n$ for some n by hypothesis. But $\mathfrak{q}R_\mathfrak{p} = tR_\mathfrak{p}$ by **(11.15)**(3)(b). So $tR_\mathfrak{p} = \mathfrak{m}^n$. But $t \notin \mathfrak{m}^2$. So $n = 1$. So $R_\mathfrak{p}$ is a DVR by **(23.8)**. Thus R is Dedekind by **(24.7)**. □

Exercise **(24.12)**. — Prove that a semilocal Dedekind domain A is a PID. Begin by proving that each maximal ideal is principal.

Exercise **(24.13)**. — Let R be a Dedekind domain, $\mathfrak{a}$ and $\mathfrak{b}$ two nonzero ideals. Prove (1) every ideal in $R/\mathfrak{a}$ is principal, and (2) $\mathfrak{b}$ is generated by two elements.

Lemma **(24.14)** (E. Artin). — *Let L be a field, G a group, $\sigma_i\colon G \to L^\times$ distinct homomorphisms. Then the σ_i are linearly independent over L in the vector space of set maps $\sigma\colon G \to L$ under valuewise addition and scalar multiplication.*

Proof: Suppose there's an equation $\sum_{i=1}^m a_i\sigma_i = 0$ with nonzero $a_i \in L$. Take $m \geq 1$ minimal. Now, $\sigma_i \neq 0$ as $\sigma_i\colon G \to L^\times$; so $m \geq 2$. Since $\sigma_1 \neq \sigma_2$, there's an $x \in G$ with $\sigma_1(x) \neq \sigma_2(x)$. Then $\sum_{i=1}^m a_i\sigma_i(x)\sigma_i(y) = \sum_{i=1}^m a_i\sigma_i(xy) = 0$ for every $y \in G$ since σ_i is a homomorphism.

Set $\tau_i(x) := 1 - \sigma_i(x)/\sigma_1(x)$. Then

$$\sum_{i=1}^m a_i\tau_i(x)\sigma_i = \sum_{i=1}^m a_i\sigma_i - \frac{1}{\sigma_1(x)}\sum_{i=1}^m a_i\sigma_i(x)\sigma_i = 0.$$

But $\tau_1(x) = 0$ and $\tau_2(x) \neq 0$, contradicting the minimality of m. □

(24.15) (*Trace*). — Let L/K be a finite Galois field extension. Its **trace** is this:

$$\mathrm{tr}\colon L \to K \quad \text{by} \quad \mathrm{tr}(x) := \sum_{\sigma\in \mathrm{Gal(L/K)}} \sigma(x).$$

Clearly, tr is K-linear. It is nonzero by **(24.14)** applied with $G := L^\times$.

Consider the symmetric K-bilinear **Trace Pairing**:

$$L \times L \to K \quad \text{by} \quad (x, y) \mapsto \mathrm{tr}(xy). \tag{24.15.1}$$

It is nondegenerate for this reason. Since tr is nonzero, there is a $z \in L$ with $\mathrm{tr}(z) \neq 0$. Now, given $x \in L^\times$, set $y := z/x$. Then $\mathrm{tr}(xy) \neq 0$, as desired.

Lemma **(24.16)**. — *Let R be a normal domain, K its fraction field, L/K a finite Galois field extension, and $x \in L$ integral over R. Then* $\mathrm{tr}(x) \in R$.

Proof: Let $x^n + a_1x^{n-1} + \cdots + a_n = 0$ be an equation of integral dependence for x over R. Let $\sigma \in \mathrm{Gal(L/K)}$. Then

$$(\sigma x)^n + a_1(\sigma x)^{n-1} + \cdots + a_n = 0;$$

so σx is integral over R. Hence $\mathrm{tr}(x)$ is integral over R, and lies in K. Thus $\mathrm{tr}(x) \in R$ since R is normal. □

Theorem **(24.17)** (Finiteness of integral closure). — *Let R be a normal Noetherian domain, K its fraction field, L/K a finite separable field extension, and R' the integral closure of R in L. Then R' is module finite over R.*

Proof: Let L_1 be the Galois closure of L/K, and R_1' the integral closure of R in L_1. Let $z_1, \ldots, z_n \in L_1$ form a K-basis. Using **(11.21)**, write $z_i = y_i/a_i$ with $y_i \in R_1'$ and $a_i \in R$. Clearly, $y_1, \ldots, y_n$ form a basis of L_1/K contained in R_1'.

Let $x_1, \ldots, x_n$ form the dual basis with respect to the Trace Paring, **(24.15.1)**, so that $\mathrm{tr}(x_iy_j) = \delta_{ij}$. Given $b \in R'$, write $b = \sum c_ix_i$ with $c_i \in K$. Fix j. Then

$$\mathrm{tr}(by_j) = \mathrm{tr}\Big(\sum c_ix_iy_j\Big) = \sum c_i\,\mathrm{tr}(x_iy_j) = c_j \quad \text{for each } j.$$

But $by_j \in R'_1$. So $c_j \in R$ by **(24.16)**. Thus $R' \subset \sum Rx_i$. Since R is Noetherian, R' is a finitely generated R-module, as desired. □

COROLLARY **(24.18)**. — *Let R be a Dedekind domain, K its fraction field, L/K a finite separable field extension. Then the integral closure R' of R in L is Dedekind.*

PROOF: First, R' is module finite over R by **(24.17)**; so R' is Noetherian by **(16.18)**. Second, R' is normal by **(10.24)**. Finally, $\dim(R') = \dim(R)$ by **(15.11)**, and $\dim(R) = 1$ as R is Dedekind. Thus R is Dedekind. □

THEOREM **(24.19)**. — *A ring of algebraic integers is a Dedekind domain.*

PROOF: By **(24.2)**, $\mathbb{Z}$ is a Dedekind domain; whence, so is its integral closure in any field that is a finite extension of $\mathbb{Q}$ by **(24.18)**. □

THEOREM **(24.20)** (Noether). — *Let k be a field of characteristic 0, and R a domain that is a finitely generated k-algebra. Set $K := \operatorname{Frac}(R)$. Let L/K be a finite field extension (possibly $L = K$), and let R' be the integral closure of R in L. Then R' is a finitely generated R-module and a finitely generated k-algebra.*

PROOF: By the Noether Normalization Lemma, **(15.1)**, R is a module-finite k-algebra over a polynomial subring P. Then P is normal by Gauss's Theorem, **(10.25)**, and Noetherian by the Hilbert Basis Theorem, **(16.11)**; also, $L/\operatorname{Frac}(P)$ is a finite field extension, which is separable as k is of characteristic 0. Hence, R' is module finite over P by **(24.17)**. The assertion follows. □

(24.21) (*Other cases*). — In **(24.18)**, even if L/K is inseparable, the integral closure R' of R in L is still Dedekind, as is proved below in Lecture 26.

However, Akizuki constructed an example of a DVR R and a finite inseparable extension $L/\operatorname{Frac}(R)$ such that the integral closure of R is a DVR, but is not module finite over R. The construction is nicely explained in [7, Secs. 9.4(1) and 9.5]. Thus separability is a necessary hypothesis in **(24.17)**.

Noether's Theorem, **(24.20)**, remains valid in positive characteristic, but the proof is more involved. See [3, (13.13), p. 297].

25. Fractional Ideals

A fractional ideal is defined to be a submodule of the fraction field of a domain. A fractional ideal is called invertible if its product with another fractional ideal is equal to the given domain. We characterize the invertible fractional ideals as those that are nonzero, finitely generated, and principal locally at every maximal ideal. We prove that, in a Dedekind domain, any two nonzero integral (that is, ordinary) ideals have an invertible fractional ideal as their quotient. We characterize Dedekind domains as those domains whose integral ideals are, equivalently, all invertible, all projective, or all finitely generated and flat. Further, we prove a Noetherian domain is Dedekind if and only if every torsion-free module is flat. Finally, we prove the ideal class group is equal to the Picard group; the former is the group of invertible fractional ideals modulo those that are principal, and the latter is the group, under tensor product, of isomorphism classes of modules local free of rank 1.

Definition **(25.1)**. — Let R be a domain, and set $K := \operatorname{Frac}(R)$. We call an R-submodule M of K a **fractional ideal**. We call M **integral** if $M \subset R$. We call M **principal** if there is an $x \in K$ with $M = Rx$.

Given another fractional ideal N, form these two new fractional ideals:

$$MN := \left\{ \sum x_i y_i \;\middle|\; x_i \in M \text{ and } y_i \in N \right\} \quad \text{and} \quad (M : N) := \{\, z \in K \mid zN \subset M \,\}.$$

We call them the **product** of M and N and the **quotient** of M by N.

Exercise **(25.2)**. — Let R be a domain, M and N nonzero fractional ideals. Prove that M is principal if and only if there exists some isomorphism $M \simeq R$. Construct the following canonical surjection and canonical isomorphism:

$$\pi\colon M \otimes N \twoheadrightarrow MN \quad \text{and} \quad \varphi\colon (M : N) \xrightarrow{\sim} \operatorname{Hom}(N, M).$$

Proposition **(25.3)**. — *Let R be a domain, and $K := \operatorname{Frac}(R)$. Consider these finiteness conditions on a fractional ideal M:*

(1) *There exist integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ with $\mathfrak{b} \neq 0$ and $(\mathfrak{a} : \mathfrak{b}) = M$.*
(2) *There exists an $x \in K^\times$ with $xM \subset R$.*
(3) *There exists a nonzero $x \in R$ with $xM \subset R$.*
(4) *M is finitely generated.*

Then (1), (2), *and* (3) *are equivalent, and they are implied by* (4). *Further, all four conditions are equivalent for every M if and only if R is Noetherian.*

Proof: Assume (1) holds. Take any nonzero $x \in \mathfrak{b}$. Given $m \in M$, clearly $xm \in \mathfrak{a} \subset R$; so $xM \subset R$. Thus (2) holds.

Assume (2) holds. Write $x = a/b$ with $a, b \in R$ and $a, b \neq 0$. Then $aM \subset bR \subset R$. Thus (3) holds.

If (3) holds, then xM and xR are integral, and $M = (xM : xR)$; thus (1) holds.

Assume (4) holds. Say $y_1/x_1, \dots, y_n/x_n \in K^\times$ generate M with $x_i, y_i \in R$. Set $x := \prod x_i$. Then $x \neq 0$ and $xM \subset R$. Thus (3) holds.

Assume (3) holds and R is Noetherian. Then $xM \subset R$. So xM is finitely generated, say by $y_1, \dots, y_n$. Then $y_1/x, \dots, y_n/x$ generate M. Thus (4) holds.

Finally, assume all four conditions are equivalent for every M. If M is integral, then (3) holds with $x := 1$, and so (4) holds. Thus R is Noetherian. □

LEMMA **(25.4)**. — *Let R be a domain, M and N fractional ideals. Let S be a multiplicative set. Then*

$$S^{-1}(MN) = (S^{-1}M)(S^{-1}N) \quad \textit{and} \quad S^{-1}(M:N) \subset (S^{-1}M : S^{-1}N),$$

with equality if N is finitely generated.

PROOF: Given $x \in S^{-1}(MN)$, write $x = (\sum m_i n_i)/s$ with $m_i \in M$, with $n_i \in N$, and with $s \in S$. Then $x = \sum (m_i/s)(n_i/1)$, and so $x \in (S^{-1}M)(S^{-1}N)$. Thus $S^{-1}(MN) \subset (S^{-1}M)(S^{-1}N)$.

Conversely, given $x \in (S^{-1}M)(S^{-1}N)$, say $x = \sum (m_i/s_i)(n_i/t_i)$ with $m_i \in M$ and $n_i \in N$ and $s_i, t_i \in S$. Set $s := \prod s_i$ and $t := \prod t_i$. Then

$$x = \sum (m_i n_i / s_i t_i) = \sum m_i' n_i' / st \in S^{-1}(MN)$$

with $m_i' \in M$ and $n_i' \in N$. Thus $S^{-1}(MN) \supset (S^{-1}M)(S^{-1}N)$, so equality holds.

Given $z \in S^{-1}(M:N)$, write $z = x/s$ with $x \in (M:N)$ and $s \in S$. Given $y \in S^{-1}N$, write $y = n/t$ with $n \in N$ and $t \in S$. Then $z \cdot n/t = xn/st$ and $xn \in M$ and $st \in S$. So $z \in (S^{-1}M : S^{-1}N)$. Thus $S^{-1}(M:N) \subset (S^{-1}M : S^{-1}N)$.

Conversely, say N is generated by $n_1, \dots, n_r$. Given $z \in (S^{-1}M : S^{-1}N)$, write $zn_i/1 = m_i/s_i$ with $m_i \in M$ and $s_i \in S$. Set $s := \prod s_i$. Then $sz \cdot n_i \in M$. So $sz \in (M:N)$. Hence $z \in S^{-1}(M:N)$, as desired. □

DEFINITION **(25.5)**. — Let R be a domain. We call a fractional ideal M **locally principal** if, for every maximal ideal $\mathfrak{m}$, the localization $M_{\mathfrak{m}}$ is principal over $R_{\mathfrak{m}}$.

EXERCISE **(25.6)**. — Let R be a domain, M and N fractional ideals. Prove that the map $\pi\colon M \otimes N \to MN$ is an isomorphism if M is locally principal.

(25.7) (*Invertible fractional ideals*). — Let R be a domain. A fractional ideal M is said to be **invertible** if there is some fractional ideal M^{-1} with $MM^{-1} = R$.

For example, a nonzero principal ideal Rx is invertible, as $(Rx)(R \cdot 1/x) = R$.

PROPOSITION **(25.8)**. — *Let R be a domain, M an invertible fractional ideal. Then M^{-1} is unique; in fact, $M^{-1} = (R:M)$.*

PROOF: Clearly $M^{-1} \subset (R:M)$ as $MM^{-1} = R$. But, if $x \in (R:M)$, then $x \cdot 1 \in (R:M)MM^{-1} \subset M^{-1}$, so $x \in M^{-1}$. Thus $(R:M) \subset M^{-1}$, as desired. □

LEMMA **(25.9)**. — *An invertible ideal is finitely generated and nonzero.*

PROOF: Let R be the domain, M the ideal. Say $1 = \sum m_i n_i$ with $m_i \in M$ and $n_i \in M^{-1}$. Let $m \in M$. Then $m = \sum m_i m n_i$. But $mn_i \in R$ as $m \in M$ and $n_i \in M^{-1}$. So the m_i generate M. Trivially, $M \neq 0$. □

LEMMA **(25.10)**. — *Let A be a local domain. Then a fractional ideal M is invertible if and only if M is principal and nonzero.*

PROOF: Assume M is invertible. Say $1 = \sum m_i n_i$ with $m_i \in M$ and $n_i \in M^{-1}$. As A is local, $A - A^\times$ is an ideal. So there's a j with $m_j n_j \in A^\times$. Let $m \in M$. Then $mn_j \in A$. Set $a := (mn_j)(m_j n_j)^{-1} \in A$. Then $m = am_j$. Thus $M = Am_j$.

Conversely, if M is principal and nonzero, then it's always invertible by **(25.7)**. □

EXERCISE **(25.11)**. — Let R be a UFD. Show that a fractional ideal M is invertible if and only if M is principal and nonzero.

THEOREM **(25.12)**. — *Let R be a domain, M a fractional ideal. Then M is invertible if and only if M is finitely generated and locally principal.*

PROOF: Say $MN = R$. Then M is finitely generated and nonzero by **(25.9)**. Let S be a multiplicative set. Then $(S^{-1}M)(S^{-1}N) = S^{-1}R$ by **(25.4)**. Let $\mathfrak{m}$ be a maximal ideal. Then, therefore, $M_{\mathfrak{m}}$ is an invertible fractional ideal over $R_{\mathfrak{m}}$. Thus $M_{\mathfrak{m}}$ is principal by **(25.10)**, as desired.

Conversely, set $\mathfrak{a} := M(R : M) \subset R$. Assume M is finitely generated. Then **(25.4)** yields $\mathfrak{a}_{\mathfrak{m}} = M_{\mathfrak{m}}(R_{\mathfrak{m}} : M_{\mathfrak{m}})$. In addition, assume $M_{\mathfrak{m}}$ is principal and nonzero. Then **(25.7)** and **(25.8)** yield $\mathfrak{a}_{\mathfrak{m}} = R_{\mathfrak{m}}$. Hence **(13.13)** yields $\mathfrak{a} = R$, as desired. □

THEOREM **(25.13)**. — *Let R be a Dedekind domain, $\mathfrak{a}$, $\mathfrak{b}$ nonzero integral ideals. Set $M := (\mathfrak{a} : \mathfrak{b})$. Then M is invertible, and has a unique factorization into powers of primes $\mathfrak{p}$. In fact, if $v_{\mathfrak{p}}$ denotes the valuation of $R_{\mathfrak{p}}$, then*

$$M = \prod \mathfrak{p}^{v_{\mathfrak{p}}(M)} \quad \textit{where} \quad v_{\mathfrak{p}}(M) := \min\{\, v_{\mathfrak{p}}(x) \mid x \in M \,\}.$$

Finally, $v_{\mathfrak{p}}(M) = \min\{v_{\mathfrak{p}}(x_i)\}$ if the x_i generate M.

PROOF: First, R is Noetherian. So **(25.2)** yields that M is finitely generated and that there is a nonzero $x \in R$ with $xM \subset R$. Hence, each localization $xM_{\mathfrak{p}}$ is principal by **(23.1.3)**. Thus M is invertible by **(25.12)**.

Next, the Main Theorem of Classical Ideal Theory, **(24.10)**, yields $\langle x \rangle = \prod \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ and $xM = \prod \mathfrak{p}^{v_{\mathfrak{p}}(xM)}$. Since $v_{\mathfrak{p}}(xM) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(M)$, we can cancel the $v_{\mathfrak{p}}(x)$ to conclude $M = \prod \mathfrak{p}^{v_{\mathfrak{p}}(M)}$.

Finally, given $x \in M$, say $x = \sum_{i=1}^{n} a_i x_i$ with $a_i \in R$. Then **(23.1.1)** yields

$$v_{\mathfrak{p}}(x) \geq \min\{v_{\mathfrak{p}}(a_i x_i)\} \geq \min\{v_{\mathfrak{p}}(x_i)\}$$

by induction on n. Thus $v_{\mathfrak{p}}(M) = \min\{v_{\mathfrak{p}}(x_i)\}$. □

EXERCISE **(25.14)**. — Show that a ring is a PID if and only if it's a Dedekind domain and a UFD.

(25.15) (*Invertible modules*). — Let R be an arbitrary ring. We call a module M **invertible** if there is another module N with $M \otimes N \simeq R$.

For example, suppose R is a domain. Let M be an invertible fractional ideal; say N is a fractional ideal with $MN = R$. Then M is locally principal by **(25.12)**. So $M \otimes N = MN$ by **(25.6)**. Thus M is an invertible abstract module.

EXERCISE **(25.16)**. — Let R be an ring, M an invertible module. Prove that M is finitely generated, and that, if R is local, then M is free of rank 1.

EXERCISE **(25.17)**. — Show these conditions on an R-module M are equivalent:

(1) M is invertible.
(2) M is finitely generated, and $M_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ at each maximal ideal $\mathfrak{m}$.
(3) M is locally free of rank 1.

Assuming these conditions hold, show that $M \otimes \operatorname{Hom}(M, R) = R$.

LEMMA **(25.18)**. — *Let R be a domain, M a fractional ideal. Then M is an invertible fractional ideal if and only if M is a projective abstract module.*

PROOF: Assume M is an invertible fractional ideal. Then M is an invertible abstract module by **(25.15)**. Hence M is locally free of rank 1 by **(25.17)**. So M is projective by **(13.22)**.

Conversely, assume M is projective. Then by **(5.22)**, there exists a module M' with $M \oplus M' \simeq R^{\oplus\Lambda}$. Let $\rho\colon R^{\oplus\Lambda} \to M$ be the projection, and set $x_\lambda := \rho(e_\lambda)$. Define $\varphi_\lambda\colon M \hookrightarrow R^{\oplus\Lambda} \to R$ as the composition of the injection with the projection φ_λ on the λth factor. Then for all $x \in M$, we have $x = \sum_{\lambda\in\Lambda} \varphi_\lambda(x)x_\lambda$ and $\varphi_\lambda(x) = 0$ for almost all λ.

Fix a nonzero $y \in M$. For $\lambda \in \Lambda$, set $q_\lambda := \frac{1}{y}\varphi_\lambda(y) \in \mathrm{Frac}(R)$. Set $N := \sum Rq_\lambda$. Then for any nonzero $x \in M$, let's check that $xq_\lambda = \varphi_\lambda(x)$. Write $x = a/b$ and $y = c/d$ with $a, b, c, d \in R$. Then $a, c \in M$; whence, $ad\varphi(y) = \varphi(ac) = bc\varphi(x)$. Thus $xq_\lambda = \varphi_\lambda(x) \in R$. Hence $M \cdot N \subset R$. But $y = \sum \varphi_\lambda(y)y_\lambda$, so $1 = y_\lambda q_\lambda$. Thus $M \cdot N = R$. □

THEOREM **(25.19)**. — *Let R be a domain. Then the following are equivalent:*

(1) *R is Dedekind;*
(2) *every integral ideal is invertible;*
(3) *every integral ideal is projective;*
(4) *every integral ideal is finitely generated and flat.*

PROOF: Let $\mathfrak{a}$ be an integral ideal. Assume (1). Since $\mathfrak{a} = (\mathfrak{a} : R)$, it is invertible by **(25.13)**. Thus (2) holds.

Conversely, assume (2). Then $\mathfrak{a}$ is finitely generated by **(25.9)**. Thus R is Noetherian. Let $\mathfrak{p}$ be any nonzero prime of R. Then by hypothesis, $\mathfrak{p}$ is invertible. So by **(25.12)**, it is locally principal. So $R_\mathfrak{p}$ is a DVR by **(23.8)**. Hence R is Dedekind by **(24.7)**. Thus (1) holds. Thus (1) and (2) are equivalent.

Recall that (2) and (3) are equivalent by **(25.18)**. But (2) implies that R is Noetherian by **(25.9)**. Thus (3) and (4) are equivalent by **(16.18)** and **(13.22)**. □

THEOREM **(25.20)**. — *A Noetherian domain R is Dedekind if and only if every torsion-free module is flat.*

PROOF: (Of course, as R is a domain, every flat module is torsion free by **(9.20)**.)

Assume R is Dedekind. Let M be a torsion-free module, $\mathfrak{m}$ a maximal ideal. Let's see that $M_\mathfrak{m}$ is torsion free over $R_\mathfrak{m}$. Let $z \in R_\mathfrak{m}$ be nonzero, and say $z = x/s$ with $x, s \in R$ and $s \notin \mathfrak{m}$. Then $\mu_x\colon M \to M$ is injective as M is torsion free. So $\mu_x\colon M_\mathfrak{m} \to M_\mathfrak{m}$ is injective by the Exactness of Localization. But $\mu_{x/s} = \mu_x\mu_{1/s}$ and $\mu_{1/s}$ is invertible. So $\mu_{x/s}$ is injective. Thus $M_\mathfrak{m}$ is torsion free.

Since R is Dedekind, $R_\mathfrak{m}$ is a DVR by **(24.7)**, so a PID by **(24.1)**. Hence $M_\mathfrak{m}$ is flat over $R_\mathfrak{m}$ by **(9.20)**. But $\mathfrak{m}$ is arbitrary. Therefore, M is flat over R by **(13.19)**.

Conversely, assume every torsion-free module is flat. Then, in particular, every integral ideal is flat. But R is Noetherian. Thus R is Dedekind by **(25.19)**. □

(25.21) (*The Picard Group*). — Let R be a ring. We denote the collection of isomorphism classes of invertible modules by $\mathrm{Pic}(R)$. By **(25.16)**, every invertible module is finitely generated, so isomorphic to a quotient of R^n for some integer n. Hence, $\mathrm{Pic}(R)$ is a set. Further, $\mathrm{Pic}(R)$ is, clearly, a group under tensor product with the class of R as identity. We call $\mathrm{Pic}(R)$ the **Picard Group** of R.

Assume R is a domain, and set $K := \mathrm{Frac}(R)$. Given an invertible module M, we can embed M into K as follows. Set $S := R - 0$, and form the canonical map $M \to S^{-1}M$. It is injective owing to **(12.15)** if the multiplication map $\mu_x\colon M \to M$

is injective for any $x \in S$. Fix x, and let's prove μ_x is injective.

Let $\mathfrak{m}$ be a maximal ideal. Clearly, $M_\mathfrak{m}$ is an invertible $R_\mathfrak{m}$-module. So $M_\mathfrak{m} \simeq R_\mathfrak{m}$ by **(25.16)**. Hence $\mu_x \colon M_\mathfrak{m} \to M_\mathfrak{m}$ is injective. Therefore, $\mu_x \colon M \to M$ is injective by **(13.17)**. Thus M embeds canonically into $S^{-1}M$. Now, $S^{-1}M$ is a localization of $M_\mathfrak{m}$, so is a 1-dimensional K-vector space, again as $M_\mathfrak{m} \simeq R_\mathfrak{m}$. Choose an isomorphism $S^{-1}M \simeq K$. It yields the desired embedding of M into K.

Since M is invertible, M is finitely generated by **(25.16)**. Further, as noted, $M_\mathfrak{m} \simeq R_\mathfrak{m}$ at each maximal ideal $\mathfrak{m}$. Say $x \in M_\mathfrak{m}$ corresponds to $1 \in R_\mathfrak{m}$. Then $yx \in M_\mathfrak{m}$ corresponds to $y \in R_\mathfrak{m}$. Thus M is locally principal. So, by **(25.12)**, M is also invertible as a fractional ideal.

The invertible fractional ideals M, clearly, form a group $\mathcal{F}(R)$. Sending an M to its isomorphism class yields a map $\kappa \colon \mathcal{F}(R) \to \operatorname{Pic}(R)$ by **(25.15)**. By the above, κ is surjective. Further, κ is a group homomorphism by **(25.6)**. It's not hard to check that its kernel is the group $\mathcal{P}(R)$ of principal ideals and that $\mathcal{P}(R) = K^\times/R^\times$. We call $\mathcal{F}(R)/\mathcal{P}(R)$ the **Ideal Class Group** of R. Thus $\mathcal{F}(R)/\mathcal{P}(R) = \operatorname{Pic}(R)$; in other words, the Ideal Class Group is canonically isomorphic to the Picard Group.

Every invertible fractional ideal is, by **(25.12)**, finitely generated and nonzero, so of the form $(\mathfrak{a} : \mathfrak{b})$ where $\mathfrak{a}$ and $\mathfrak{b}$ are integral and nonzero by **(25.3)**. Conversely, by **(25.13)** and **(25.19)**, every fractional ideal of this form is invertible if and only if R is Dedekind. In fact, then $\mathcal{F}(R)$ is the free abelian group on the prime ideals. Further, then $\operatorname{Pic}(R) = 0$ if and only if R is UFD, or equivalently by **(25.14)**, a PID. See [1, Ch. 11, Sects. 10–11, pp. 424–437] for a discussion of the case in which R is a ring of quadratic integers, including many examples where $\operatorname{Pic}(R) \neq 0$.

26. Arbitrary Valuation Rings

A valuation ring is, by definition, a subring of a field whose elements either lie in the subring or their reciprocals do. Valuation rings are normal local domains. They are maximal under domination, that is, inclusion of both the local rings and their maximal ideals. Given any subring, its normalization is equal to the intersection of all the valuation rings containing it. We end with the Krull–Akizuki Theorem: given a 1-dimensional Noetherian domain, a finite extension of its fraction field, and a proper subring of the extension containing the domain, that subring too is 1-dimensional and Noetherian. We conclude that, if we normalize a Dedekind domain in any finite extension of its fraction field, we obtain another Dededind domain.

DEFINITION **(26.1)**. — A subring V of a field K is said to be a **valuation ring** of K if, whenever $z \in K - V$, then $1/z \in V$.

PROPOSITION **(26.2)**. — *Let V be a valuation ring of a field K, and set*

$$\mathfrak{m} := \{1/z \mid z \in K - V\} \cup \{0\}.$$

Then V is local, $\mathfrak{m}$ is its maximal ideal, and K is its fraction field.

PROOF: Clearly $\mathfrak{m} = V - V^\times$. Let's show $\mathfrak{m}$ is an ideal. Take a nonzero $a \in V$ and nonzero $x, y \in \mathfrak{m}$. Suppose $ax \notin \mathfrak{m}$. Then $ax \in V^\times$. So $a(1/ax) \in V$. So $1/x \in V$. So $x \in V^\times$, a contradiction. Thus $ax \in \mathfrak{m}$. Now, by hypothesis, either $x/y \in V$ or $y/x \in V$. Say $y/x \in V$. Then $1 + (y/x) \in V$. So $x + y = (1 + (y/x))x \in \mathfrak{m}$. Thus $\mathfrak{m}$ is an ideal. Hence V is local and $\mathfrak{m}$ is its maximal ideal by **(3.4)**. Finally, K is its fraction field, because whenever $z \in K - V$, then $1/z \in V$. □

EXERCISE **(26.3)**. — Let V be a domain. Show that V is a valuation ring if and only if, given any two ideals $\mathfrak{a}$ and $\mathfrak{b}$, either $\mathfrak{a}$ lies in $\mathfrak{b}$ or $\mathfrak{b}$ lies in $\mathfrak{a}$.

EXERCISE **(26.4)**. — Let V be a valuation ring, $\mathfrak{m}$ its maximal ideal, and $\mathfrak{p} \subset \mathfrak{m}$ another prime ideal. Prove that $V_\mathfrak{p}$ is a valuation ring, that its maximal ideal $\mathfrak{p}V_\mathfrak{p}$ is equal to $\mathfrak{p}$, and that $V/\mathfrak{p}$ is a valuation ring of the field $V_\mathfrak{p}/\mathfrak{p}$.

EXERCISE **(26.5)**. — Prove that a valuation ring V is normal.

LEMMA **(26.6)**. — *Let R be a domain, $\mathfrak{a}$ an ideal, $K := \mathrm{Frac}(R)$, and $x \in K^\times$. Then either $1 \notin \mathfrak{a}R[x]$ or $1 \notin \mathfrak{a}R[1/x]$.*

PROOF: Assume $1 \in \mathfrak{a}R[x]$ and $1 \in \mathfrak{a}R[1/x]$. Then there are equations

$$1 = a_0 + \cdots + a_n x^n \quad \text{and} \quad 1 = b_0 + \cdots + b_m/x^m \quad \text{with all} \quad a_i, b_j \in \mathfrak{a}.$$

Assume n, m minimal and $m \leq n$. Multiply through by $1 - b_0$ and $a_n x^n$, getting

$$1 - b_0 = (1 - b_0)a_0 + \cdots + (1 - b_0)a_n x^n \quad \text{and}$$
$$(1 - b_0)a_n x^n = a_n b_1 x^{n-1} + \cdots + a_n b_m x^{n-m}.$$

Combine the latter equations, getting

$$1 - b_0 = (1 - b_0)a_0 + \cdots + (1 - b_0)a_{n-1}x^{n-1} + a_n b_1 x^{n-1} + \cdots + a_n b_m x^{n-m}.$$

Simplify, getting an equation of the form $1 = c_0 + \cdots + c_{n-1}x^{n-1}$ with $c_i \in \mathfrak{a}$, which contradicts the minimality of n. □

LEMMA **(26.7)**. — *Let A, B be local rings, and $\mathfrak{m}$, $\mathfrak{n}$ their maximal ideals. If $B \supset A$, then these conditions are equivalent:* (1) $\mathfrak{n} \cap A = \mathfrak{m}$; (2) $1 \notin \mathfrak{m}B$; (3) $\mathfrak{m} \subset \mathfrak{n}$.

PROOF: Assume $B \supset A$. If (1) holds, then $\mathfrak{m}B \subset \mathfrak{n}$, so (2) holds. If (2) holds, then $\mathfrak{m}B \subset \mathfrak{n}$, so (3) holds. If (3) holds, then $\mathfrak{m} \subset \mathfrak{n} \cap A \subsetneq A$, so (1) holds. □

(26.8) (*Domination*). — Let A, B be local rings, and $\mathfrak{m}$, $\mathfrak{n}$ their maximal ideals. We say B **dominates** A if $B \supset A$ and $\mathfrak{n} \cap A = \mathfrak{m}$.

PROPOSITION **(26.9)**. — *Let K be a field, A a local subring. Then A is dominated by a valuation ring V of K.*

PROOF: Let $\mathfrak{m}$ be the maximal ideal of A. Let $\mathcal{S}$ be the set of subrings R of K with $R \supset A$ and $1 \notin \mathfrak{m}R$. Then $A \in \mathcal{S}$. Order $\mathcal{S}$ by inclusion. Let $\{R_\lambda\}$ be a totally ordered subset. Set $R := \bigcup R_\lambda$. If $1 \in \mathfrak{m}R$, then

$$1 = a_1x_1 + \cdots + a_nx_n \quad \text{with} \quad a_i \in \mathfrak{m} \quad \text{and} \quad x_i \in R.$$

But then there is λ such that $x_i \in R_\lambda$ for all i; so $1 \in \mathfrak{m}R_\lambda$, a contradiction. Thus $R \in \mathcal{S}$. Hence, by Zorn's Lemma, $\mathcal{S}$ has a maximal element V.

For any nonzero $x \in K$, set $V' := V[x]$ and $V'' := V[1/x]$. By **(26.6)**, either $1 \notin \mathfrak{m}V'$ or $1 \notin \mathfrak{m}V''$. Hence by maximality, either $V = V'$ or $V = V''$. So either $x \in V$ or $1/x \in V$. Thus V is a valuation ring. So V is local by **(26.2)**, and dominates A by **(26.8)** as $1 \notin \mathfrak{m}V$. □

EXERCISE **(26.10)**. — Let K be a field, $\mathcal{S}$ the set of local subrings with fraction field K, ordered by domination. Show its maximal elements are the valuation rings.

THEOREM **(26.11)**. — *Let K be a field, and R a subring of K. Then the integral closure R' of R in K is the intersection of all valuation rings V of K containing R. Further, if R is local, then the V dominating R suffice.*

PROOF: Every valuation ring V is normal by **(26.5)**. So if $V \supset R$, then $V \supset R'$. Thus $\bigcap_{V \supset R} V \supset R'$.

To prove the opposite inclusion, take any $x \in K - R'$. To find a valuation ring V with $V \supset R$ and $x \notin V$, set $y := 1/x$. If $1/y \in R[y]$, then for some n,

$$1/y = a_0y^n + a_1y^{n-1} + \cdots + a_n \quad \text{with} \quad a_\lambda \in R.$$

Multiplying by x^n yields $x^{n+1} - a_nx^n - \cdots - a_0 = 0$. So $x \in R'$, a contradiction.

Thus $1 \notin yR[y]$. So there is a maximal ideal $\mathfrak{m}$ of $R[y]$ containing y. Then the composition $R \to R[y] \to R[y]/\mathfrak{m}$ is surjective as $y \in \mathfrak{m}$. So $\mathfrak{m} \cap R$ is a maximal ideal of R. By **(26.9)**, there is a valuation ring V that dominates $R[y]_\mathfrak{m}$; whence, if R is local, then V also dominates R. But $y \in \mathfrak{m}$; so $x = 1/y \notin V$, as desired. □

(26.12) (*Valuations*). — We call an additive abelian group Γ **totally ordered** if Γ has a subset Γ_+ that is closed under addition and satisfies $-\Gamma_+ \sqcup \{0\} \sqcup \Gamma_+ = \Gamma$.

Given $x, y \in \Gamma$, write $x > y$ if $x - y \in \Gamma_+$. Note that either $x > y$ or $x = y$ or $y > x$. Note that, if $x > y$, then $x + z > y + z$ for any $z \in \Gamma$.

Let V be a domain, and set $K := \operatorname{Frac}(V)$ and $\Gamma := K^\times/V^\times$. Write the group Γ additively, and let $v\colon K^\times \to \Gamma$ be the quotient map. It is a homomorphism:

$$v(xy) = v(x) + v(y). \qquad \textbf{(26.12.1)}$$

Set $\Gamma_+ := v\big(V - 0\big) - 0$. Then Γ_+ is closed under addition. Clearly, V is a valuation ring if and only if $-\Gamma_+ \sqcup \{0\} \sqcup \Gamma_+ = \Gamma$, so if and only if Γ is totally ordered.

Assume V is a valuation ring. Let's prove that, for all $x, y \in K^\times$,

$$v(x+y) \geq \min\{v(x),\, v(y)\} \quad \text{if} \quad x \neq -y. \tag{26.12.2}$$

Indeed, say $v(x) \geq v(y)$. Then $z := x/y \in V$. So $v(z+1) \geq 0$. Hence

$$v(x+y) = v(z+1) + v(y) \geq v(y) = \min\{v(x), v(y)\},$$

Note that **(26.12.1)** and **(26.12.2)** are the same as (1) and (2) of **(23.1)**.

Conversely, start with a field K, with a totally ordered additive abelian group Γ, and with a surjective homomorphism $v\colon K^\times \to \Gamma$ satisfying **(26.12.2)**. Set

$$V := \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}.$$

Then V is a valuation ring, and $\Gamma = K^\times/V^\times$. We call such a v a **valuation** of K, and Γ the **value group** of v or of V.

For example, a DVR V of K is just a valuation ring with value group $\mathbb{Z}$, since any $x \in K^\times$ has the form $x = ut^n$ with $u \in V^\times$ and $n \in \mathbb{Z}$.

Example **(26.13)**. — Fix totally ordered additive abelian group Γ, and a field k. Form the k-vector space R with basis the symbols X^a for $a \geq 0$ in Γ. Define $X^a X^b := X^{a+b}$, and extend this product to R by linearity. Then R is a k-algebra with $X_0 = 1$. We call R the **group algebra** of Γ. Define $v\colon (R-0) \to \Gamma$ by

$$v\Big(\sum r_a X^a\Big) := \min\{a \mid r_a \neq 0\}.$$

Then for $x, y \in (R-0)$, clearly $v(xy) = v(x) + v(y)$ because k is a domain and Γ is ordered. Hence R is a domain. Moreover, if $v(x+y) = a$, then either $v(x) \leq a$ or $v(y) \leq a$. Thus $v(x+y) \geq \min\{v(x),\, v(y)\}$.

Set $K := \mathrm{Frac}(R)$, and extend v to a map $v\colon K^\times \to \Gamma$ by $v(x/y) := v(x) - v(y)$ if $y \neq 0$. Clearly v is well defined, surjective, and a homomorphism. Further, for $x, y \in K^\times$, clearly $v(x+y) \geq \min\{v(x),\, v(y)\}$. Thus v is a valuation with group Γ.

Set $R' := \{x \in R \mid v(x) \geq 0\}$ and $\mathfrak{p} := \{x \in R \mid v(x) > 0\}$. Clearly, R' is a ring, and $\mathfrak{p}$ is a prime of R'. Further, $R'_{\mathfrak{p}}$ is the valuation ring of v.

There are many choices for Γ other than $\mathbb{Z}$. Examples include the additive rationals, the additive reals, its subgroup generated by two incommensurate reals, and the lexicographically ordered product of any two totally ordered abelian groups.

Proposition **(26.14)**. — *Let v be a valuation of a field K, and $x_1, \ldots, x_n \in K^\times$ with $n \geq 2$. Set $m := \min\{v(x_i)\}$.*

(1) *If $n = 2$ and if $v(x_1) \neq v(x_2)$, then $v(x_1 + x_2) = m$.*

(2) *If $x_1 + \cdots + x_n = 0$, then $m = v(x_i) = v(x_j)$ for some $i \neq j$.*

Proof: For (1), say $v(x_1) > v(x_2)$; so $v(x_2) = m$. Set $z := x_1/x_2$. Then $v(z) > 0$. Also $v(-z) = v(z) + v(-1) > 0$. Now,

$$0 = v(1) = v(z+1-z) \geq \min\{v(z+1),\ v(-z)\} \geq 0.$$

Hence $v(z+1) = 0$. Now, $x_1 + x_2 = (z+1)x_2$. Therefore, $v(x_1 + x_2) = v(x_2) = m$. Thus (1) holds.

For (2), reorder the x_i so $v(x_i) = m$ for $i \leq k$ and $v(x_i) > m$ for $i > k$. By induction, **(26.12.2)** yields $v(x_{k+1} + \cdots + x_n) \geq \min_{i>k}\{v(x_i)\}$. Therefore, $v(x_{k+1} + \cdots + x_n) > m$. If $k = 1$, then (1) yields $v(0) = v(x_1 + (x_2 + \cdots + x_n)) = m$, a contradiction. So $k > 1$, and $v(x_1) = v(x_2) = m$, as desired. □

Exercise **(26.15)**. — Let V be a valuation ring, such as a DVR, whose value group Γ is **Archimedean**; that is, given any nonzero $\alpha, \beta \in \Gamma$, there's $n \in \mathbb{Z}$ such that $n\alpha > \beta$. Show that V is a maximal proper subring of its fraction field K.

Exercise **(26.16)**. — Let V be a valuation ring. Show that
(1) every finitely generated ideal $\mathfrak{a}$ is principal, and
(2) V is Noetherian if and only if V is a DVR.

Lemma **(26.17)**. — *Let R be a 1-dimensional Noetherian domain, K its fraction field, M a torsion-free module, and $x \in R$ nonzero. Then $\ell(R/xR) < \infty$. Further,*

$$\ell(M/xM) \leq \dim_K(M \otimes_R K)\, \ell(R/xR), \tag{26.17.1}$$

with equality if M is finitely generated.

Proof: Set $r := \dim_K(M \otimes_R K)$. If $r = \infty$, then **(26.17.1)** is trivial; so we may assume $r < \infty$.

Set $S := R - \{0\}$. Given any module N, set $N_K := S^{-1}N$. Recall $N_K = N \otimes_R K$.

First, assume M is finitely generated. Choose any K-basis $m_1/s_1, \dots, m_r/s_r$ of M_K with $m_i \in M$ and $s_i \in S$. Then $m_1/1, \dots, m_r/1$ is also a basis. Define an R-map $\alpha\colon R^r \to M$ by sending the standard basis elements to the m_i. Then its localization α_K is an K-isomorphism. But $\operatorname{Ker}(\alpha)$ is a submodule of R^r, so torsion free. Further, $S^{-1}\operatorname{Ker}(\alpha) = \operatorname{Ker}(\alpha_K) = 0$. Hence $\operatorname{Ker}(\alpha) = 0$. Thus α is injective.

Set $N := \operatorname{Coker}(\alpha)$. Then $N_K = 0$, and N is finitely generated. Hence, $\operatorname{Supp}(N)$ is a proper closed subset of $\operatorname{Spec}(R)$. But $\dim(R) = 1$ by hypothesis. Hence, $\operatorname{Supp}(N)$ consists entirely of maximal ideals. So $\ell(N) < \infty$ by **(19.4)**.

Similarly, $\operatorname{Supp}(R/xR)$ is closed and proper in $\operatorname{Spec}(R)$. So $\ell(R/xR) < \infty$.

Consider the standard exact sequence:

$$0 \to N' \to N \to N \to N/xN \to 0 \quad \text{where} \quad N' := \operatorname{Ker}(\mu_x).$$

Apply Additivity of Length, **(19.8)**; it yields $\ell\big(N'\big) = \ell(N/xN)$.

Since M is torsion free, $\mu_x\colon M \to M$ is injective. Consider this commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & R^r & \xrightarrow{\alpha} & M & \to & N & \to & 0 \\ & & \downarrow{\scriptstyle \mu_x} & & \downarrow{\scriptstyle \mu_x} & & \downarrow{\scriptstyle \mu_x} & & \\ 0 & \to & R^r & \xrightarrow{\alpha} & M & \to & N & \to & 0 \end{array}$$

Apply the snake lemma **(5.12)**. It yields this exact sequence:

$$0 \to N' \to (R/xR)^r \to M/xM \to N/xN \to 0.$$

Hence $\ell(M/xM) = \ell\big((R/xR)^r\big)$ by additivity. But $\ell\big((R/xR)^r\big) = r\,\ell(R/xR)$ also by additivity. Thus equality holds in **(26.17.1)** when M is finitely generated.

Second, assume M is arbitrary, but **(26.17.1)** fails. Then M possesses a finitely generated submodule M' whose image H in M/xM satisfies $\ell(H) > r\ell(R/xR)$. Now, $M_K \supset M'_K$; so $r \geq \dim_K(M'_K)$. Therefore,

$$\ell(M'/xM') \geq \ell(H) > r\,\ell(R/xR) \geq \dim_K(M'_K)\,\ell\big(R/xR\big).$$

However, together these inequalities contradict the first case with M' for M. □

Theorem **(26.18)** (Krull–Akizuki). — *Let R be a 1-dimensional Noetherian domain, K its fraction field, K' a finite extension field, and R' a proper subring of K' containing R. Then R' is, like R, a 1-dimensional Noetherian domain.*

PROOF: Given a nonzero ideal $\mathfrak{a}'$ of R', take any nonzero $x \in \mathfrak{a}'$. Since K'/K is finite, there is an equation $a_n x^n + \cdots + a_0 = 0$ with $a_i \in R$ and $a_0 \neq 0$. Then $a_0 \in \mathfrak{a}' \cap R$. Further, **(26.17)** yields $\ell(R/a_0R) < \infty$.

Clearly, R' is a domain, so a torsion free R-module. Further, $R' \otimes_R K \subset K'$; hence, $\dim_K(R' \otimes_R K) < \infty$. Therefore, **(26.17)** yields $\ell_R(R'/a_0R') < \infty$.

But $\mathfrak{a}'/a_0R' \subset R'/a_0R'$. So $\ell_R(\mathfrak{a}'/a_0R') < \infty$. So $\mathfrak{a}'/a_0R'$ is finitely generated over R by **(19.2)**(3). Hence $\mathfrak{a}'$ is finitely generated over R'. Thus R' is Noetherian.

Set $R'' := R'/a_0R'$. Clearly, $\ell_{R''}R'' \leq \ell_R R''$. So $\ell_{R''}R'' < \infty$. So, in R'', every prime is maximal by **(19.4)**. So if $\mathfrak{a}'$ is prime, then $\mathfrak{a}'/a_0R'$ is maximal, whence $\mathfrak{a}'$ maximal. So in R, every nonzero prime is maximal. Thus R' is 1-dimensional. □

COROLLARY **(26.19)**. — *Let R be a 1-dimensional Noetherian domain, such as a Dedekind domain. Let K be its fraction field, K' a finite extension field, and R' the normalization of R in K'. Then R' is Dedekind.*

PROOF: Since R is 1-dimensional, it's not a field. But R' is the normalization of R. So R' is not a field by **(14.1)**. Hence, R' is Noetherian and 1-dimensional by Theorem **(26.18)**. Thus R' is Dedekind by Definition **(24.1)**. □

COROLLARY **(26.20)**. — *Let K'/K be a field extension, and V' a valuation ring of K' not containing K. Set $V := V' \cap K$. Then V is a DVR if and only if V' is.*

PROOF: It follows easily from Definition **(26.1)** that V is a valuation ring, and from Subsection **(26.12)** that its value group is a subgroup of that of V'. Now, a nonzero subgroup of $\mathbb{Z}$ is a copy of $\mathbb{Z}$. Thus V is a DVR if V' is.

Conversely, assume V is a DVR, so Noetherian and 1-dimensional. Now, V' does not contain K, so is proper in K'.- Hence, V' is Noetherian by Theorem **(26.18)**, so a DVR by Exercise **(26.16)**(2). □

Solutions

1. Rings and Ideals

EXERCISE **(1.5)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and $P := R[X_1, \dots, X_n]$ the polynomial ring. Construct an isomorphism ψ from $P/\mathfrak{a}P$ onto $(R/\mathfrak{a})[X_1, \dots, X_n]$.

SOLUTION: Let $\kappa\colon R \to R/\mathfrak{a}$ be the quotient map. Form the homomorphism $\varphi\colon P \to (R/\mathfrak{a})[X_1, \dots, X_n]$ such that $\varphi|R = \kappa$ and $\varphi(X_i) = X_i$. Then

$$\varphi\Big(\sum a_{(i_1,\dots,i_n)} X_1^{i_1} \cdots X_n^{i_n}\Big) = \sum \kappa(a_{(i_1,\dots,i_n)}) X_1^{i_1} \cdots X_n^{i_n}.$$

Since κ is surjective, so is φ. Since $\operatorname{Ker}(\kappa) = \mathfrak{a}$, it follows that

$$\operatorname{Ker}(\varphi) = \sum \mathfrak{a} X_1^{i_1} \cdots X_n^{i_n} = \mathfrak{a}P.$$

Therefore, φ induces the desired isomorphism ψ by **(1.4.1)**. □

EXERCISE **(1.8)**. — Let R be ring, and $P := R[X_1, \dots, X_n]$ the polynomial ring. Let $m \le n$ and $a_1, \dots, a_m \in R$. Set $\mathfrak{p} := \langle X_1 - a_1, \dots, X_m - a_m \rangle$. Prove that $P/\mathfrak{p} = R[X_{m+1}, \dots, X_n]$.

SOLUTION: First, assume $m = n$. Set $P' := R[X_1, \dots, X_{n-1}]$ and

$$\mathfrak{p}' := \langle X_1 - a_1, \dots, X_{n-1} - a_{n-1} \rangle \subset P'.$$

By induction on n, we may assume $P'/\mathfrak{p}' = R$. However, $P = P'[X_n]$. Hence $P/\mathfrak{p}'P = (P'/\mathfrak{p}')[X_n]$ by **(1.5)**. Thus $P/\mathfrak{p}'P = R[X_n]$.

We have $P/\mathfrak{p} = (P/\mathfrak{p}'P)/\mathfrak{p}(P/\mathfrak{p}'P)$ by **(1.7)**. But $\mathfrak{p} = \mathfrak{p}'P + \langle X_n - a_n \rangle P$. Hence $\mathfrak{p}(P/\mathfrak{p}'P) = \langle X_n - a_n \rangle (P/\mathfrak{p}'P)$. So $P/\mathfrak{p} = R[X_n]/\langle X_n - a_n \rangle$. So $P/\mathfrak{p} = R$ by **(1.6)**.

In general, $P = (R[X_1, \dots, X_m])[X_{m+1}, \dots, X_n]$. Thus $P/\mathfrak{p} = R[X_{m+1}, \dots, X_n]$ by **(1.5)**. □

EXERCISE **(1.12)** (*Chinese Remainder Theorem*). — Let R be a ring.

(1) Let $\mathfrak{a}$ and $\mathfrak{b}$ be **comaximal** ideals;that is, $\mathfrak{a} + \mathfrak{b} = R$. Prove

$$\text{(a) } \mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} \quad \text{and} \quad \text{(b) } R/\mathfrak{a}\mathfrak{b} = (R/\mathfrak{a}) \times (R/\mathfrak{b}).$$

(2) Let $\mathfrak{a}$ be comaximal to both $\mathfrak{b}$ and $\mathfrak{b}'$. Prove $\mathfrak{a}$ is also comaximal to $\mathfrak{b}\mathfrak{b}'$.

(3) Let $\mathfrak{a}$, $\mathfrak{b}$ be comaximal, and $m, n \ge 1$. Prove $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are comaximal.

(4) Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be pairwise comaximal. Prove

(a) $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ are comaximal;
(b) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$;
(c) $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\sim} \prod (R/\mathfrak{a}_i)$.

SOLUTION: To prove (1)(a), note that always $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Conversely, $\mathfrak{a} + \mathfrak{b} = R$ implies $x + y = 1$ with $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. So given $z \in \mathfrak{a} \cap \mathfrak{b}$, we have $z = xz + yz \in \mathfrak{a}\mathfrak{b}$.

To prove (1)(b), form the map $R \to R/\mathfrak{a} \times R/\mathfrak{b}$ that carries an element to its pair of residues. The kernel is $\mathfrak{a} \cap \mathfrak{b}$, which is $\mathfrak{a}\mathfrak{b}$ by (1). So we have an injection

$$\varphi\colon R/\mathfrak{a}\mathfrak{b} \hookrightarrow R/\mathfrak{a} \times R/\mathfrak{b}.$$

To show that φ is surjective, take any element $(\bar{x}, \bar{y})$ in $R/\mathfrak{a} \times R/\mathfrak{b}$. Say $\bar{x}$ and $\bar{y}$

are the residues of x and y. Since $\mathfrak{a}+\mathfrak{b}=R$, we can find $a\in\mathfrak{a}$ and $b\in\mathfrak{b}$ such that $a+b=y-x$. Then $\varphi(x+a)=(\bar{x},\bar{y})$, as desired. Thus (1) holds.

To prove (2), note that

$$R=(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{b}')=(\mathfrak{a}^2+\mathfrak{b}\mathfrak{a}+\mathfrak{a}\mathfrak{b}')+\mathfrak{b}\mathfrak{b}'\subseteq\mathfrak{a}+\mathfrak{b}\mathfrak{b}'\subseteq R.$$

To prove (3), note that (2) implies $\mathfrak{a}$ and $\mathfrak{b}^n$ are comaximal for any $n\geq 1$ by induction on n. Hence, $\mathfrak{b}^n$ and $\mathfrak{a}^m$ are comaximal for any $m\geq 1$.

To prove (4)(a), assume $\mathfrak{a}_1$ and $\mathfrak{a}_2\cdots\mathfrak{a}_{n-1}$ are comaximal by induction on n. By hypothesis, $\mathfrak{a}_1$ and $\mathfrak{a}_n$ are comaximal. Thus (2) yields (a).

To prove (4)(b) and (4)(c), again proceed by induction on n. Thus (1) yields

$$\mathfrak{a}_1\cap(\mathfrak{a}_2\cap\cdots\cap\mathfrak{a}_n)=\mathfrak{a}_1\cap(\mathfrak{a}_2\cdots\mathfrak{a}_n)=\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n;$$
$$R/(\mathfrak{a}_1\cdots\mathfrak{a}_n)\xrightarrow{\sim}R/\mathfrak{a}_1\times R/(\mathfrak{a}_2\cdots\mathfrak{a}_n)\xrightarrow{\sim}\prod(R/\mathfrak{a}_i).\qquad\square$$

Exercise **(1.13)**. — First, given a prime number p and a $k\geq 1$, find the idempotents in $\mathbb{Z}/\langle p^k\rangle$. Second, find the idempotents in $\mathbb{Z}/\langle 12\rangle$. Third, find the number of idempotents in $\mathbb{Z}/\langle n\rangle$ where $n=\prod_{i=1}^N p_i^{n_i}$ with p_i distinct prime numbers.

Solution: First, let $m\in\mathbb{Z}$ be idempotent modulo p^k. Then $m(m-1)$ is divisible by p^k. So either m or $m-1$ is divisible by p^k, as m and $m-1$ have no common prime divisor. Hence 0 and 1 are the only idempotents in $\mathbb{Z}/\langle p^k\rangle$.

Second, since $-3+4=1$, the Chinese Remainder Theorem **(1.12)** yields

$$\mathbb{Z}/\langle 12\rangle=\mathbb{Z}/\langle 3\rangle\times\mathbb{Z}/\langle 4\rangle.$$

Hence m is idempotent modulo 12 if and only if m is idempotent modulo 3 and modulo 4. By the previous case, we have the following possibilities:

$$\begin{array}{llll} m\equiv 0 \pmod 3 & \text{and} & m\equiv 0 \pmod 4;\\ m\equiv 1 \pmod 3 & \text{and} & m\equiv 1 \pmod 4;\\ m\equiv 1 \pmod 3 & \text{and} & m\equiv 0 \pmod 4;\\ m\equiv 0 \pmod 3 & \text{and} & m\equiv 1 \pmod 4. \end{array}$$

Therefore, $m\equiv 0,\ 1,\ 4,\ 9 \pmod{12}$.

Third, for each i, the two numbers $p_1^{n_1}\cdots p_{i-1}^{n_{i-1}}$ and $p_i^{n_i}$ have no common prime divisor. Hence some linear combination is equal to 1 by the Euclidean Algorithm. So the principal ideals they generate are comaximal. Hence by induction on N, the Chinese Remainder Theorem yields

$$\mathbb{Z}/\langle n\rangle=\prod_{i=1}^N\mathbb{Z}/\langle p_i^{n_i}\rangle.$$

So m is idempotent modulo n if and only if m is idempotent modulo p^{n_i} for all i; hence, if and only if m is 0 or 1 modulo p^{n_i} for all i by the first case. Thus there are 2^N idempotents in $\mathbb{Z}/\langle n\rangle$. $\square$

Exercise **(1.14)**. — Let $R:=R'\times R''$ be a **product** of rings, $\mathfrak{a}\subset R$ an ideal. Show $\mathfrak{a}=\mathfrak{a}'\times\mathfrak{a}''$ with $\mathfrak{a}'\subset R'$ and $\mathfrak{a}''\subset R''$ ideals. Show $R/\mathfrak{a}=(R'/\mathfrak{a}')\times(R''/\mathfrak{a}'')$.

SOLUTION: Set $\mathfrak{a}' := \{x' \mid (x',0) \in \mathfrak{a}\}$ and $\mathfrak{a}'' := \{x'' \mid (0,x'') \in \mathfrak{a}\}$. Clearly $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ are ideals. Clearly,

$$\mathfrak{a} \supset \mathfrak{a}' \times 0 + 0 \times \mathfrak{a}'' = \mathfrak{a}' \times \mathfrak{a}''.$$

The opposite inclusion holds, because if $\mathfrak{a} \ni (x',x'')$, then

$$\mathfrak{a} \ni (x',x'') \cdot (1,0) = (x',0) \quad \text{and} \quad \mathfrak{a} \ni (x',x'') \cdot (0,1) = (0,x'').$$

Finally, the equation $R/\mathfrak{a} = (R/\mathfrak{a}') \times (R/\mathfrak{a}'')$ is now clear from the construction of the residue class ring. □

2. Prime Ideals

EXERCISE **(2.2)**. — Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals, and $\mathfrak{p}$ a prime ideal. Prove that these conditions are equivalent: (1) $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$; and (2) $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p}$; and (3) $\mathfrak{ab} \subset \mathfrak{p}$.

SOLUTION: Trivially, (1) implies (2). If (2) holds, then (3) follows as $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Finally, assume $\mathfrak{a} \not\subset \mathfrak{p}$ and $\mathfrak{b} \not\subset \mathfrak{p}$. Then there are $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ with $x, y \notin \mathfrak{p}$. Hence, since $\mathfrak{p}$ is prime, $xy \notin \mathfrak{p}$. However, $xy \in \mathfrak{ab}$. Thus (3) implies (1). □

EXERCISE **(2.4)**. — Given a prime number p and an integer $n \geq 2$, prove that the residue ring $\mathbb{Z}/\langle p^n \rangle$ does not contain a domain.

SOLUTION: Any subring of $\mathbb{Z}/\langle p^n \rangle$ must contain 1, and 1 generates $\mathbb{Z}/\langle p^n \rangle$ as an abelian group. So $\mathbb{Z}/\langle p^n \rangle$ contains no proper subrings. However, $\mathbb{Z}/\langle p^n \rangle$ is not a domain, because in it, $p \cdot p^{n-1} = 0$ but neither p nor p^{n-1} is 0. □

EXERCISE **(2.5)**. — Let $R := R' \times R''$ be a **product** of two rings. Show that R is a domain if and only if either R' or R'' is a domain and the other is 0.

SOLUTION: Assume R is a domain. As $(1,0) \cdot (0,1) = (0,0)$, either $(1,0) = (0,0)$ or $(0,1) = (0,0)$. Correspondingly, either $R' = 0$ and $R = R''$, or $R'' = 0$ and $R = R'$. The assertion is now obvious. □

EXERCISE **(2.10)**. — Let R be a domain, and $R[X_1, \ldots, X_n]$ the polynomial ring in n variables. Let $m \leq n$, and set $\mathfrak{p} := \langle X_1, \ldots, X_m \rangle$. Prove $\mathfrak{p}$ is a prime ideal.

SOLUTION: Simply combine **(2.9)**, **(2.3)**, and **(1.8)** □

EXERCISE **(2.11)**. — Let $R := R' \times R''$ be a **product** of rings. Show every prime ideal of R has the form $\mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime.

SOLUTION: Simply combine **(1.14)**, **(2.9)**, and **(2.5)**. □

EXERCISE **(2.15)**. — Let k be a field, R a nonzero ring, $\varphi\colon k \to R$ a ring map. Prove φ is injective.

SOLUTION: By **(1.1)**, $1 \neq 0$ in R. So $\operatorname{Ker}(\varphi) \neq k$. So $\operatorname{Ker}(\varphi) = 0$ by **(2.14)**. Thus φ is injective. □

EXERCISE **(2.18)**. — Prove the following statements or give a counterexample.

(1) The complement of a multiplicative set is a prime ideal.
(2) Given two prime ideals, their intersection is prime.
(3) Given two prime ideals, their sum is prime.
(4) Given a ring map $\varphi\colon R \to R'$, the operation φ^{-1} carries maximal ideals of R' to maximal ideals of R.

(5) In **(1.7)**, κ^{-1} takes maximal ideals of $R/\mathfrak{a}$ to maximal ideals of R.

SOLUTION: (1) False. In the ring $\mathbb{Z}$, consider the set S of powers of 2. The complement T of S contains 3 and 5, but not 8; so T is not an ideal.

(2) False. In the ring $\mathbb{Z}$, consider the prime ideals $\langle 2\rangle$ and $\langle 3\rangle$; their intersection $\langle 2\rangle \cap \langle 3\rangle$ is equal to $\langle 6\rangle$, which is not prime.

(3) False. Since $2 \cdot 3 - 5 = 1$, we have $\langle 3\rangle + \langle 5\rangle = \mathbb{Z}$.

(4) False. Let $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. Then $\varphi^{-1}\langle 0\rangle = \langle 0\rangle$.

(5) True. The assertion is immediate from **(1.7)**. □

EXERCISE **(2.21)**. — Prove that, in a PID, elements x and y are **relatively prime** (share no prime factor) if and only if the ideals $\langle x\rangle$ and $\langle y\rangle$ are comaximal.

SOLUTION: Say $\langle x\rangle + \langle y\rangle = \langle d\rangle$. Then $d = \gcd(x, y)$, as is easy to check. The assertion is now obvious. □

EXERCISE **(2.24)**. — Preserve the setup of **(2.23)**. Let $f := a_0X^n + \cdots + a_n$ be a polynomial of positive degree n. Assume that R has infinitely many prime elements p, or simply that there is a p such that $p \nmid a_0$. Show that $\langle f\rangle$ is not maximal.

SOLUTION: Set $\mathfrak{a} := \langle p, f\rangle$. Then $\mathfrak{a} \supsetneqq \langle f\rangle$, because p is not a multiple of f. Set $k := R/\langle p\rangle$. Since p is irreducible, k is a domain by **(2.6)** and **(2.8)**. Let $f' \in k[X]$ denote the image of f. By hypothesis, $\deg(f') = n \geq 1$. Hence f' is not a unit by **(2.3)** since k is a domain. Therefore, $\langle f'\rangle$ is proper. But $P/\mathfrak{a} \xrightarrow{\sim} k[X]/\langle f'\rangle$ by **(1.5)** and **(1.7)**. So $\mathfrak{a}$ is proper. Thus $\langle f\rangle$ is not maximal. □

3. Radicals

EXERCISE **(3.6)**. — Let A be a ring, $\mathfrak{m}$ a maximal ideal such that $1 + m$ is a unit for every $m \in \mathfrak{m}$. Prove A is local. Is this assertion still true if $\mathfrak{m}$ is not maximal?

SOLUTION: Take $y \in A$. Let's prove that, if $y \notin \mathfrak{m}$, then y is a unit. Since $\mathfrak{m}$ is maximal, $\langle y\rangle + \mathfrak{m} = A$. Hence there exist $x \in R$ and $m \in \mathfrak{m}$ such that $xy + m = 1$, or in other words, $xy = 1 - m$. So xy is a unit by hypothesis; whence, y is a unit. Thus A is local by **(3.4)**.

The assertion is not true if $\mathfrak{m}$ is not maximal. Indeed, take any ring that is not local, for example $\mathbb{Z}$, and take $\mathfrak{m} := \langle 0\rangle$. □

EXERCISE **(3.10)**. — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{p}$ an ideal of R. Prove

(1) there is an ideal $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ if and only if $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$;

(2) if $\mathfrak{p}$ is prime with $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$, then there's a prime $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

SOLUTION: In (1), given $\mathfrak{q}$, note $\varphi(\mathfrak{p}) \subset \mathfrak{q}$, as always $\varphi(\varphi^{-1}(\mathfrak{q})) \subset \mathfrak{q}$. So $\mathfrak{p}R' \subset \mathfrak{q}$. Hence $\varphi^{-1}(\mathfrak{p}R') \subset \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. But, always $\mathfrak{p} \subset \varphi^{-1}(\mathfrak{p}R')$. Thus $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$. The converse is trivial: take $\mathfrak{q} := \mathfrak{p}R'$.

In (2), set $S := \varphi(R - \mathfrak{p})$. Then $S \cap \mathfrak{p}R' = \emptyset$, as $\varphi(x) \in \mathfrak{p}R'$ implies $x \in \varphi^{-1}(\mathfrak{p}R')$ and $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$. So there's a prime $\mathfrak{q}$ of R' containing $\mathfrak{p}R'$ and disjoint from S by **(3.9)**. So $\varphi^{-1}(\mathfrak{q}) \supset \varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$ and $\varphi^{-1}(\mathfrak{q}) \cap (R - \mathfrak{p}) = \emptyset$. Thus $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

EXERCISE **(3.11)**. — Use Zorn's lemma to prove that any prime ideal $\mathfrak{p}$ contains a minimal prime ideal.

Solution: Let $\mathcal{S}$ be the set of all prime ideals contained in $\mathfrak{p}$. Then $\mathfrak{p} \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$. Order $\mathcal{S}$ by reverse inclusion. To apply Zorn's Lemma, we must show that, for any decreasing chain $\{\mathfrak{p}_\lambda\}$ of prime ideals, the intersection $\mathfrak{p}_0 := \bigcap \mathfrak{p}_\lambda$ is a prime ideal. So take $x, y \notin \mathfrak{p}_0$. Then there exists λ such that $x, y \notin \mathfrak{p}_\lambda$. Since $\mathfrak{p}_\lambda$ is prime, $xy \notin \mathfrak{p}_\lambda$. Hence $xy \notin \mathfrak{p}_0$. Thus $\mathfrak{p}_0$ is prime. □

Exercise **(3.14)**. — Find the nilpotents in $\mathbb{Z}/\langle n\rangle$. In particular, take $n = 12$.

Solution: An integer m is nilpotent modulo n if and only if some power m^k is divisible by n. The latter holds if and only if every prime factor of n occurs in m. In particular, in $\mathbb{Z}/\langle 12\rangle$, the nilpotents are 0 and 6. □

Exercise **(3.15)**. — Let $\varphi\colon R \to R'$ be a ring map, $\mathfrak{b} \subset R'$ a subset. Prove

$$\varphi^{-1}\sqrt{\mathfrak{b}} = \sqrt{\varphi^{-1}\mathfrak{b}}.$$

Solution: Below, (1) is clearly equivalent to (2); and (2), to (3); and so forth:

(1) $x \in \varphi^{-1}\sqrt{\mathfrak{b}}$;
(2) $\varphi x \in \sqrt{\mathfrak{b}}$;
(3) $(\varphi x)^n \in \mathfrak{b}$ for some n;
(4) $\varphi(x^n) \in \mathfrak{b}$ for some n;
(5) $x^n \in \varphi^{-1}\mathfrak{b}$ for some n;
(6) $x \in \sqrt{\varphi^{-1}\mathfrak{b}}$. □

Exercise **(3.16)**. — Let R be a ring, $\mathfrak{a} \subset \sqrt{\langle 0\rangle}$ an ideal, and $P := R[Y]$ the polynomial ring in one variable. Let $u \in R$ be a unit, and $x \in R$ a nilpotent.

(1) Prove (a) that $u + x$ is a unit in R and (b) that $u + xY$ is a unit in P.
(2) Suppose $w \in R$ maps to a unit of $R/\mathfrak{a}$. Prove that w is a unit in R.

Solution: In (1), say $x^n = 0$. Set $y := -xu^{-1}$. Then (a) holds as

$$(u + x) \cdot u^{-1}(1 + y + y^2 + \cdots + y^{n-1}) = 1.$$

Now, u is also a unit in P, and $(xY)^n = 0$; hence, (a) implies (b).

In (2), say $wy \in R$ maps to $1 \in R/\mathfrak{a}$. Set $z := wy - 1$. Then $z \in \mathfrak{a}$, so z is nilpotent. Hence, $1+z$ is a unit by (1)(a). So wy is a unit. Then $w \cdot y(wy)^{-1} = 1$. □

Exercise **(3.19)**. — Let R be a ring, and $\mathfrak{a}$ an ideal. Assume $\sqrt{\mathfrak{a}}$ is finitely generated. Show there is an $n \geq 1$ such that $\left(\sqrt{\mathfrak{a}}\right)^n \subset \mathfrak{a}$.

Solution: Let $x_1, \ldots, x_m$ be generators of $\sqrt{\mathfrak{a}}$. For each i, there is n_i such that $x_i^{n_i} \in \mathfrak{a}$. Set $n := 1 + \sum(n_i - 1)$. Given $a \in \sqrt{\mathfrak{a}}$, write $a = \sum_{i=1}^m y_i x_i$ with $y_i \in R$. Then a^n is a linear combination of terms of the form $x_1^{j_1} \cdots x_m^{j_m}$ with $\sum_{i=1}^m j_i = n$. Hence $j_i \geq n$ for some i, because if $j_i \leq n_i - 1$ for all i, then $\sum j_i \leq \sum(n_i - 1)$. Thus $a^n \in \mathfrak{a}$, as desired. □

Exercise **(3.20)**. — Let R be a ring, $\mathfrak{q}$ an ideal, $\mathfrak{p}$ a finitely generated prime. Prove that $\mathfrak{p} = \sqrt{\mathfrak{q}}$ if and only if there is $n \geq 1$ such that $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$.

Solution: If $\mathfrak{p} = \sqrt{\mathfrak{q}}$, then $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$ by **(3.19)**. Conversely, if $\mathfrak{q} \supset \mathfrak{p}^n$, then clearly $\sqrt{\mathfrak{q}} \supset \mathfrak{p}$. Further, since $\mathfrak{p}$ is prime, if $\mathfrak{p} \supset \mathfrak{q}$, then $\mathfrak{p} \supset \sqrt{\mathfrak{q}}$. □

Exercise **(3.22)**. — Let R be a ring. Assume R is reduced and has finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Prove that $\varphi\colon R \to \prod(R/\mathfrak{p}_i)$ is injective, and for each i, there is some $(x_1, \ldots, x_n) \in \mathrm{Im}(\varphi)$ with $x_i \neq 0$ but $x_j = 0$ for $j \neq i$.

SOLUTION: Clearly $\operatorname{Ker}(\varphi) = \bigcap \mathfrak{p}_i$. Now, R is reduced and the $\mathfrak{p}_i$ are its minimal primes; hence, **(3.17)** and **(3.11)** yield

$$\langle 0 \rangle = \sqrt{\langle 0 \rangle} = \bigcap \mathfrak{p}_i.$$

Thus $\operatorname{Ker}(\varphi) = \langle 0 \rangle$, and so φ is injective.

Finally, fix i. Since $\mathfrak{p}_i$ is minimal, $\mathfrak{p}_i \not\supset \mathfrak{p}_j$ for $j \neq i$; say $a_j \in \mathfrak{p}_j - \mathfrak{p}_i$. Set $a := \prod_{j \neq i} a_j$. Then $a \in \mathfrak{p}_j - \mathfrak{p}_i$ for all $j \neq i$. Thus $\operatorname{Im}(\varphi)$ meets $R/\mathfrak{p}_i$. □

4. Modules

EXERCISE **(4.3)**. — Let R be a ring, M a module. Consider the set map

$$\theta\colon \operatorname{Hom}(R, M) \to M \quad \text{defined by} \quad \theta(\rho) := \rho(1).$$

Show that θ is an isomorphism, and describe its inverse.

SOLUTION: First off, θ is R-linear, because

$$\theta(x\rho + x'\rho') = (x\rho + x'\rho')(1) = x\rho(1) + x'\rho'(1) = x\theta(\rho) + x'\theta(\rho').$$

Set $H := \operatorname{Hom}(R, M)$. Define $\eta\colon M \to H$ by $\eta(m)(x) := xm$. It is easy to check that $\eta\theta = 1_H$ and $\theta\eta = 1_M$. Thus θ and η are inverse isomorphisms by **(4.2)**. □

EXERCISE **(4.12)**. — Let R be a domain, and $x \in R$ nonzero. Let M be the submodule of $\operatorname{Frac}(R)$ generated by 1, x^{-1}, $x^{-2}, \dots$. Suppose that M is finitely generated. Prove that $x^{-1} \in R$, and conclude that $M = R$.

SOLUTION: Suppose M is generated by $m_1, \dots, m_k$. Say $m_i = \sum_{j=0}^{n_i} a_{ij} x^{-j}$ for some n_i and $a_{ij} \in R$. Set $n := \max\{n_i\}$. Then 1, $x^{-1}, \dots, x^{-n}$ generate M. So

$$x^{-(n+1)} = a_n x^{-n} + \cdots + a_1 x^{-1} + a_0$$

for some $a_i \in R$. Thus

$$x^{-1} = a_n + \cdots + a_1 x^{n-1} + a_0 x^n \in R.$$

Finally, as $x^{-1} \in R$ and R is a ring, also 1, x^{-1}, $x^{-2}, \dots \in R$; so $M \subset R$. Conversely, $M \supset R$ as $1 \in M$. Thus $M = R$. □

EXERCISE **(4.14)**. — Let Λ be an infinite set, R_λ a ring for $\lambda \in \Lambda$. Endow $\prod R_\lambda$ and $\bigoplus R_\lambda$ with componentwise addition and multiplication. Show that $\prod R_\lambda$ has a multiplicative identity (so is a ring), but that $\bigoplus R_\lambda$ does not (so is not a ring).

SOLUTION: Consider the vector (1) whose every component is 1. Obviously, (1) is a multiplicative identity of $\prod R_\lambda$. On the other hand, no restricted vector (e_λ) can be a multiplicative identity in $\bigoplus R_\lambda$; indeed, because Λ is infinite, e_μ must be zero for some μ. So $(e_\lambda) \cdot (x_\lambda) \neq (x_\lambda)$ if $x_\mu \neq 0$. □

EXERCISE **(4.15)**. — Let R be a ring, L, M, and N modules. Consider a diagram

$$L \underset{\rho}{\overset{\alpha}{\rightleftarrows}} M \underset{\sigma}{\overset{\beta}{\rightleftarrows}} N$$

where α, β, ρ, and σ are homomorphisms. Prove that

$$M = L \oplus N \quad \text{and} \quad \alpha = \iota_L,\ \beta = \pi_N,\ \sigma = \iota_N,\ \rho = \pi_L$$

if and only if the following relations hold:

$$\beta\alpha = 0,\ \beta\sigma = 1,\ \rho\sigma = 0,\ \rho\alpha = 1,\ \text{and } \alpha\rho + \sigma\beta = 1.$$

Solution: If $M = L \oplus N$ and $\alpha = \iota_L$, $\beta = \pi_N$, $\sigma = \iota_N$, $\rho = \pi_L$, then the definitions immediately yield $\alpha\rho + \sigma\beta = 1$ and $\beta\alpha = 0$, $\beta\sigma = 1$, $\rho\sigma = 0$, $\rho\alpha = 1$.

Conversely, assume $\alpha\rho + \sigma\beta = 1$ and $\beta\alpha = 0$, $\beta\sigma = 1$, $\rho\sigma = 0$, $\rho\alpha = 1$. Consider the maps $\varphi\colon M \to L \oplus N$ and $\theta\colon L \oplus N \to M$ given by $\varphi m := (\rho m, \beta m)$ and $\theta(l, n) := \alpha l + \sigma n$. They are inverse isomorphisms, because

$$\varphi\theta(l, n) = (\rho\alpha l + \rho\sigma n,\ \beta\alpha l + \beta\sigma n) = (l, n) \quad \text{and} \quad \theta\varphi m = \alpha\rho m + \sigma\beta m = m.$$

Lastly, $\beta = \pi_N\varphi$ and $\rho = \pi_L\varphi$ by definition of φ, and $\alpha = \theta\iota_L$ and $\sigma = \theta\iota_N$ by definition of θ. □

Exercise **(4.16)**. — Let R be a ring, N a module, Λ a set, M_λ a module for $\lambda \in \Lambda$. Show that the injections $\iota_\kappa\colon M_\kappa \to \bigoplus M_\lambda$ induce an injection

$$\bigoplus \operatorname{Hom}(N,\, M_\lambda) \hookrightarrow \operatorname{Hom}(N,\, \bigoplus M_\lambda),$$

and that it is an isomorphism if N is finitely generated.

Solution: For $\lambda \in \Lambda$, let $\alpha_\lambda\colon N \to M_\lambda$ be maps, almost all 0. Then

$$\big(\textstyle\sum \iota_\lambda\alpha_\lambda\big)(n) = \big(\alpha_\lambda(n)\big) \in \bigoplus M_\lambda.$$

So if $\sum \iota_\lambda\alpha_\lambda = 0$, then $\alpha_\lambda = 0$ for all λ. Thus the ι_κ induce an injection.

Assume N is finitely generated, say by $n_1, \dots, n_k$. Let $\alpha\colon N \to \bigoplus M_\lambda$ be a map. Then each $\alpha(n_i)$ lies in a finite direct subsum of $\bigoplus M_\lambda$. So $\alpha(N)$ lies in one too. Set $\alpha_\kappa := \pi_\kappa\alpha$ for all $\kappa \in \Lambda$. Then almost all α_κ vanish. So (α_κ) lies in $\bigoplus \operatorname{Hom}(N, M_\lambda)$, and $\sum \iota_\kappa\alpha_\kappa = \alpha$. Thus the ι_κ induce a surjection, so an isomorphism. □

Exercise **(4.17)**. — Let R be a ring, $\mathfrak{a}$ an ideal, Λ a set, M_λ a module for $\lambda \in \Lambda$. Show $\mathfrak{a}\big(\bigoplus M_\lambda\big) = \bigoplus \mathfrak{a}M_\lambda$. Show $\mathfrak{a}(\prod M_\lambda) = \prod \mathfrak{a}M_\lambda$ if $\mathfrak{a}$ is finitely generated.

Solution: First, $\mathfrak{a}\big(\bigoplus M_\lambda\big) \subset \bigoplus \mathfrak{a}M_\lambda$ because $a \cdot (m_\lambda) = (am_\lambda)$. Conversely, $\mathfrak{a}\big(\bigoplus M_\lambda\big) \supset \bigoplus \mathfrak{a}M_\lambda$ because $(a_\lambda m_\lambda) = \sum a_\lambda\iota_\lambda m_\lambda$ since the sum is finite.

Second, $\mathfrak{a}\big(\prod M_\lambda\big) \subset \prod \mathfrak{a}M_\lambda$ as $a(m_\lambda) = (am_\lambda)$. Conversely, say $\mathfrak{a}$ is generated by $f_1, \dots, f_n$. Then $\mathfrak{a}\big(\prod M_\lambda\big) \supset \prod \mathfrak{a}M_\lambda$. Indeed, take $(m'_\lambda) \in \prod \mathfrak{a}M_\lambda$. Then for each λ, there is n_λ such that $m'_\lambda = \sum_{j=1}^{n_\lambda} a_{\lambda j}m_{\lambda j}$ with $a_{\lambda j} \in \mathfrak{a}$ and $m_{\lambda j} \in M_\lambda$. Write $a_{\lambda j} = \sum_{i=1}^{n} x_{\lambda ji}f_i$ with $x_{\lambda ji} \in R$. Then

$$(m'_\lambda) = \Big(\sum_{j=1}^{n_\lambda}\sum_{i=1}^{n} f_i x_{\lambda ji} m_{\lambda j}\Big) = \sum_{i=1}^{n} f_i\Big(\sum_{j=1}^{n_\lambda} x_{\lambda ji} m_{\lambda j}\Big) \in \mathfrak{a}\Big(\prod M_\lambda\Big). \qquad \square$$

5. Exact Sequences

Exercise **(5.5)**. — Let M' and M'' be modules, $N \subset M'$ a submodule. Set $M := M' \oplus M''$. Using **(5.3)**(1) and **(5.4)** and **(5.2)**, prove $M/N = M'/N \oplus M''$.

Solution: By **(5.3)**(1) and **(5.4)**, the two sequences $0 \to M'' \to M'' \to 0$ and $0 \to N \to M' \to M'/N \to 0$ are exact. So by **(5.2)**, the sequence

$$0 \to N \to M' \oplus M'' \to (M'/N) \oplus M'' \to 0$$

is exact. Thus **(5.4)** yields the assertion. □

EXERCISE **(5.6)**. — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Prove that, if M' and M'' are finitely generated, then so is M.

SOLUTION: Let $m''_1, \dots, m''_n \in M$ map to elements generating M''. Let $m \in M$, and write its image in M'' as a linear combination of the images of the m''_i. Let $m'' \in M$ be the same combination of the m''_i. Set $m' := m - m''$. Then m' maps to 0 in M''; so m' is the image of an element of M'.

Let $m'_1, \dots, m'_l \in M$ be the images of elements generating M'. Then m' is a linear combination of the m'_j. So m is a linear combination of the m''_i and m'_j. Thus the m'_i and m''_j together generate M. □

EXERCISE **(5.10)**. — Let M', M'' be modules, and set $M := M' \oplus M''$. Let N be a submodule of M containing M', and set $N'' := N \cap M''$. Prove $N = M' \oplus N''$.

SOLUTION: Form the sequence $0 \to M' \to N \to \pi_{M''}N \to 0$. It splits by **(5.9)** as $(\pi_{M'}|N) \circ \iota_{M'} = 1_{M'}$. Finally, if $(m', m'') \in N$, then $(0, m'') \in N$ as $M' \subset N$; hence, $\pi_{M''}N = N''$. □

EXERCISE **(5.11)**. — Criticize the following misstatement of **(5.9)**: given a short exact sequence $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$, there is an isomorphism $M \simeq M' \oplus M''$ if and only if there is a section $\sigma\colon M'' \to M$ of β.

SOLUTION: We have $\alpha\colon M' \to M$, and $\iota_{M'}\colon M' \to M' \oplus M''$, but **(5.9)** requires that they be compatible with the isomorphism $M \simeq M' \oplus M''$, and similarly for $\beta\colon M \to M''$ and $\pi_{M''}\colon M' \oplus M'' \to M''$.

Let's construct a counterexample (due to B. Noohi). For each integer $n \geq 2$, let M_n be the direct sum of countably many copies of $\mathbb{Z}/\langle n\rangle$. Set $M := \bigoplus M_n$.

First, let us check these two statements:

(1) For any finite abelian group G, we have $G \oplus M \simeq M$.
(2) For any finite subgroup $G \subset M$, we have $M/G \simeq M$.

Statement (1) holds since G is isomorphic to a direct sum of copies of $\mathbb{Z}/\langle n\rangle$ for various n by the structure theorem for finite abelian groups [1, (6.4), p. 472], [4, Thm. 13.3, p. 200].

To prove (2), write $M = B \bigoplus M'$, where B contains G and involves only finitely many components of M. Then $M' \simeq M$. Therefore, **(5.10)** and (1) yield

$$M/G \simeq (B/G) \oplus M' \simeq M.$$

To construct the counterexample, let p be a prime number. Take one of the $\mathbb{Z}/\langle p^2\rangle$ components of M, and let $M' \subset \mathbb{Z}/\langle p^2\rangle$ be the cyclic subgroup of order p. There is no retraction $\mathbb{Z}/\langle p^2\rangle \to M'$, so there is no retraction $M \to M'$ either, since the latter would induce the former. Finally, take $M'' := M/M'$. Then (1) and (2) yield $M \simeq M' \oplus M''$. □

EXERCISE **(5.13)**. — Referring to **(4.8)**, give an alternative proof that β is an isomorphism by applying the Snake Lemma to the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & N/M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \beta} & & \\
0 & \to & M/L & \to & N/L & \xrightarrow{\lambda} & (N/L)\big/(M/L) & \to & 0
\end{array}$$

SOLUTION: The Snake Lemma yields an exact sequence,

$$L \xrightarrow{1} L \to \operatorname{Ker}(\beta) \to 0;$$

hence, $\operatorname{Ker}(\beta) = 0$. Moreover, β is surjective because κ and λ are. □

EXERCISE **(5.14)** (*Five Lemma*). — Consider this commutative diagram:

$$\begin{array}{ccccccccc} M_4 & \xrightarrow{\alpha_4} & M_3 & \xrightarrow{\alpha_3} & M_2 & \xrightarrow{\alpha_2} & M_1 & \xrightarrow{\alpha_1} & M_0 \\ \downarrow{\scriptstyle \gamma_4} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_0} \\ N_4 & \xrightarrow{\beta_4} & N_3 & \xrightarrow{\beta_3} & N_2 & \xrightarrow{\beta_2} & N_1 & \xrightarrow{\beta_1} & N_0 \end{array}$$

Assume it has exact rows. Via a chase, prove these two statements:

(1) If γ_3 and γ_1 are surjective and if γ_0 is injective, then γ_2 is surjective.
(2) If γ_3 and γ_1 are injective and if γ_4 is surjective, then γ_2 is injective.

SOLUTION: Let's prove (1). Take $n_2 \in N_2$. Since γ_1 is surjective, there is $m_1 \in M_1$ such that $\gamma_1(m_1) = \beta_2(n_2)$. Then $\gamma_0\alpha_1(m_1) = \beta_1\gamma_1(m_1) = \beta_1\beta_2(n_2) = 0$ by commutativity and exactness. Since γ_0 is injective, $\alpha_1(m_1) = 0$. Hence exactness yields $m_2 \in M_2$ with $\alpha_2(m_2) = m_1$. So $\beta_2(\gamma_2(m_2) - n_2) = \gamma_1\alpha_2(m_2) - \beta_2(n_2) = 0$.

Hence exactness yields $n_3 \in N_3$ with $\beta_3(n_3) = \gamma_2(m_2) - n_2$. Since γ_3 is surjective, there is $m_3 \in M_3$ with $\gamma_3(m_3) = n_3$. Then $\gamma_2\alpha_3(m_3) = \beta_3\gamma_3(m_3) = \gamma_2(m_2) - n_2$. Hence $\gamma_2(m_2 - \alpha_3(m_3)) = n_2$. Thus γ_2 is surjective.

The proof of (2) is similar. □

EXERCISE **(5.15)** (*Nine Lemma*). — Consider this commutative diagram:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & L' & \to & L & \to & L'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M' & \to & M & \to & M'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & N' & \to & N & \to & N'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Assume all the columns are exact and the middle row is exact. Prove that the first row is exact if and only if the third is.

SOLUTION: The first row is exact if the third is owing to the Snake Lemma **(5.12)** applied to the bottom two rows. The converse is proved similarly. □

EXERCISE **(5.16)**. — Consider this commutative diagram with exact rows:

$$\begin{array}{ccccc} M' & \xrightarrow{\beta} & M & \xrightarrow{\gamma} & M'' \\ \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} \\ N' & \xrightarrow{\beta'} & N & \xrightarrow{\gamma'} & N'' \end{array}$$

Assume α' and γ are surjective. Given $n \in N$ and $m'' \in M''$ with $\alpha''(m'') = \gamma'(n)$, show that there is $m \in M$ such that $\alpha(m) = n$ and $\gamma(m) = m''$.

SOLUTION: Since γ is surjective, there is $m_1 \in M$ with $\gamma(m_1) = m''$. Then $\gamma'\big(n-\alpha(m_1)\big) = 0$ as $\alpha''(m'') = \gamma'(n)$ and as the right-hand square is commutative. So by exactness of the bottom row, there is $n' \in N'$ with $\beta'(n') = n-\alpha(m_1)$. Since α' is surjective, there is $m' \in M'$ with $\alpha'(m') = n'$. Set $m := m_1 + \beta(m')$. Then $\gamma(m) = m''$ as $\gamma\beta = 0$. Further, $\alpha(m) = \alpha(m_1)+\beta'(n') = n$ as the left-hand square is commutative. Thus m works. □

EXERCISE **(5.21)**. — Show that a free module $R^{\oplus\Lambda}$ is projective.

SOLUTION: Given $\beta\colon M \twoheadrightarrow N$ and $\alpha\colon R^{\oplus\Lambda} \to N$, use the UMP of **(4.10)** to define $\gamma\colon R^{\oplus\Lambda} \to M$ by sending the standard basis vector e_λ to any **lift** of $\alpha(e_\lambda)$, that is, any $m_\lambda \in M$ with $\beta(m_\lambda) = \alpha(e_\lambda)$. (The Axiom of Choice permits a simultaneous choice of all m_λ if Λ is infinite.) Clearly $\alpha = \beta\gamma$. Thus $R^{\oplus\Lambda}$ is projective. □

EXERCISE **(5.25)**. — Let R be a ring, $X_1, X_2, \dots$ infinitely many variables. Set $P := R[X_1, X_2, \dots]$ and $M := P/\langle X_1, X_2, \dots\rangle$. Is M finitely generated? Finitely presented? Explain.

SOLUTION: Yes, M is finitely generated, namely by the image of 1. No, M is not finitely presented; otherwise, by **(5.24)**, the ideal $\langle X_1, X_2, \dots\rangle$ would be finitely generated, say by $f_1, \dots, f_n$, whence also by $X_1, \dots, X_m$ for some m. □

EXERCISE **(5.26)**. — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Assume M' and M'' are finitely presented. Show that M is too.

SOLUTION: Let $0 \to K' \to F' \xrightarrow{\alpha'} M' \to 0$ and $0 \to K_1'' \to F'' \xrightarrow{\alpha''} M'' \to 0$ be exact sequences with F' and F'' free of finite rank and with K' and K'' finitely generated. Set $F := F' \oplus F''$. Define $\beta'\colon F' \to M$ to be α' followed by the inclusion $M' \hookrightarrow M$. Now, F'' is projective by **(5.21)**; so we may lift α'' to $\beta''\colon F'' \to M$. Set $\alpha := \beta' + \beta''$. Then the following diagram of exact sequences is commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F' & \longrightarrow & F & \longrightarrow & F'' & \longrightarrow & 0 \\ & & {\scriptstyle\alpha'}\big\downarrow & & {\scriptstyle\alpha}\big\downarrow & & {\scriptstyle\alpha''}\big\downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

The map α is surjective and the sequence of kernels $0 \to K' \to K \to K'' \to 0$ is exact by the Snake Lemma **(5.12)**. Moreover, K' and K'' are finitely generated by hypothesis. So K is finitely generated by **(5.6)**. Thus M is finitely presented. □

6. Direct Limits

EXERCISE **(6.3)**. — (1) Show that the condition **(6.2)**(1) is equivalent to the commutativity of the corresponding diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\ \big\downarrow & & \big\downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(C)\big) \end{array}$$

(2) Given $\gamma\colon C \to D$, show **(6.2)**(1) yields the commutativity of this diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,D) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(D)\big) \end{array}$$

SOLUTION: The left-hand vertical map is given by composition with α, and the right-hand vertical map is given by composition with $F(\alpha)$. So the composition of the top map and the right-hand map sends β to $F(\beta)F(\alpha)$, whereas the composition of the left-hand map with the bottom map sends β to $F(\beta\alpha)$. These two images are always equal if and only if the diagram commutes. Thus (1) holds if and only if the diagram commutes.

As to (2), the argument is similar. □

EXERCISE **(6.5)**. — Let $\mathcal{C}$ and $\mathcal{C}'$ be categories, $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ an adjoint pair. Let $\varphi_{A,A'}\colon \mathrm{Hom}_{\mathcal{C}'}(FA,\, A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(A,\, F'A')$ denote the natural bijection, and set $\eta_A := \varphi_{A,FA}(1_{FA})$. Do the following:

(1) Prove η_A is natural in A; that is, given $g\colon A \to B$, the induced square

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & F'FA \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle F'Fg} \\ B & \xrightarrow{\eta_B} & F'FB \end{array}$$

is commutative. We call the natural transformation $A \mapsto \eta_A$ the **unit** of $(F,\, F')$.

(2) Given $f'\colon FA \to A'$, prove $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

(3) Prove the natural map $\eta_A\colon A \to F'FA$ is **universal** from A to F'; that is, given $f\colon A \to F'A'$, there is a unique map $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$.

(4) Conversely, instead of assuming $(F,\, F')$ is an adjoint pair, assume given a natural transformation $\eta\colon 1_{\mathcal{C}} \to F'F$ satisfying (1) and (3). Prove the equation in (2) defines a natural bijection making $(F,\, F')$ an adjoint pair, whose unit is η.

(5) Identify the units in the two examples in **(6.4)**: the "free module" functor and the "polynomial ring" functor.

(Dually, we can define a **counit** $\varepsilon\colon FF' \to 1_{\mathcal{C}'}$, and prove similar statements.)

SOLUTION: For (1), form this canonical diagram, with horizontal induced maps:

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathcal{C}'}(FA,\, FA) & \xrightarrow{(Fg)_*} & \mathrm{Hom}_{\mathcal{C}'}(FA,\, FB) & \xleftarrow{(Fg)^*} & \mathrm{Hom}_{\mathcal{C}'}(FB,\, FB) \\ {\scriptstyle \varphi_{A,\,FA}}\downarrow & & {\scriptstyle \varphi_{A,\,FB}}\downarrow & & {\scriptstyle \varphi_{B,\,FB}}\downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,\, F'FA) & \xrightarrow{(F'Fg)_*} & \mathrm{Hom}_{\mathcal{C}}(A,\, F'FB) & \xleftarrow{g^*} & \mathrm{Hom}_{\mathcal{C}}(B,\, F'FB) \end{array}$$

It commutes since φ is natural. Follow 1_{FA} out of the upper left corner to find $F'Fg \circ \eta_A = \varphi_{A,\,FB}(g)$ in $\mathrm{Hom}_{\mathcal{C}}(A,\, F'FB)$. Follow 1_{FB} out of the upper right corner to find $\varphi_{A,\,FB}(g) = \eta_B \circ g$ in $\mathrm{Hom}_{\mathcal{C}}(A,\, F'FB)$. Thus $(F'Fg) \circ \eta_A = \eta_B \circ g$.

For (2), form this canonical commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}'}(FA,\, FA) & \xrightarrow{f'_*} & \mathrm{Hom}_{\mathcal{C}'}(FA, A') \\ {\scriptstyle \varphi_{A,\,FA}}\downarrow & & {\scriptstyle \varphi_{A,A'}}\downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,\, F'FA) & \xrightarrow{(F'f')_*} & \mathrm{Hom}_{\mathcal{C}}(A,\, F'A') \end{array}$$

Follow 1_{FA} out of the upper left-hand corner to find $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

For (3), given an f', note that (2) yields $\varphi_{A,A'}(f') = f$; whence, $f' = \varphi^{-1}_{A,A'}(f)$. Thus f' is unique. Further, an f' exists: just set $f' := \varphi^{-1}_{A,A'}(f)$.

For (4), set $\psi_{A,A'}(f') := F'f' \circ \eta_A$. As η_A is universal, given $f\colon A \to F'A'$, there is a unique $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$. Thus $\psi_{A,A'}$ is a bijection:

$$\psi_{A,A'}\colon \operatorname{Hom}_{\mathcal{C}'}(FA, A') \xrightarrow{\sim} \operatorname{Hom}_{\mathcal{C}}(A,\, F'A').$$

Also, $\psi_{A,A'}$ is natural in A, as η_A is natural in A and F' is a functor. And, $\psi_{A,A'}$ is natural in A', as F' is a functor. Clearly, $\psi_{A,\,FA}(1_{FA}) = \eta_A$. Thus (4) holds.

For (5), use the notation of **(6.4)**. Clearly, if F is the "free module" functor, then $\eta_\Lambda\colon \Lambda \to R^{\oplus\Lambda}$ carries an element of Λ to the corresponding standard basis vector. Further, if F is the "polynomial ring" functor and if A is the set of variables $X_1, \dots, X_n$, then $\eta_A(X_i)$ is just X_i viewed in $R[X_1, \dots, X_n]$. □

Exercise **(6.9)**. — Let $\alpha\colon L \to M$ and $\beta\colon L \to N$ be two maps. Their **pushout** is defined as the universal example of an object P equipped with a pair of maps $\gamma\colon M \to P$ and $\delta\colon N \to P$ such that $\gamma\alpha = \delta\beta$. In terms of the definitions, express the pushout as a direct limit. Show directly that, in ((Sets)), the pushout is the disjoint union $M \sqcup N$ modulo the smallest equivalence relation $\sim$ with $m \sim n$ if there is $\ell \in L$ with $\alpha(\ell) = m$ and $\beta(\ell) = n$. Show directly that, in ((R-mod)), the pushout is the direct sum $M \oplus N$ modulo the image of L under the map $(\alpha, -\beta)$.

Solution: Let Λ be the category with three objects λ, μ, and ν and two non-identity maps $\lambda \to \mu$ and $\lambda \to \nu$. Define a functor $\lambda \mapsto M_\lambda$ by $M_\lambda := L$, $M_\mu := M$, $M_\nu := N$, $\alpha^\lambda_\mu := \alpha$, and $\alpha^\lambda_\nu := \beta$. Set $Q := \varinjlim M_\lambda$. Then writing

$$\begin{array}{ccccc} N & \xleftarrow{\beta} & L & \xrightarrow{\alpha} & M \\ {\scriptstyle\eta_\nu}\downarrow & & {\scriptstyle\eta_\lambda}\downarrow & & {\scriptstyle\eta_\mu}\downarrow \\ Q & \xleftarrow{1_R} & Q & \xrightarrow{1_R} & Q \end{array} \qquad \text{as} \qquad \begin{array}{ccc} L & \xrightarrow{\alpha} & M \\ {\scriptstyle\beta}\downarrow & & {\scriptstyle\eta_\mu}\downarrow \\ N & \xrightarrow{\eta_\nu} & Q \end{array}$$

we see that Q is equal to the pushout of α and β; here $\gamma = \eta_\mu$ and $\delta = \eta_\nu$.

In ((Sets)), take γ and δ to be the inclusions followed by the quotient map. Clearly $\gamma\alpha = \delta\beta$. Further, given P and maps $\gamma'\colon M \to P$ and $\delta'\colon N \to P$, they define a unique map $M \sqcup N \to P$, and it factors through the quotient if and only if $\gamma'\alpha = \delta'\beta$. Thus $(M \sqcup N)/\sim$ is the pushout.

In ((R-mod)), take γ and δ to be the inclusions followed by the quotient map. Then for all $\ell \in L$, clearly $\iota_M\alpha(\ell) - \iota_N\beta(\ell) = (\alpha(\ell), -\beta(\ell))$. So $\iota_M\alpha(\ell) - \iota_N\beta(\ell)$ is in $\operatorname{Im}(L)$; hence, $\iota_M\alpha(\ell)$ and $\iota_N\beta(\ell)$ have the same image in the quotient. Thus $\gamma\alpha = \delta\beta$. Given $\gamma'\colon M \to P$ and $\delta'\colon N \to P$, let $\varphi\colon M \oplus N \to P$ be the induced map. Clearly φ factors through the quotient if and only if with $\gamma'\alpha = \delta'\beta$. Thus $(M \oplus N)/\operatorname{Im}(L)$ is the pushout. □

Exercise **(6.16)**. — Let $\mathcal{C}$ be a category, Σ and Λ small categories.

(1) Prove $\mathcal{C}^{\Sigma\times\Lambda} = (\mathcal{C}^\Lambda)^\Sigma$ with $(\sigma, \lambda) \mapsto M_{\sigma,\lambda}$ corresponding to $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$.

(2) Assume $\mathcal{C}$ has direct limits indexed by Σ and by Λ. Prove that $\mathcal{C}$ has direct limits indexed by $\Sigma \times \Lambda$ and that $\varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma} = \varinjlim_{(\sigma,\lambda)\in\Sigma\times\Lambda}$.

Solution: In $\Sigma \times \Lambda$, a map $(\sigma, \lambda) \to (\tau, \mu)$ factors in two ways:

$$(\sigma, \lambda) \to (\tau, \lambda) \to (\tau, \mu) \quad \text{and} \quad (\sigma, \lambda) \to (\sigma, \mu) \to (\tau, \mu).$$

So, given a functor $(\sigma,\lambda)\mapsto M_{\sigma,\lambda}$, there is a commutative diagram like **(6.13.1)**. It shows that the map $\sigma\to\tau$ in Σ induces a natural transformation from $\lambda\mapsto M_{\sigma,\lambda}$ to $\lambda\mapsto M_{\tau,\lambda}$. Thus the rule $\sigma\mapsto(\lambda\mapsto M_{\sigma\lambda})$ is a functor from Σ to $\mathcal{C}^\Lambda$.

A map from $(\sigma,\lambda)\mapsto M_{\sigma,\lambda}$ to a second functor $(\sigma,\lambda)\mapsto N_{\sigma,\lambda}$ is a collection of maps $\theta_{\sigma,\lambda}\colon M_{\sigma,\lambda}\to N_{\sigma,\lambda}$ such that, for every map $(\sigma,\lambda)\to(\tau,\mu)$, the square

$$\begin{array}{ccc} M_{\sigma\lambda} & \longrightarrow & M_{\tau\mu} \\ {\scriptstyle\theta_{\sigma,\lambda}}\downarrow & & \downarrow{\scriptstyle\theta_{\tau,\mu}} \\ N_{\sigma\lambda} & \longrightarrow & N_{\tau\mu} \end{array}$$

is commutative. Factoring $(\sigma,\lambda)\to(\tau,\mu)$ in two ways as above, we get a commutative cube. It shows that the $\theta_{\sigma,\lambda}$ define a map in $(\mathcal{C}^\Lambda)^\Sigma$.

This passage from $\mathcal{C}^{\Sigma\times\Lambda}$ to $(\mathcal{C}^\Lambda)^\Sigma$ is reversible. Thus (1) holds.

Assume $\mathcal{C}$ has direct limits indexed by Σ and Λ. Then $\mathcal{C}^\Lambda$ has direct limits indexed by Σ by **(6.13)**. So the functors $\varinjlim_{\lambda\in\Lambda}\colon\mathcal{C}^\Lambda\to\mathcal{C}$ and $\varinjlim_{\sigma\in\Sigma}\colon(\mathcal{C}^\Lambda)^\Sigma\to\mathcal{C}^\Lambda$ exist, and they are the left adjoints of the diagonal functors $\mathcal{C}\to\mathcal{C}^\Lambda$ and $\mathcal{C}^\Lambda\to(\mathcal{C}^\Lambda)^\Sigma$ by **(6.6)**. Hence the composition $\varinjlim_{\lambda\in\Lambda}\varinjlim_{\sigma\in\Sigma}$ is the left adjoint of the composition of the two diagonal functors. But the latter is just the diagonal $\mathcal{C}\to\mathcal{C}^{\Sigma\times\Lambda}$ owing to (1). So this diagonal has a left adjoint, which is necessarily $\varinjlim_{(\sigma,\lambda)\in\Sigma\times\Lambda}$ owing to the uniqueness of adjoints. Thus (2) holds. □

Exercise **(6.17)**. — Let $\lambda\mapsto M_\lambda$ and $\lambda\mapsto N_\lambda$ be two functors from a small category Λ to $((R\text{-mod}))$, and $\{\theta_\lambda\colon M_\lambda\to N_\lambda\}$ a natural transformation. Show

$$dlim\,\mathrm{Coker}(\theta_\lambda)=\mathrm{Coker}(\varinjlim M_\lambda\to\varinjlim N_\lambda).$$

Show that the analogous statement for kernels can be false by constructing a counterexample using the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} \mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/\langle 2\rangle & \longrightarrow & 0 \\ \downarrow{\scriptstyle\mu_2} & & \downarrow{\scriptstyle\mu_2} & & \downarrow{\scriptstyle\mu_2} & & \\ \mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/\langle 2\rangle & \longrightarrow & 0 \end{array}$$

Solution: By **(6.8)**, the cokernel is a direct limit, and by **(6.14)**, direct limits commute; thus, the asserted equation holds.

To construct the desired counterexample using the given diagram, view its rows as expressing the cokernel $\mathbb{Z}/\langle 2\rangle$ as a direct limit over the category Λ of **(6.8)**. View the left two columns as expressing a natural transformation $\{\theta_\lambda\}$, and view the third column as expressing the induced map between the two limits. The latter map is 0, so its kernel is $\mathbb{Z}/\langle 2\rangle$. However, $\mathrm{Ker}(\theta_\lambda)=0$ for $\lambda\in\Lambda$; so $\varinjlim\mathrm{Ker}(\theta_\lambda)=0$. □

7. Filtered direct limits

Exercise **(7.2)**. — Let R be a ring, M a module, Λ a set, M_λ a submodule for each $\lambda\in\Lambda$. Assume $\bigcup M_\lambda=M$. Assume, given $\lambda,\mu\in\Lambda$, there is $\nu\in\Lambda$ such that $M_\lambda,\,M_\mu\subset M_\nu$. Order Λ by inclusion: $\lambda\le\mu$ if $M_\lambda\subset M_\mu$. Prove that $M=\varinjlim M_\lambda$.

SOLUTION: Let us prove that M has the UMP characterizing $\varinjlim M_\lambda$. Given homomorphisms $\beta_\lambda\colon M_\lambda \to P$ with $\beta_\lambda = \beta_\nu|M_\lambda$ when $\lambda \leq \nu$, define $\beta\colon M \to P$ by $\beta(m) := \beta_\lambda(m)$ if $m \in M_\lambda$. Such a λ exists as $\bigcup M_\lambda = M$. If also $m \in M_\mu$ and M_λ, $M_\mu \subset M_\nu$, then $\beta_\lambda(m) = \beta_\nu(m) = \beta_\mu(m)$; so β is well defined. Clearly, $\beta\colon M \to P$ is the unique set map such that $\beta|M_\lambda = \beta_\lambda$. Further, given $m, n \in M$ and $x \in R$, there is ν such that $m, n \in M_\nu$. So $\beta(m+n) = \beta_\nu(m+n) = \beta(m)+\beta(n)$ and $\beta(xm) = \beta_\nu(xm) = x\beta(m)$. Thus β is R-linear. Thus $M = \varinjlim M_\lambda$. □

EXERCISE **(7.3)**. — Show that every module M is the filtered direct limit of its finitely generated submodules.

SOLUTION: Every element $m \in M$ belongs to the submodule generated by m; hence, M is the union of all its finitely generated submodules. Any two finitely generated submodules are contained in a third, for example, their sum. So the assertion results from **(7.2)** with Λ the set of all finite subsets of M. □

EXERCISE **(7.4)**. — Show that every direct sum of modules is the filtered direct limit of its finite direct subsums.

SOLUTION: Consider an element of the direct sum. It has only finitely many nonzero components. So it lies in the corresponding finite direct subsum. Thus the union of the subsums is the whole direct sum. Now, given any two finite direct subsums, their sum is a third. Thus the finite subsets of indices form a directed partially ordered set Λ. So the assertion results from **(7.2)**. □

EXERCISE **(7.6)**. — Keep the setup of **(7.5)**. For each $n \in \Lambda$, set $N_n := \mathbb{Z}/\langle n\rangle$; if $n = ms$, define $\alpha_n^m\colon N_m \to N_n$ by $\alpha_n^m(x) := xs \pmod n$. Show $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$.

SOLUTION: For each $n \in \Lambda$, set $Q_n := M_n/\mathbb{Z} \subset \mathbb{Q}/Z$. If $n = ms$, then clearly Diagram **(7.5.1)** induces this one:

$$\begin{array}{ccc} N_m & \xrightarrow{\alpha_n^m} & N_n \\ {\scriptstyle\gamma_m}\downarrow\simeq & & {\scriptstyle\gamma_n}\downarrow\simeq \\ Q_m & \xhookrightarrow{\eta_n^m} & Q_n \end{array}$$

where η_n^m is the inclusion. Now, $\bigcup Q_n = \mathbb{Q}/\mathbb{Z}$ and Q_n, $Q_{n'} \subset Q_{nn'}$. So **(7.2)** yields $\mathbb{Q}/\mathbb{Z} = \varinjlim M_n$. Thus $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$. □

EXERCISE **(7.9)**. — Let R be a filtered direct limit of rings R_λ. Show $R = 0$ if and only if $R_\lambda = 0$ for some λ. Show R is a domain if R_λ is a domain for every λ.

SOLUTION: If $R_\lambda = 0$, then $1 = 0$ in R_λ; so $1 = 0$ in R as $\alpha_\lambda\colon R_\lambda \to R$ carries 1 to 1 and 0 to 0; hence, $R = 0$ by **(1.1)**. Conversely, assume $R = 0$. Then $1 = 0$ in R. So $\alpha_\lambda 1 = 0$ for any given λ. Hence, by **(7.8)**(3) with $\mathbb{Z}$ for R, there is α_μ^λ such that $\alpha_\mu^\lambda 1 = 0$. But $\alpha_\mu^\lambda 1 = 1$. Thus $1 = 0$ in R_μ, and so $R_\mu = 0$ by **(1.1)**.

Suppose every R_λ is a domain. Given x, $y \in R$ with $xy = 0$, we can lift x, y back to x_λ, $y_\lambda \in R_\lambda$ for some λ by **(7.8)**(1) and **(7.1)**(1). Then $x_\lambda y_\lambda$ maps to $0 \in R$. Hence, by **(7.8)**(3), there is a transition map α_μ^λ with $\alpha_\mu^\lambda(x_\lambda y_\lambda) = 0$ in R_μ. However, $\alpha_\mu^\lambda(x_\lambda y_\lambda) = \alpha_\mu^\lambda(x_\lambda)\alpha_\mu^\lambda(y_\lambda)$, and R_μ is a domain. Hence either $\alpha_\mu^\lambda(x_\lambda) = 0$ or $\alpha_\mu^\lambda(y_\lambda) = 0$. Therefore, either $x = 0$ or $y = 0$. Thus R is a domain. □

EXERCISE **(7.11)**. — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, and $N \subset M$ a submodule. For each λ, let $\alpha_\lambda \colon M_\lambda \to M$ be the insertion, and set $N_\lambda := \alpha_\lambda^{-1} N \subset M_\lambda$. Prove that $N = \varinjlim N_\lambda$.

SOLUTION: The given functor $\lambda \mapsto M_\lambda$ induces a functor $\lambda \mapsto N_\lambda$, and the insertions $\alpha_\lambda \colon M_\lambda \to M$ induce maps $\beta_\lambda \colon N_\lambda \to N$. So there is $\beta \colon \varinjlim N_\lambda \to N$ with $\beta\alpha_\lambda = \beta_\lambda$. By **(7.10)**, $\varinjlim N_\lambda \to M$ is injective; so β is too. Further, for any $m \in M$, there is an $m_\lambda \in M_\lambda$ such that $m = \alpha_\lambda m_\lambda$, and if $m \in N$, then $m_\lambda \in N_\lambda$ since $N_\lambda := \alpha_\lambda^{-1} N$. Thus β is surjective, so an isomorphism. □

EXERCISE **(7.13)**. — Let Λ and Λ' be small categories, $C \colon \Lambda' \to \Lambda$ a functor. Assume Λ' is filtered. Assume C is **cofinal**; that is,

(1) given $\lambda \in \Lambda$, there is a map $\lambda \to C\lambda'$ for some $\lambda' \in \Lambda'$, and
(2) given $\psi, \varphi \colon \lambda \rightrightarrows C\lambda'$, there is $\chi \colon \lambda' \to \lambda_1'$ with $(C\chi)\psi = (C\chi)\varphi$.

Let $\lambda \mapsto M_\lambda$ be a functor from Λ to $\mathcal{C}$ whose direct limit exists. Show that

$$\varinjlim_{\lambda' \in \Lambda'} M_{C\lambda'} = \varinjlim_{\lambda \in \Lambda} M_\lambda;$$

more precisely, show that the right side has the UMP characterizing the left.

SOLUTION: Let P be an object of $\mathcal{C}$. For $\lambda' \in \Lambda'$, take maps $\gamma_{\lambda'} \colon M_{C\lambda'} \to P$ compatible with the transition maps $M_{C\lambda'} \to M_{C\mu'}$. Given $\lambda \in \Lambda$, choose a map $\lambda \to C\lambda'$, and define $\beta_\lambda \colon M_\lambda \to P$ to be the composition

$$\beta_\lambda \colon M_\lambda \longrightarrow M_{C\lambda'} \xrightarrow{\gamma_{\lambda'}} P.$$

Let's check that β_λ is independent of the choice of $\lambda \to C\lambda'$.

Given a second choice $\lambda \to C\lambda''$, there are maps $\lambda'' \to \mu'$ and $\lambda' \to \mu'$ for some $\mu' \in \Lambda'$ since Λ' is filtered. So there is a map $\mu' \to \mu_1'$ such that the compositions $\lambda \to C\lambda' \to C\mu' \to C\mu_1'$ and $\lambda \to C\lambda'' \to C\mu' \to C\mu_1'$ are equal since C is cofinal. Therefore, $\lambda \to C\lambda''$ gives rise to the same β_λ, as desired.

Clearly, the β_λ are compatible with the transition maps $M_\kappa \to M_\lambda$. So the β_λ induce a map $\beta \colon \varinjlim M_\lambda \to P$ with $\beta\alpha_\lambda = \beta_\lambda$ for every insertion $\alpha_\lambda \colon M_\lambda \to \varinjlim M_\lambda$. In particular, this equation holds when $\lambda = C\lambda'$ for any $\lambda' \in \Lambda'$, as required. □

EXERCISE **(7.14)**. — Show that every R-module M is the filtered direct limit over a directed set of finitely presented modules.

SOLUTION: By **(5.19)**, there is a presentation $R^{\oplus\Phi_1} \xrightarrow{\alpha} R^{\oplus\Phi_2} \to M \to 0$. For $i = 1, 2$, let Λ_i be the set of finite subsets Ψ_i of Φ_i, and order Λ_i by inclusion. Clearly, an inclusion $\Psi_i \hookrightarrow \Phi_i$ yields an injection $R^{\oplus\Psi_i} \hookrightarrow R^{\oplus\Phi_i}$, which is given by extending vectors by 0. Hence **(7.2)** yields $\varinjlim R^{\oplus\Psi_i} = R^{\oplus\Phi_i}$.

Let $\Lambda \subset \Lambda_1 \times \Lambda_2$ be the set of pairs $\lambda := (\Psi_1, \Psi_2)$ such that α induces a map $\alpha_\lambda \colon R^{\oplus\Psi_1} \to R^{\oplus\Psi_2}$. Order Λ by componentwise inclusion. Clearly, Λ is directed. For $\lambda \in \Lambda$, set $M_\lambda := \operatorname{Coker}(\alpha_\lambda)$. Then M_λ is finitely presented.

For $i = 1, 2$, the projection $C_i \colon \Lambda \to \Lambda_i$ is surjective, so cofinal. Hence, **(7.13)** yields $\varinjlim_{\lambda \in \Lambda} R^{\oplus C_i\lambda} = \varinjlim_{\Psi_i \in \Lambda_i} R^{\oplus\Psi_i}$. Thus **(6.17)** yields $\varinjlim M_\lambda = M$. □

8. Tensor Products

EXERCISE **(8.6)**. — Let R be a domain. Set $K := \operatorname{Frac}(R)$. Given a nonzero submodule $M \subset K$, show that $M \otimes_R K = K$.

Solution: Define a map $\beta\colon \mathfrak{a}\times K \to K$ by $\beta(x,y) := xy$. It is clearly R-bilinear. Given any R-bilinear map $\alpha\colon \mathfrak{a}\times K \to P$, fix a nonzero $z \in \mathfrak{a}$, and define an R-linear map $\gamma\colon K \to P$ by $\gamma(y) := \alpha(z, y/z)$. Then $\alpha = \gamma\beta$ as

$$\alpha(x,y) = \alpha(xz, y/z) = \alpha(z, xy/z) = \gamma(xy) = \gamma\beta(x,y).$$

Clearly, β is surjective. So γ is unique with this property. Thus the UMP implies that $K = \mathfrak{a} \otimes_R K$. (Also, as γ is unique, γ is independent of the choice of z.)

Alternatively, form the linear map $\varphi\colon \mathfrak{a}\otimes K \to K$ induced by the bilinear map β. Since β is surjective, so is φ. Now, given any $w \in \mathfrak{a}\otimes K$, say $w = \sum a_i \otimes x_i/x$ with all x_i and x in R. Set $a := \sum a_i x_i \in \mathfrak{a}$. Then $w = a \otimes (1/x)$. Hence, if $\varphi(w) = 0$, then $a/x = 0$; so $a = 0$ and so $w = 0$. Thus φ is injective, so bijective. □

Exercise **(8.8)**. — Let R be a ring, R' an R-algebra, M, N two R'-modules. Show there is a canonical R-linear map $\tau\colon M \otimes_R N \to M \otimes_{R'} N$.

Let $K \subset M \otimes_R N$ denote the R-submodule generated by all the differences $(x'm)\otimes n - m \otimes (x'n)$ for $x' \in R'$ and $m \in M$ and $n \in N$. Show $K = \operatorname{Ker}(\tau)$. Show τ is surjective, and is an isomorphism if R' is a quotient of R.

Solution: The canonical map $\beta'\colon M \times N \to M \otimes_{R'} N$ is R'-bilinear, so R-bilinear. Hence, by **(8.3)**, it factors: $\beta' = \tau\beta$ where $\beta\colon M \times N \to M \otimes_R N$ is the canonical map and τ is the desired map.

Set $Q := (M \otimes_R N)/K$. Then τ factors through a map $\tau'\colon Q \to M \otimes_{R'} N$ since each generator $(x'm)\otimes n - m \otimes (x'n)$ of K maps to 0 in $M \otimes_{R'} N$.

By **(8.7)**, there is an R'-structure on $M \otimes_R N$ with $y'(m \otimes n) = m \otimes (y'n)$, and so by **(8.5)**(1), another one with $y'(m\otimes n) = (y'm)\otimes n$. Clearly, K is a submodule for each structure, so Q is too. But on Q the two structures coincide. Further, the canonical map $M \times N \to Q$ is R'-bilinear. Hence the latter factors through $M \otimes_{R'} N$, furnishing an inverse to τ'. So $\tau'\colon Q \xrightarrow{\sim} M \otimes_{R'} N$. Hence $\operatorname{Ker}(\tau)$ is equal to K, and τ is surjective.

Finally, suppose R' is a quotient of R. Then every $x' \in R'$ is the residue of some $x \in R$. So each $(x'm)\otimes n - m \otimes (x'n)$ is equal to 0 in $M \otimes_R N$ as $x'm = xm$ and $x'n = xn$. Hence $\operatorname{Ker}(\tau)$ vanishes. Thus τ is an isomorphism. □

Exercise **(8.13)**. — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module.

(1) Use **(8.11)** to show that $(R/\mathfrak{a}) \otimes M = M/\mathfrak{a}M$.

(2) Use (1) to show that $(R/\mathfrak{a}) \otimes (R/\mathfrak{b}) = R/(\mathfrak{a}+\mathfrak{b})$.

Solution: To prove (1), view $R/\mathfrak{a}$ as the cokernel of the inclusion $\mathfrak{a} \to R$. Then **(8.11)** implies that $(R/\mathfrak{a})\otimes M$ is the cokernel of $\mathfrak{a}\otimes M \to R\otimes M$. Now, $R\otimes M = M$ and $x \otimes m = xm$ by **(8.5)**(2). Correspondingly, $\mathfrak{a} \otimes M \to M$ has $\mathfrak{a}M$ as image. The assertion follows. (Caution: $\mathfrak{a} \otimes M \to M$ needn't be injective; if it's not, then $\mathfrak{a} \otimes M \neq \mathfrak{a}M$. For example, take $R := \mathbb{Z}$, take $\mathfrak{a} := \langle 2\rangle$, and take $M := \mathbb{Z}/\langle 2\rangle$; then $\mathfrak{a} \otimes M \to M$ is just multiplication by 2 on $\mathbb{Z}/\langle 2\rangle$, and so $\mathfrak{a}M = 0$.)

To prove (2), apply (1) with $M := R/\mathfrak{b}$. Note $\mathfrak{a}(R/\mathfrak{b}) = (\mathfrak{a}+\mathfrak{b})/\mathfrak{b}$. Hence

$$R/\mathfrak{a} \otimes R/\mathfrak{b} = (R/\mathfrak{b})\big/((\mathfrak{a}+\mathfrak{b})/\mathfrak{b}).$$

The latter is equal to $R/(\mathfrak{a}+\mathfrak{b})$ by **(4.8)**. □

Exercise **(8.14)**. — Let k be a field, M and N nonzero vector spaces. Prove that $M \otimes N \neq 0$.

SOLUTION: Since k is a field, M and N are free; say $M = k^{\oplus\Phi}$ and $N = k^{\oplus\Psi}$. Then **(8.11)** yields $M \otimes N = k^{\oplus(\Phi\times\Psi)}$ as $k \otimes k = k$ by **(8.5)**(2). Thus $M \otimes N \neq 0$. □

EXERCISE **(8.16)**. — Let $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a linear functor. Show that F always preserves finite direct sums. Show that $\theta(M)\colon M \otimes F(R) \to F(M)$ is surjective if F preserves surjections and M is finitely generated, and that $\theta(M)$ is an isomorphism if F preserves cokernels and M is finitely presented.

SOLUTION: The first assertion follows immediately from the characterization of finite direct sum in terms of maps **(4.15)**, since F preserves the stated relations.

The second assertion follows from the first via the second part of the proof of Watt's Theorem **(8.15)**, but with Σ and Λ finite. □

EXERCISE **(8.20)**. — Let X be a variable, ω a complex cubic root of 1, and $\sqrt[3]{2}$ the real cube root of 2. Set $k := \mathbb{Q}(\omega)$ and $K := k[\sqrt[3]{2}]$. Show $K = k[X]/\langle X^3 - 2\rangle$ and then $K \otimes_k K = K \times K \times K$.

SOLUTION: Note ω is a root of $X^2 + X + 1$, which is irreducible over $\mathbb{Q}$; hence, $[k : \mathbb{Q}] = 2$. But the three roots of $X^3 - 2$ are $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. Therefore, $X^3 - 2$ has no root in k. So $X^3 - 2$ is irreducible over k. Thus $k[X]/\langle X^3 - 2\rangle \xrightarrow{\sim} K$.

Note $K[X] = K \otimes_k k[X]$ as k-algebras by **(8.19)**. So **(8.5)**(2) and **(8.10)** and **(8.13)**(1) yield

$$\begin{aligned} k[X]/\langle X^3 - 2\rangle \otimes_k K &= k[X]/\langle X^3 - 2\rangle \otimes_{k[X]} (k[X] \otimes_k K) \\ &= k[X]/\langle X^3 - 2\rangle \otimes_{k[X]} K[X] = K[X]/\langle X^3 - 2\rangle. \end{aligned}$$

However, $X^3 - 2$ factors in K as follows:

$$X^3 - 2 = \bigl(X - \sqrt[3]{2}\bigr)\bigl(X - \omega\sqrt[3]{2}\bigr)\bigl(X - \omega^2\sqrt[3]{2}\bigr).$$

So the Chinese Remainder Theorem, **(1.12)**, yields

$$K[X]/\langle X^3 - 2\rangle = K \times K \times K,$$

because $K[X]/\langle X - \omega^i\sqrt[3]{2}\rangle \xrightarrow{\sim} K$ for any i by **(1.6)**. □

9. Flatness

EXERCISE **(9.7)**. — Let R be a ring, R' a flat algebra, and P a flat R'-module. Show that P is a flat R-module.

SOLUTION: Cancellation **(8.10)** yields $\bullet \otimes_R P = (\bullet \otimes_R R') \otimes_{R'} P$. But $\bullet \otimes_R R'$ and $\bullet \otimes_{R'} P$ are exact. Hence, $\bullet_R P$ is too. Thus P is R-flat. □

EXERCISE **(9.8)**. — Let R be a ring, M a flat module, and R' an algebra. Show that $M \otimes_R R'$ is a flat R'-module.

SOLUTION: Cancellation **(8.10)** yields $(M \otimes_R R') \otimes_{R'} \bullet = M \otimes_R \bullet$. Therefore, $(M \otimes_R R') \otimes_{R'} \bullet$ is exact. Thus $M \otimes_R R'$ is R'-flat. □

EXERCISE **(9.9)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume that $R/\mathfrak{a}$ is R-flat. Show that $\mathfrak{a} = \mathfrak{a}^2$.

SOLUTION: Since $R/\mathfrak{a}$ is flat, tensoring it with the inclusion $\mathfrak{a} \hookrightarrow R$ yields an injection $\mathfrak{a} \otimes_R (R/\mathfrak{a}) \hookrightarrow R \otimes_R (R/\mathfrak{a})$. But the image vanishes: $a \otimes r = 1 \otimes ar = 0$. Further, $\mathfrak{a} \otimes_R (R/\mathfrak{a}) = \mathfrak{a}/\mathfrak{a}^2$ by **(8.13)**. Hence $\mathfrak{a}/\mathfrak{a}^2 = 0$. Thus $\mathfrak{a} = \mathfrak{a}^2$. □

EXERCISE **(9.13)**. — Let R be a ring, R' an algebra, M and N modules. Show that there is a canonical map

$$\sigma\colon \operatorname{Hom}_R(M, N) \otimes_R R' \to \operatorname{Hom}_{R'}(M \otimes_R R', N \otimes_R R').$$

Assume R' is flat over R. Show that if M is finitely generated, then σ is injective, and that if M is finitely presented, then σ is an isomorphism.

SOLUTION: Simply put $R' := R$ and $P := R'$ in **(9.12)**, put $P := N \otimes_R R'$ in the second equation in **(8.10)**, and combine the two results. □

EXERCISE **(9.17)** (*Equational Criterion for Flatness*). — Prove that Condition **(9.16)**(4) can be reformulated as follows: For every relation $\sum_i x_i y_i = 0$ with $x_i \in R$ and $y_i \in M$, there are $x_{ij} \in R$ and $y'_j \in M$ such that

$$\textstyle\sum_j x_{ij} y'_j = y_i \text{ for all } i \text{ and } \sum_i x_{ij} x_i = 0 \text{ for all } j. \qquad \textbf{(9.17.1)}$$

SOLUTION: Assume **(9.16)**(4) holds. Let $e_1, \dots, e_m$ be the standard basis of R^m. Given a relation $\sum_1^m x_i y_i = 0$, define $\alpha\colon R^m \to M$ by $\alpha(e_i) := y_i$ for each i. Set $k := \sum x_i e_i$. Then $\alpha(k) = 0$. So **(9.16)**(4) yields a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \xrightarrow{\beta} M$ with $\varphi(k) = 0$. Let $e'_1, \dots, e'_n$ be the standard basis of R^n, and set $y'_j := \beta(e'_j)$ for each j. Let (x_{ij}) be the $n \times m$ matrix of φ; that is, $\varphi(e_i) = \sum x_{ji} e'_j$. Then $y_i = \sum x_{ji} y'_j$. Now, $\varphi(k) = 0$; hence, $\sum_{i,j} x_{ji} x_i e'_j = 0$. Thus **(9.17.1)** holds.

Conversely, given $\alpha\colon R^m \to M$ and $k \in \operatorname{Ker}(\alpha)$, write $k = \sum x_i e_i$. Assume **(9.17.1)**. Let $\varphi\colon R^m \to R^n$ be the map with matrix (x_{ij}); that is, $\varphi(e_i) = \sum x_{ji} e'_j$. Then $\varphi(k) = \sum x_i x_{ji} e'_j = 0$. Define $\beta\colon R^n \to M$ by $\beta(e'_j) := y'_j$. Then $\beta\varphi(e_i) = y_i$; hence, $\beta\varphi = \alpha$. Thus **(9.16)**(4) holds. □

EXERCISE **(9.20)**. — Let R be a domain, M a module. Prove that, if M is flat, then M is **torsion free**; that is, $\mu_x\colon M \to M$ is injective for all nonzero $x \in R$. Prove that, conversely, if R is a PID and M is torsion free, then M is flat.

SOLUTION: Since R is a domain, $\mu_x\colon R \to R$ is injective. So if M is flat, then $\mu_x \otimes M\colon R \otimes M \to R \otimes M$ is injective too. But $R \otimes M = M$ by **(8.5)**.

Conversely, assume R is a PID and M is torsion free. Let $\mathfrak{a}$ be a nonzero ideal, say $\mathfrak{a} = \langle x \rangle$. Define $\alpha\colon R \to \mathfrak{a}$ by $\alpha(y) := xy$. Then α is injective as R is a domain and $x \neq 0$. Further, α is surjective as $\mathfrak{a} = \langle x \rangle$. So α is bijective.

Consider the composition

$$\beta\colon M = R \otimes M \xrightarrow{\alpha \otimes M} \mathfrak{a} \otimes M \to M.$$

Clearly, $\beta = \mu_x$. So β is injective since M is torsion free. Hence $\mathfrak{a} \otimes M \to M$ is injective too. So M is flat by the Ideal Criterion **(9.18)**. □

10. Cayley–Hamilton Theorem

EXERCISE **(10.6)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a}$ is finitely generated and satisfies $\mathfrak{a} = \mathfrak{a}^2$. Prove there is a unique idempotent e such that $\langle e \rangle = \mathfrak{a}$.

SOLUTION: By **(10.3)** with $\mathfrak{a}$ for M, there is $e \in \mathfrak{a}$ such that $(1-e)\mathfrak{a} = 0$. In other words, for all $x \in \mathfrak{a}$, we have $(1-e)x = 0$, or $x = ex$. Thus $\mathfrak{a} = \langle e \rangle$ and $e = e^2$.

Suppose also $\mathfrak{a} = \langle f \rangle$ and $f = f^2$. Say $e = fx$ and $f = ey$. Then

$$e = fx = f^2x = fe = e^2y = ey = f. \qquad \square$$

EXERCISE **(10.10)**. — Let A be a local ring, $\mathfrak{m}$ the maximal ideal, M a finitely generated A-module, and $m_1, \dots, m_n \in M$. Set $k := A/\mathfrak{m}$ and $M' := M/\mathfrak{m}M$, and write m_i' for the image of m_i in M'. Prove that $m_1', \dots, m_n' \in M'$ form a basis of the k-vector space M' if and only if $m_1, \dots, m_n$ form a **minimal generating set** of M (that is, no proper subset generates M), and prove that every minimal generating set of M has the same number of elements.

SOLUTION: By **(10.9)**, reduction mod $\mathfrak{m}$ gives a bijective correspondence between generating sets of M as an A-module, and generating sets of M' as an A-module, or equivalently by **(4.5)**, as an k-vector space. This correspondence preserves inclusion. Hence, a minimal generating set of M corresponds to a minimal generating set of M', that is, to a basis. But any two bases have the same number of elements. $\square$

EXERCISE **(10.11)**. — Let A be a local ring, k its residue field, M and N finitely generated modules. (1) Show that $M = 0$ if and only if $M \otimes_A k = 0$. (2) Show that $M \otimes_A N \neq 0$ if $M \neq 0$ and $N \neq 0$.

SOLUTION: Let $\mathfrak{m}$ be the maximal ideal. Then $M \otimes k = M/\mathfrak{m}M$ by **(8.13)**(1). So (1) is nothing but a form of Nakayama's lemma **(10.8)**.

In (2), $M \otimes k \neq 0$ and $N \otimes k \neq 0$ by (1). So $(M \otimes k) \otimes (N \otimes k) \neq 0$ by **(8.14)** and **(8.8)**. But $(M \otimes k) \otimes (N \otimes k) = (M \otimes N) \otimes (k \otimes k)$ by the associative and commutative laws. Finally, $k \otimes k = k$ by **(8.13)**(1). $\square$

EXERCISE **(10.14)**. — Let G be a finite group acting on a domain R, and R' the ring of invariants. Show every $x \in R$ is integral over R', in fact, over the subring R'' generated by the elementary symmetric functions in the conjugates gx for $g \in G$.

SOLUTION: Given an $x \in R$, form $F(X) := \prod_{g \in G}(X - gx)$. Then the coefficients of $F(X)$ are the elementary symmetric functions in the conjugates gx for $g \in G$; hence, they are invariant under the action of G. So $F(x) = 0$ is a relation of integral dependence for x over R', in fact, over its subring R''. $\square$

EXERCISE **(10.16)**. — Let k be a field, $P := k[X]$ the polynomial ring in one variable, $f \in P$. Set $R := k[X^2] \subset P$. Using the free basis $1, X$ of P over R, find an explicit equation of integral dependence of degree 2 on R for f.

SOLUTION: Write $f = f_e + f_o$, where f_e and f_o are the polynomials formed by the terms of f of even and odd degrees. Say $f_o = gX$. Then the matrix of μ_f is $\left(\begin{smallmatrix} f_e & gX^2 \\ g & f_e \end{smallmatrix}\right)$. Its characteristic polynomial is $T^2 - 2f_eT + f_e^2 - f_o^2$. So the Cayley–Hamilton Theorem **(10.1)** yields $f^2 - 2f_ef + f_e^2 - f_o^2 = 0$. $\square$

EXERCISE **(10.21)**. — Let $R_1, \dots, R_n$ be R-algebras that are integral over R. Show that their product $\prod R_i$ is a integral over R.

SOLUTION: Let $y = (y_1, \dots, y_n) \in \prod_{i=1}^n R_i$. Since R_i/R is integral, $R[y_i]$ is a module-finite R-subalgebra of R_i. Hence $\prod_{i=1}^n R[y_i]$ is a module-finite R-subalgebra of $\prod_{i=1}^n R_i$ by **(4.14)** and induction on n. Now, $y \in \prod_{i=1}^n R[y_i]$. Therefore, y is integral over R. Thus $\prod_{i=1}^n R_i$ is integral over R. □

EXERCISE **(10.23)**. — For $1 \le i \le r$, let R_i be a ring, R_i' an extension of R_i, and $x_i \in R_i'$. Set $R := \prod R_i$, set $R' := \prod R_i'$, and set $x := (x_1, \dots, x_r)$. Prove

(1) x is integral over R if and only if x_i is integral over R_i for each i;

(2) R is integrally closed in R' if and only if each R_i is integrally closed in R_i'.

SOLUTION: Assume x is integral over R. Say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_j \in R$. Say $a_j =: (a_{1j}, \dots, a_{rj})$. Fix i. Then $x_i^n + a_{i1}x^{n-1} + \cdots + a_{in} = 0$. So x_i is integral over R_i.

Conversely, assume each x_i is integral over R_i. Say $x_i^{n_i} + a_{i1}x_i^{n_i-1} + \cdots + a_{in_i} = 0$. Set $n := \max n_i$, set $a_{ij} := 0$ for $j > n_i$, and set $a_j := (a_{1j}, \dots, a_{rj}) \in R$ for each j. Then $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Thus x is integral over R. Thus (1) holds.

Assertion (2) is an immediate consequence of (1). □

EXERCISE **(10.27)**. — Let k be a field, X and Y variables. Set

$$R := k[X, Y]/\langle Y^2 - X^2 - X^3 \rangle,$$

and let $x, y \in R$ be the residues of X, Y. Prove that R is a domain, but not a field. Set $t := y/x \in \mathrm{Frac}(R)$. Prove that $k[t]$ is the integral closure of R in $\mathrm{Frac}(R)$.

SOLUTION: As $k[X, Y]$ is a UFD and $Y^2 - X^2 - X^3$ is irreducible, $\langle Y^2 - X^2 - X^3 \rangle$ is prime by **(2.6)**; however, it is not maximal by **(2.24)**. Hence R is a domain by **(2.9)**, but not a field by **(2.16)**.

Note $y^2 - x^2 - x^3 = 0$. Hence $x = t^2 - 1$ and $y = t^3 - t$. So $k[t] \supset k[x, y] = R$. Further, t is integral over R; so $k[t]$ is integral over R by (2)⇒(1) of **(10.20)**.

Finally, $k[t]$ has $\mathrm{Frac}(R)$ as fraction field. Further, $\mathrm{Frac}(R) \neq R$, so x and y cannot be algebraic over k; hence, t must be transcendental. So $k[t]$ is normal by **(10.26)**(1). Thus $k[t]$ is the integral closure of R in $\mathrm{Frac}(R)$. □

11. Localization of Rings

EXERCISE **(11.2)**. — Let R be a ring, S a multiplicative set. Prove $S^{-1}R = 0$ if and only if S contains a nilpotent element.

SOLUTION: By **(1.1)**, $S^{-1}R = 0$ if and only if $1/1 = 0/1$. But by construction, $1/1 = 0/1$ if and only if $0 \in S$. Finally, since S is multiplicative, $0 \in S$ if and only if S contains a nilpotent element. □

EXERCISE **(11.4)**. — Find all intermediate rings $\mathbb{Z} \subset R \subset \mathbb{Q}$, and describe each R as a localization of $\mathbb{Z}$. As a starter, prove $\mathbb{Z}[2/3] = S^{-1}\mathbb{Z}$ where $S = \{3^i \mid i \ge 0\}$.

SOLUTION: Clearly $\mathbb{Z}[2/3] \subset \mathbb{Z}[1/3]$ as $2/3 = 2 \cdot (1/3)$. But the opposite inclusion holds as $1/3 = 1 - (2/3)$. Obviously, $S^{-1}\mathbb{Z} = \mathbb{Z}[1/3]$.

Let $P \subset \mathbb{Z}$ be the set of all prime numbers that appear as factors of the denominators of elements of R in lowest terms; recall that $x = r/s \in \mathbb{Q}$ is in **lowest terms** if r and s have no common prime divisor. Let S be the multiplicative set **generated by** P, that is, the smallest multiplicative set containing P. Clearly, S is equal to the set of all products of elements of P.

First note that, if $p \in P$, then $1/p \in R$. Indeed, take an element $x = r/ps \in R$ in lowest terms. Then $sx = r/p \in R$. Also the Euclidean algorithm yields m, $n \in \mathbb{Z}$ such that $mp + nr = 1$. Then $1/p = m + nsx \in R$, as desired. Hence $S^{-1}\mathbb{Z} \subset R$. But the opposite inclusion holds because, by the very definition of S, every element of R is of the form r/s for some $s \in S$. Thus $S^{-1}\mathbb{Z} = R$. □

Exercise **(11.7)**. — Let R' and R'' be rings. Consider $R := R' \times R''$ and set $S := \{(1,1), (1,0)\}$. Prove $R' = S^{-1}R$.

Solution: Let's show that the projection map $\pi\colon R' \times R'' \to R'$ has the UMP of **(11.5)**. First, note that $\pi S = \{1\} \subset R'^{\times}$. Let $\psi\colon R' \times R'' \to B$ be a ring map such that $\psi(1,0) \in B^{\times}$. Then in B,

$$\psi(1,0) \cdot \psi(0,x) = \psi\big((1,0) \cdot (0,x)\big) = \psi(0,0) = 0 \text{ in } B.$$

Hence $\psi(0,x) = 0$ for all $x \in R''$. So ψ factors uniquely through π by **(1.4)**. □

Exercise **(11.8)**. — Take R and S as in **(11.7)**. On $R \times S$, impose this relation:

$$(x,s) \sim (y,t) \quad \text{if} \quad xt = ys.$$

Prove that it is not an equivalence relation.

Solution: Observe that, for any $z \in R''$, we have

$$\big((1,z), (1,1)\big) \sim \big((1,0), (1,0)\big).$$

However, if $z \neq 0$, then

$$\big((1,z), (1,1)\big) \not\sim \big((1,0), (1,1)\big).$$

Thus although $\sim$ is reflexive and symmetric, it is *not* transitive if $R'' \neq 0$. □

Exercise **(11.14)**. — Let R be a ring, S a multiplicative set. Prove that

$$\operatorname{nil}(R)(S^{-1}R) = \operatorname{nil}(S^{-1}R).$$

Solution: Proceed by double inclusion. Given an element of $\operatorname{nil}(R)(S^{-1}R)$, put it in the form x/s with $x \in \operatorname{nil}(R)$ and $s \in S$ using **(11.11)**(1). Then $x^n = 0$ for some $n \geq 1$. So $(x/s)^n = 0$. So $x/s \in \operatorname{nil}(S^{-1}R)$. Thus $\operatorname{nil}(R)(S^{-1}R) \subset \operatorname{nil}(S^{-1}R)$.

Conversely, take $x/s \in \operatorname{nil}(S^{-1}R)$. Then $(x/s)^m = 0$ with $m \geq 1$. So there's $t \in S$ with $tx^m = 0$ by **(11.13)**(1). Then $(tx)^m = 0$. So $tx \in \operatorname{nil}(R)$. But $tx/ts = x/s$. So $x/s \in \operatorname{nil}(R)(S^{-1}R)$ by **(11.11)**(1). Thus $\operatorname{nil}(R)(S^{-1}R) \supset \operatorname{nil}(S^{-1}R)$. □

Exercise **(11.20)**. — Let R'/R be an integral extension of rings, and S a multiplicative subset of R. Show that $S^{-1}R'$ is integral over $S^{-1}R$.

Solution: Given $x/s \in S^{-1}R'$, let $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ be an equation of integral dependence of x on R. Then

$$(x/s)^n + (a_{n-1}/1)(1/s)(x/s)^{n-1} + \cdots + a_0(1/s)^n = 0$$

is an equation of integral dependence of x/s on $S^{-1}R$, as required. □

Exercise **(11.21)**. — Let R be a domain, K its fraction field, L a finite extension field, and $\overline{R}$ the integral closure of R in L. Show that L is the fraction field of $\overline{R}$. Show that, in fact, every element of L can be expressed as a fraction b/a where b is in $\overline{R}$ and a is in R.

SOLUTION: Let $x \in L$. Then x is algebraic (integral) over K, say

$$x^n + y_1 x^{n-1} + \cdots + y_n = 0$$

with $y_i \in K$. Write $y_i = a_i/a$ with $a_1, \ldots, a_n, a \in R$. Then

$$(ax)^n + (aa_1)(ax)^{n-1} + \cdots + a^n a_0 = 0.$$

Set $b := ax$. Then $b \in \overline{R}$ and $x = b/a$. □

EXERCISE **(11.22)**. — Let $R \subset R'$ be domains, K and L their fraction fields. Assume that R' is a finitely generated R-algebra, and that L is a finite dimensional K-vector space. Find an $f \in R$ such that R'_f is module finite over R_f.

SOLUTION: Let $x_1, \ldots, x_n$ generate R' over R. Using **(11.21)**, write $x_i = b_i/a_i$ with b_i integral over R and a_i in R. Set $f := \prod a_i$. The x_i generate R'_f as an R_f-algebra; so the b_i do too. Thus R'_f is s module finite over R_f by **(10.20)**. □

EXERCISE **(11.25)**. — Let R be a ring, S and T multiplicative sets.

(1) Set $T' := \varphi_S(T)$ and assume $S \subset T$. Prove

$$T^{-1}R = T'^{-1}(S^{-1}R) = T^{-1}(S^{-1}R).$$

(2) Set $U := \{st \in R \mid s \in S \text{ and } t \in T\}$. Prove

$$T^{-1}(S^{-1}R) = S^{-1}(T^{-1}R) = U^{-1}R.$$

(3) Let $S' := \{t' \in R \mid t't \in S \text{ for some } t \in R\}$. Prove $S'^{-1}R = S^{-1}R$.

SOLUTION: A proof similar to that of **(11.23)** shows $T^{-1}R = T'^{-1}(S^{-1}R)$. By **(11.19)**, $T'^{-1}(S^{-1}R) = T^{-1}(S^{-1}R)$. Thus (1) holds.

As $1 \in T$, obviously $S \subset U$. So (1) yields $U^{-1}R = U^{-1}(S^{-1}R)$. Now, clearly $U^{-1}(S^{-1}R) = T^{-1}(S^{-1}R)$. Similarly, $U^{-1}R = S^{-1}(T^{-1}R)$. Thus (2) holds.

Finally, in any ring, a product is a unit if and only if each factor is a unit. So a homomorphism $\varphi\colon R \to R'$ carries S' into $R'^{\times}$ if and only if φ carries S into $R'^{\times}$. Thus $S'^{-1}R$ and $S^{-1}R$ are universal examples of R-algebras that satisfy equivalent conditions. Thus (3) holds. □

EXERCISE **(11.28)** (*Localization and normalization commute*). — Given a domain R and a multiplicative set S with $0 \notin S$. Show that the localization of the normalization $S^{-1}\overline{R}$ is equal to the normalization of the localization $\overline{S^{-1}R}$.

SOLUTION: Since $0 \notin S$, clearly $\operatorname{Frac}(S^{-1}R) = \operatorname{Frac}(R)$ owing to **(11.3)**. Now, $S^{-1}\overline{R}$ is integral over $S^{-1}R$ by **(11.20)**. Thus $S^{-1}\overline{R} \subset \overline{S^{-1}R}$.

Conversely, given $x \in \overline{S^{-1}R}$, consider an equation of integral dependence:

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

Say $a_i = b_i/s_i$ with $b_i \in R$ and $s_i \in S$; set $s := \prod s_i$. Multiplying by s^n yields

$$(sx)^n + sa_1(sx)^{n-1} + \cdots + s^n a_n = 0.$$

Hence $sx \in \overline{R}$. So $x \in S^{-1}\overline{R}$. Thus $S^{-1}\overline{R} \supset \overline{S^{-1}R}$, as desired. □

12. Localization of Modules

EXERCISE **(12.4)**. — Let R be a ring, S a multiplicative set, and M a module. Show that $M = S^{-1}M$ if and only if M is an $S^{-1}R$-module.

SOLUTION: If $M = S^{-1}M$, then obviously M is an $S^{-1}R$-module. Conversely, if M is an $S^{-1}R$-module, then M equipped with the identity map has the UMP that characterizes $S^{-1}M$; whence, $M = S^{-1}M$. □

EXERCISE **(12.5)**. — Let R be a ring, $S \subset T$ multiplicative sets, M a module. Set $T_1 := \varphi_S(T) \subset S^{-1}R$. Show $T^{-1}M = T^{-1}(S^{-1}M) = T_1^{-1}(S^{-1}M)$.

SOLUTION: Let's check that both $T^{-1}(S^{-1}M)$ and $T_1^{-1}(S^{-1}M)$ have the UMP characterizing $T^{-1}M$. Let $\psi\colon M \to N$ be an R-linear map into an $T^{-1}R$-module. Then the multiplication map $\mu_s\colon N \to N$ is bijective for all $s \in T$ by **(12.1)**, so for all $s \in S$ since $S \subset T$. Hence ψ factors via a unique $S^{-1}R$-linear map $\rho\colon S^{-1}M \to N$ by **(12.3)** and by **(12.1)** again.

Similarly, ρ factors through a unique $T^{-1}R$-linear map $\rho'\colon T^{-1}(S^{-1}M) \to N$. Hence $\psi = \rho'\varphi_T\varphi_S$, and ρ' is clearly unique, as required. Also, ρ factors through a unique $T_1^{-1}(S^{-1}R)$-linear map $\rho_1'\colon T_1^{-1}(S^{-1}M) \to N$. Hence $\psi = \rho_1'\varphi_{T_1}\varphi_S$, and ρ_1' is clearly unique, as required. □

EXERCISE **(12.6)**. — Let R be a ring, S a multiplicative set. Show that S becomes a filtered category when equipped as follows: given $s, t \in S$, set

$$\mathrm{Hom}(s,t) := \{x \in R \mid xs = t\}.$$

Given a module M, define a functor $S \to ((R\text{-mod}))$ as follows: for $s \in S$, set $M_s := M$; to each $x \in \mathrm{Hom}(s,t)$, associate $\mu_x\colon M_s \to M_t$. Define $\beta_s\colon M_s \to S^{-1}M$ by $\beta_s(m) := m/s$. Show the β_s induce an isomorphism $\varinjlim M_s \xrightarrow{\sim} S^{-1}M$.

SOLUTION: Clearly, S is a category. Now, given $s, t \in S$, set $u := st$. Then $u \in S$; also $t \in \mathrm{Hom}(s,u)$ and $s \in \mathrm{Hom}(t,u)$. Given $x, y \in \mathrm{Hom}(s,t)$, we have $xs = t$ and $ys = t$. So $s \in \mathrm{Hom}(t,u)$ and $xs = ys$ in $\mathrm{Hom}(s,u)$. Thus S is filtered.

Further, given $x \in \mathrm{Hom}(s,t)$, we have $\beta_t\mu_x = \beta_s$ since $m/s = xm/t$ as $xs = t$. So the β_s induce a homomorphism $\beta\colon \varinjlim M_s \to S^{-1}M$. Now, every element of $S^{-1}M$ is of the form m/s, and $m/s =: \beta_s(m)$; hence, β is surjective.

Each $m \in \varinjlim M_s$ lifts to an $m' \in M_s$ for some $s \in S$ by **(7.8)**(1). Assume $\beta m = 0$. Then $\beta_s m' = 0$ as the β_s induce β. But $\beta_s m' = m'/s$. So there is $t \in S$ with $tm' = 0$. So $\mu_t m' = 0$ in M_{st}, and $\mu_t m' \mapsto m$. So $m = 0$. Thus β is injective, so an isomorphism. □

EXERCISE **(12.7)**. — Let R be a ring, S a multiplicative set, M a module. Prove $S^{-1}M = 0$ if $\mathrm{Ann}(M) \cap S \neq \emptyset$. Prove the converse if M is finitely generated.

SOLUTION: Say $f \in \mathrm{Ann}(M) \cap S$. Let $m/t \in S^{-1}M$. Then $f/1 \cdot m/t = fm/t = 0$. Hence $m/t = 0$. Thus $S^{-1}M = 0$.

Conversely, assume $S^{-1}M = 0$, and say $m_1, \dots m_n$ generate M. Then for each i, there is $f_i \in S$ with $f_i m_i = 0$. Then $\prod f_i \in \mathrm{Ann}(M) \cap S$, as desired. □

EXERCISE **(12.11)**. — Let R be a ring, S a multiplicative set, P a projective module. Then $S^{-1}P$ is a projective $S^{-1}R$-module.

SOLUTION: By **(5.22)**, there is a module K such that $F := K \oplus P$ is free. So **(12.9)** yields that $S^{-1}F = S^{-1}P \oplus S^{-1}L$ and that $S^{-1}F$ is free over $S^{-1}R$. Hence $S^{-1}P$ is a projective $S^{-1}R$-module again by **(5.22)**. □

EXERCISE **(12.13)**. — Let R be a ring, S a multiplicative set, M and N modules. Show $S^{-1}(M \otimes_R N) = S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} S^{-1}N = S^{-1}M \otimes_R S^{-1}N$.

SOLUTION: By **(12.12)**, $S^{-1}(M \otimes_R N) = S^{-1}R \otimes_R (M \otimes_R N)$. The latter is equal to $(S^{-1}R \otimes_R M) \otimes_R N$ by associativity **(8.9)**. Again by **(12.12)**, the latter is equal to $S^{-1}M \otimes_R N$. Thus the first equality holds.

By cancellation **(8.10)**, $S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} (S^{-1}R \otimes_R N)$, and the latter is equal to $S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ by **(12.12)**. Thus the second equality holds.

Finally by **(8.8)**, the kernel of the map $S^{-1}M \otimes_R S^{-1}N \to S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ is generated by elements $(xm/s) \otimes (n/1) - (m/1) \otimes (xn/s)$ with $m \in M$, $n \in N$, $x \in R$, and $s \in S$. Those elements are zero because μ_s is an isomorphism on the $S^{-1}R$-module $S^{-1}M \otimes_R S^{-1}N$. Thus the third equality holds. □

EXERCISE **(12.24)**. — Set $R := \mathbb{Z}$ and $S = \mathbb{Z} - \langle 0 \rangle$. Set $M := \bigoplus_{n \geq 2} \mathbb{Z}/\langle n \rangle$ and $N := M$. Show that the map σ of **(12.21)** is not injective.

SOLUTION: Given $m > 0$, let e_n be the nth standard basis element for some $n > m$. Then $m \cdot e_n \neq 0$. Hence $\mu_R \colon R \to \mathrm{Hom}_R(M, M)$ is injective. But $S^{-1}M = 0$, as any $x \in M$ has only finitely many nonzero components; so $kx = 0$ for some nonzero integer k. So $\mathrm{Hom}(S^{-1}M, S^{-1}M) = 0$. Thus σ is not injective. □

13. Support

EXERCISE **(13.2)**. — Let R be a ring, $\mathfrak{p} \in \mathrm{Spec}(R)$. Show that $\mathfrak{p}$ is a closed point — that is, $\{\mathfrak{p}\}$ is a closed set — if and only if $\mathfrak{p}$ is a maximal ideal.

SOLUTION: If $\mathfrak{p}$ is maximal, then $\mathbf{V}(\mathfrak{p}) = \{\mathfrak{p}\}$; so $\mathfrak{p}$ is closed.

Conversely, suppose $\mathfrak{p}$ is not maximal. Then $\mathfrak{p} \subsetneqq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. If $\mathfrak{p} \in \mathbf{V}(\mathfrak{a})$, then $\mathfrak{m} \in \mathbf{V}(\mathfrak{a})$ too. So $\{\mathfrak{p}\} \neq \mathbf{V}(\mathfrak{a})$. Thus $\{\mathfrak{p}\}$ is not closed. □

EXERCISE **(13.4)**. — Let R be a ring, $X := \mathrm{Spec}(R)$, and U an open subset. Show U is quasi-compact if and only if $X - U = V(\mathfrak{a})$ where $\mathfrak{a}$ is finitely generated.

SOLUTION: Assume U is quasi-compact. By **(13.1)**, $U = \bigcup_\lambda \mathbf{D}(f_\lambda)$ for some f_λ. Hence $U = \bigcup_1^n \mathbf{D}(f_i)$ for some f_i. Thus $X - U = \bigcap \mathbf{V}(f_i) = \mathbf{V}(\langle f_1, \ldots, f_n \rangle)$.

Conversely, assume $X - U = \mathbf{V}(\langle f_1, \ldots, f_n \rangle)$. Then $U = \bigcup_{i=1}^n \mathbf{D}(f_i)$. By **(13.3)**, each $\mathbf{D}(f_i)$ is quasi-compact. Thus U is quasi-compact. □

EXERCISE **(13.11)**. — Let R be a ring, M a module, $\mathfrak{p} \in \mathrm{Supp}(M)$. Prove

$$\mathbf{V}(\mathfrak{p}) \subset \mathrm{Supp}(M).$$

SOLUTION: Let $\mathfrak{q} \in \mathbf{V}(\mathfrak{p})$. Then $\mathfrak{q} \supset \mathfrak{p}$. So $M_\mathfrak{p} = (M_\mathfrak{q})_\mathfrak{p}$ by **(11.25)**(1). Now, $\mathfrak{p} \in \mathrm{Supp}(M)$. So $M_\mathfrak{p} \neq 0$. Hence $M_\mathfrak{q} \neq 0$. Thus $\mathfrak{q} \in \mathrm{Supp}(M)$. □

EXERCISE **(13.12)**. — Let $\mathbb{Z}$ be the integers, $\mathbb{Q}$ the rational numbers, and set $M := \mathbb{Q}/\mathbb{Z}$. Find $\mathrm{Supp}(M)$, and show that it is not Zariski closed.

SOLUTION: Let $\mathfrak{p} \in \mathrm{Spec}(R)$. Then $M_\mathfrak{p} = \mathbb{Q}_\mathfrak{p}/\mathbb{Z}_\mathfrak{p}$ since localization is exact by **(12.16)**. Now, $\mathbb{Q}_\mathfrak{p} = \mathbb{Q}$ by **(12.4)** and **(12.1)** since $\mathbb{Q}$ is a field. If $\mathfrak{p} \neq \langle 0 \rangle$, then $\mathbb{Z}_\mathfrak{p} \neq \mathbb{Q}_\mathfrak{p}$ since $\mathfrak{p}\mathbb{Z}_\mathfrak{p} \cap \mathbb{Z} = \mathfrak{p}$ by **(11.15)**. If $\mathfrak{p} = \langle 0 \rangle$, then $\mathbb{Z}_\mathfrak{p} = \mathbb{Q}_\mathfrak{p}$. Thus $\mathrm{Supp}(M)$ consists of all the nonzero primes of $\mathbb{Z}$.

Finally, suppose $\mathrm{Supp}(M) = \mathbf{V}(\mathfrak{a})$. Then $\mathfrak{a}$ lies in every nonzero prime; so $\mathfrak{a} = \langle 0 \rangle$. But $\langle 0 \rangle$ is prime. Hence $\langle 0 \rangle \in \mathbf{V}(\mathfrak{a}) = \mathrm{Supp}(M)$, contradicting the above. Thus $\mathrm{Supp}(M)$ is not closed. □

EXERCISE **(13.14)**. — Let R be a ring, P a module, and M, N submodules. Show $M = N$ if $M_{\mathfrak{m}} = N_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. First assume $M \subset N$.

SOLUTION: If $M \subset N$, then **(12.16)** yields $(N/M)_{\mathfrak{m}} = N_{\mathfrak{m}}/M_{\mathfrak{m}} = 0$ for each $\mathfrak{m}$; so $N/M = 0$ by **(13.13)**. The general case follows by replacing N by $M + N$ owing to **(12.15)**(4), (5). □

EXERCISE **(13.15)**. — Prove these three conditions on a ring R are equivalent:

(1) R is reduced.
(2) $S^{-1}R$ is reduced for all multiplicatively closed sets S.
(3) $R_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$.

SOLUTION: Assume (1) holds. Then $\operatorname{nil}(R) = 0$. But $\operatorname{nil}(R)(S^{-1}R) = \operatorname{nil}(S^{-1}R)$ by **(11.14)**. Thus (2) holds. Trivially (2) implies (3).

Assume (3) holds. Then $\operatorname{nil}(R_{\mathfrak{m}}) = 0$. Hence $\operatorname{nil}(R)_{\mathfrak{m}} = 0$ by **(11.14)** and **(12.2)**. So $\operatorname{nil}(R) = 0$ by **(13.13)**. Thus (1) holds. □

EXERCISE **(13.16)**. — Let R be a ring, Σ the set of minimal primes. Prove this:

(1) If $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$, then the $\mathfrak{p} \in \Sigma$ are pairwise comaximal.
(2) $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$ and Σ is finite if and only if $R = \prod_{i=1}^{n} R_i$ where R_i is a domain. If so, then $R_i = R/\mathfrak{p}_i$ with $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \Sigma$.

SOLUTION: Consider (1). Suppose $\mathfrak{p}, \mathfrak{q} \in \Sigma$ are not comaximal. Then $\mathfrak{p} + \mathfrak{q}$ lies in some maximal ideal $\mathfrak{m}$. Hence $R_{\mathfrak{m}}$ contains two minimal primes, $\mathfrak{p}R_{\mathfrak{m}}$ and $\mathfrak{q}R_{\mathfrak{m}}$, by **(11.16)**. However, $R_{\mathfrak{m}}$ is a domain by hypothesis, and so $\langle 0 \rangle$ is its only minimal prime. Hence $\mathfrak{p}R_{\mathfrak{m}} = \mathfrak{q}R_{\mathfrak{m}}$. So $\mathfrak{p} = \mathfrak{q}$. Thus (1) holds.

Consider (2). Assume $R_{\mathfrak{p}}$ is a domain for any $\mathfrak{p}$. Then R is reduced by **(13.15)**. Assume, also, Σ is finite. Form the canonical map $\varphi\colon R \to \prod_{\mathfrak{p} \in \Sigma} R/\mathfrak{p}$; it is injective by **(3.22)**, and surjective by (1) and the Chinese Remainder Theorem **(1.12)**. Thus R is a finite product of domains.

Conversely, assume $R = \prod_{i=1}^{n} R_i$ where R_i is a domain. Let $\mathfrak{p}$ be a prime of R. Then $R_{\mathfrak{p}} = \prod (R_i)_{\mathfrak{p}}$ by **(12.10)**. Each $(R_i)_{\mathfrak{p}}$ is a domain by **(11.3)**. But $R_{\mathfrak{p}}$ is local. So $R_{\mathfrak{p}} = (R_i)_{\mathfrak{p}}$ for some i by **(2.5)**. Thus $R_{\mathfrak{p}}$ is a domain. Further, owing to **(2.11)**, each $\mathfrak{p}_i \in \Sigma$ has the form $\mathfrak{p}_i = \prod \mathfrak{a}_j$ where, after renumbering, $\mathfrak{a}_i = \langle 0 \rangle$ and $\mathfrak{a}_j = R_j$ for $j \neq i$. Thus the ith projection gives $R/\mathfrak{p}_i \xrightarrow{\sim} R_i$. Thus (2) holds. □

EXERCISE **(13.18)**. — Let R be a ring, M a module. Prove elements $m_\lambda \in M$ generate M if and only if, at every maximal ideal $\mathfrak{m}$, their images m_λ generate $M_{\mathfrak{m}}$.

SOLUTION: The m_λ define a map $\alpha\colon R^{\oplus\{\lambda\}} \to M$. By **(13.17)**, it is surjective if and only if $\alpha_{\mathfrak{m}}\colon \left(R^{\oplus\{\lambda\}}\right)_{\mathfrak{m}} \to M_{\mathfrak{m}}$ is surjective for all $\mathfrak{m}$. But $\left(R^{\oplus\{\lambda\}}\right)_{\mathfrak{m}} = R_{\mathfrak{m}}^{\oplus\{\lambda\}}$ by **(12.10)**. Hence **(4.10)**(1) yields the assertion. □

EXERCISE **(13.23)**. — Given n, prove an R-module P is locally free of rank n if and only if P is finitely generated and $P_{\mathfrak{m}} \simeq R_{\mathfrak{m}}^n$ holds at each maximal ideal $\mathfrak{m}$.

SOLUTION: If P is locally free of rank n, then P is finitely generated by **(13.22)**. Also, for any $\mathfrak{p} \in \operatorname{Spec}(R)$, there's $f \in R - \mathfrak{p}$ with $P_f \simeq R_f^n$; so $P_{\mathfrak{p}} \simeq R_{\mathfrak{p}}^n$ by **(12.5)**.

As to the converse, given any prime $\mathfrak{p}$, take a maximal ideal $\mathfrak{m}$ containing it. Assume $P_{\mathfrak{m}} \simeq R_{\mathfrak{m}}^n$. Take a free basis $p_1/f_1^{k_1}, \dots, p_n/f_n^{k_n}$ of $P_{\mathfrak{m}}$ over $R_{\mathfrak{m}}$. The p_i define a map $\alpha\colon R^n \to P$, and $\alpha_{\mathfrak{m}}\colon R_{\mathfrak{m}}^n \to P_{\mathfrak{m}}$ is bijective, so surjective.

Assume P is finitely generated. Then **(12.20)**(1) provides $f \in R - \mathfrak{m}$ such that

$\alpha_f\colon R_f^n \to P_f$ is surjective. Hence $\alpha_{\mathfrak{q}}\colon R_{\mathfrak{q}}^n \to P_{\mathfrak{q}}$ is surjective for every $\mathfrak{q} \in \mathbf{D}(f)$ by **(12.5)** and **(12.16)**. Assume $P_{\mathfrak{q}} \simeq R_{\mathfrak{q}}^n$ if also $\mathfrak{q}$ is maximal. So $\alpha_{\mathfrak{q}}$ is bijective by **(10.4)**. Clearly, $\alpha_{\mathfrak{q}} = (\alpha_f)_{(\mathfrak{q}R_f)}$. Hence $\alpha_f\colon R_f^n \to P_f$ is bijective owing to **(13.17)** with R_f for R, as desired. □

14. Krull–Cohen–Seidenberg Theory

Exercise **(14.4)**. — Let $R \subset R'$ be an integral extension of rings, and $\mathfrak{p}$ a prime of R. Suppose R' has just one prime $\mathfrak{p}'$ over $\mathfrak{p}$. Show (a) that $\mathfrak{p}'R'_{\mathfrak{p}}$ is the only maximal ideal of $R'_{\mathfrak{p}}$, (b) that $R'_{\mathfrak{p}'} = R'_{\mathfrak{p}}$, and (c) that $R'_{\mathfrak{p}'}$ is integral over $R_{\mathfrak{p}}$.

Solution: Since R' is integral over R, the localization $R'_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$ by **(11.20)**. Moreover, $R_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ by **(11.18)**. Hence, every maximal ideal of $R'_{\mathfrak{p}}$ lies over $\mathfrak{p}R_{\mathfrak{p}}$ by **(14.3)**(1). But every maximal ideal of $R'_{\mathfrak{p}}$ is the extension of some prime $\mathfrak{q}' \subset R'$ by **(11.16)**(2), and therefore $\mathfrak{q}'$ lies over $\mathfrak{p}$ in R. So, by hypothesis, $\mathfrak{q}' = \mathfrak{p}'$. Thus $\mathfrak{p}'R'_{\mathfrak{p}}$ is the only maximal ideal of $R'_{\mathfrak{p}}$; that is, (a) holds. So $R'_{\mathfrak{p}} - \mathfrak{p}'R'_{\mathfrak{p}}$ consists of units. Hence **(11.25)** and **(11.6)** yield (b). But $R'_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$; so (c) holds too. □

Exercise **(14.5)**. — Let $R \subset R'$ be an integral extension of domains, and $\mathfrak{p}$ a prime of R. Suppose R' has at least two distinct primes $\mathfrak{p}'$ and $\mathfrak{q}'$ lying over $\mathfrak{p}$. Show that $R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$. Show that, in fact, if y lies in $\mathfrak{q}'$, but not in $\mathfrak{p}'$, then $1/y \in R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$.

Solution: Suppose $1/y$ is integral over $R_{\mathfrak{p}}$. Say

$$(1/y)^n + a_1(1/y)^{n-1} + \cdots + a_n = 0$$

with $n \geq 1$ and $a_i \in R_{\mathfrak{p}}$. Multiplying by y^{n-1}, we obtain

$$1/y = -(a_1 + \cdots + a_n y^{n-1}) \in R'_{\mathfrak{p}}.$$

However, $y \in \mathfrak{q}'$, so $y \in \mathfrak{q}'R'_{\mathfrak{p}}$. Hence $1 \in \mathfrak{q}'R'_{\mathfrak{p}}$. So $\mathfrak{q}' \cap (R - \mathfrak{p}) \neq \emptyset$ by **(11.15)**(3). But $\mathfrak{q}' \cap R = \mathfrak{p}$, a contradiction. So $1/y$ is not integral over $R_{\mathfrak{p}}$. □

Exercise **(14.6)**. — Let k be a field, and X an indeterminate. Set $R' := k[X]$, and $Y := X^2$, and $R := k[Y]$. Set $\mathfrak{p} := (Y-1)R$ and $\mathfrak{p}' := (X-1)R'$. Is $R'_{\mathfrak{p}'}$ integral over $R_{\mathfrak{p}}$? Explain.

Solution: Note that R' is a domain, and that the extension $R \subset R'$ is integral as R' is generated by 1 and X as an R-module.

Suppose the characteristic is not 2. Set $\mathfrak{q}' := (X+1)R'$. Then both $\mathfrak{p}'$ and $\mathfrak{q}'$ contain $Y - 1$, so lie over the maximal ideal $\mathfrak{p}$ of R. Further $X + 1$ lies in $\mathfrak{q}'$, but not in $\mathfrak{p}'$. Hence $R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$ by **(14.5)**.

Suppose the characteristic is 2. Then $(X-1)^2 = Y - 1$. Let $\mathfrak{q}' \subset R'$ be a prime over $\mathfrak{p}$. Then $(X-1)^2 \in \mathfrak{q}'$. So $\mathfrak{p}' \subset \mathfrak{q}'$. But $\mathfrak{p}'$ is maximal. So $\mathfrak{q}' = \mathfrak{p}'$. Thus R' has just one prime $\mathfrak{p}'$ over $\mathfrak{p}$. Hence $R'_{\mathfrak{p}'}$ is integral over $R_{\mathfrak{p}}$ by **(14.4)**. □

Exercise **(14.12)**. — Let R be a reduced ring, Σ the set of minimal primes. Prove that $\operatorname{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ and that $R_{\mathfrak{p}} = \operatorname{Frac}(R/\mathfrak{p})$ for any $\mathfrak{p} \in \Sigma$.

Solution: If $\mathfrak{p} \in \Sigma$, then $\mathfrak{p} \subset \operatorname{z.div}(R)$ by **(14.10)**. Thus $\operatorname{z.div}(R) \supset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Conversely, say $xy = 0$. If $x \notin \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $y \in \mathfrak{p}$. So if $x \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, then $y \in \bigcap_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. But $\bigcap_{\mathfrak{p}\in\Sigma} \mathfrak{p} = \langle 0\rangle$ by the Scheinnullstellensatz **(3.17)** and **(3.11)**. So $y = 0$. Hence if $x \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, then $x \notin \text{z.div}(R)$. Thus $\text{z.div}(R) \subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Thus $\text{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Fix $\mathfrak{p} \in \Sigma$. Then $R_\mathfrak{p}$ is reduced by **(13.15)**. Further, $R_\mathfrak{p}$ has only one prime, namely $\mathfrak{p}R_\mathfrak{p}$, by **(11.16)**(2). Hence $R_\mathfrak{p}$ is a field, and $\mathfrak{p}R_\mathfrak{p} = \langle 0\rangle$. But by **(12.19)**, $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \text{Frac}(R/\mathfrak{p})$. Thus $R_\mathfrak{p} = \text{Frac}(R/\mathfrak{p})$. □

Exercise **(14.13)**. — Let R be a ring, Σ the set of minimal primes, and K the total quotient ring. Assume Σ is finite. Prove these three conditions are equivalent:

(1) R is reduced.
(2) $\text{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, and $R_\mathfrak{p} = \text{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$.
(3) $K/\mathfrak{p}K = \text{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$, and $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$.

Solution: Assume (1) holds. Then **(14.12)** yields (2).

Assume (2) holds. Set $S := R - \text{z.div}(R)$. Let $\mathfrak{q}$ be a prime of R with $\mathfrak{q} \cap S = \emptyset$. Then $\mathfrak{q} \subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. But Σ is finite. So $\mathfrak{q} \subset \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$ by Prime Avoidance **(3.12)**. Hence $\mathfrak{q} = \mathfrak{p}$ since $\mathfrak{p}$ is minimal. But $K = S^{-1}R$. Therefore, by **(11.16)**(2), for $\mathfrak{p} \in \Sigma$, the extensions $\mathfrak{p}K$ are the only primes of K, and they all are both maximal and minimal.

Fix $\mathfrak{p} \in \Sigma$. Then $K/\mathfrak{p}K = S^{-1}(R/\mathfrak{p})$ by **(12.18)**. So $S^{-1}(R/\mathfrak{p})$ is a field. But clearly $S^{-1}(R/\mathfrak{p}) \subset \text{Frac}(R/\mathfrak{p})$. Therefore, $K/\mathfrak{p}K = \text{Frac}(R/\mathfrak{p})$ by **(2.3)**. Further, $S \subset R - \mathfrak{p}$. Hence **(11.16)**(2) yields $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{p}K)$. Therefore, $\varphi_S^{-1}(K - \mathfrak{p}K) = R - \mathfrak{p}$. So $K_{\mathfrak{p}K} = R_\mathfrak{p}$ by **(11.23)**. But $R_\mathfrak{p} = \text{Frac}(R/\mathfrak{p})$ by hypothesis. Thus K has only finitely many primes, the $\mathfrak{p}K$; each $\mathfrak{p}K$ is minimal, and each $K_{\mathfrak{p}K}$ is a domain. Therefore, **(13.16)**(2) yields $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$. Thus (3) holds.

Assume (3) holds. Then K is a finite product of fields, and fields are reduced. But clearly, a product of reduced ring is reduced. Further, $R \subset K$, and trivially, a subring of a reduced ring is reduced. Thus (1) holds. □

Exercise **(14.15)**. — Let R be a ring, $\mathfrak{p}_1 \ldots, \mathfrak{p}_r$ all its minimal primes, and K the total quotient ring. Prove that these three conditions are equivalent:

(1) R is normal.
(2) R is reduced and integrally closed in K.
(3) R is a finite product of normal domains R_i.

If so, then the R_i are equal to the $R/\mathfrak{p}_j$ up to order.

Solution: Assume (1). Then R is reduced by **(13.15)**. Let $x \in K$ be integral over R, and $\mathfrak{m}$ any maximal ideal. Then $x/1$ is integral over $R_\mathfrak{m}$. So $x/1 \in R_\mathfrak{m}$ by hypothesis. Hence $(R[x]/R)_\mathfrak{m} = 0$. Therefore, $R[x]/R = 0$ by **(13.13)**. So $x \in R$ Thus (2) holds.

Assume (2). Set $R_i := R/\mathfrak{p}_i$ and $K_i := \text{Frac}(R_i)$. Then $K = \prod K_i$ by **(14.13)**. Let R_i' be the normalization of R_i. Then $R \subset \prod R_i \subset \prod R_i'$. Further, the first extension is integral by **(10.21)**, and the second, by **(10.23)**; whence, $R \subset \prod R_i'$ is integral by the tower property **(10.19)**. However, R is integrally closed in K by hypothesis. Hence $R = \prod R_i = \prod R_i'$. Thus (3) and the last assertion hold.

Assume (3). Let $\mathfrak{p}$ be any prime of R. Then $R_\mathfrak{p} = \prod (R_i)_\mathfrak{p}$ by **(12.10)**, and each $(R_i)_\mathfrak{p}$ is normal by **(11.28)**. But $R_\mathfrak{p}$ is local. So $R_\mathfrak{p} = (R_i)_\mathfrak{p}$ for some i by **(3.5)**. Hence $R_\mathfrak{p}$ is a normal domain. Thus (1) holds. □

15. Noether Normalization

EXERCISE **(15.2)**. — Let $k := \mathbb{F}_q$ be the finite field with q elements, and $k[X, Y]$ the polynomial ring. Set $f := X^qY - XY^q$ and $R := k[X, Y]/\langle f\rangle$. Let x, $y \in R$ be the residues of X, Y. For every $a \in k$, show that R is not module finite over $P := k[y-ax]$. (Thus, in **(15.1)**, no k-linear combination works.) First, take $a = 0$.

SOLUTION: Take $a = 0$. Then $P = k[y]$. Any algebraic relation over P satisfied by x is given by a polynomial in $k[X, Y]$, which is a multiple of f. However, no multiple of f is monic in X. So x is not integral over P. By **(10.15)**, R is not module finite over P.

Consider an arbitrary a. Since $a^q = a$, after the change of variable $Y' := Y - aX$, our f still has the same form. Thus, we have reduced to the previous case. □

EXERCISE **(15.3)**. — Let k be a field, and X, Y, Z variables. Set

$$R := k[X, Y, Z]/\langle X^2 - Y^3 - 1, XZ - 1\rangle,$$

and let x, y, $z \in R$ be the residues of X, Y, Z. Fix $a, b \in k$, and set $t := x + ay + bz$ and $P := k[t]$. Show that x and y are integral over P for any a, b and that z is integral over P if and only if $b \neq 0$.

SOLUTION: To see x is integral, notice $xz = 1$, so $x^2 - tx + b = -axy$. Raising both sides of the latter equation to the third power, and using the equation $y^3 = x^2 - 1$, we obtain an equation of integral dependence of degree 6 for x over P. Now, $y^3 - x^2 - 1 = 0$, so y is integral over $P[x]$. Hence, the Tower Property, **(10.19)**, implies that y too is integral over P.

If $b \neq 0$, then $z = b^{-1}(t - x - ay) \in P[x, y]$, and so z is integral over P by **(10.20)**.

Assume $b = 0$ and z is integral over P. Now, $P \subset k[x, y]$. So z is integral over $k[x, y]$ as well. But $y^3 - x^2 + 1 = 0$. So y is integral over $k[x]$. Hence z is too. However, $k[x]$ is a polynomial ring, so integrally closed in its fraction field $k(x)$ by **(10.26)**(1). Moreover, $z = 1/x \in k(x)$. Hence, $1/x \in k[x]$, which is absurd. Thus z is not integral over P if $b = 0$. □

EXERCISE **(15.7)**. — Let k be a field, K an algebraically closed extension field. (So K contains a copy of every finite extension field.) Let $P := k[X_1, \dots, X_n]$ be the polynomial ring, and $f, f_1, \dots, f_r \in P$. Assume f vanishes at every zero in K^n of $f_1, \dots, f_r$; in other words, if $(a) := (a_1, \dots, a_n) \in K^n$ and $f_1(a) = 0, \dots, f_r(a) = 0$, then $f(a) = 0$ too. Prove that there are polynomials $g_1, \dots, g_r \in P$ and an integer N such that $f^N = g_1f_1 + \cdots + g_rf_r$.

SOLUTION: Set $\mathfrak{a} := \langle f_1, \dots, f_r\rangle$. We have to show $f \in \sqrt{\mathfrak{a}}$. But, by the Hilbert Nullstellensatz, $\sqrt{\mathfrak{a}}$ is equal to the intersection of all the maximal ideals $\mathfrak{m}$ containing $\mathfrak{a}$. So given an $\mathfrak{m}$, we have to show that $f \in \mathfrak{m}$.

Set $L := P/\mathfrak{m}$. By the weak Nullstellensatz, L is a finite extension field of k. So we may embed L/k as a subextension of K/k. Let $a_i \in K$ be the image of the variable $X_i \in P$, and set $(a) := (a_1, \dots, a_n) \in K^n$. Then $f_1(a) = 0, \dots, f_r(a) = 0$. Hence $f(a) = 0$ by hypothesis. Therefore, $f \in \mathfrak{m}$, as desired. □

EXERCISE **(15.10)**. — Let R be a domain of (finite) dimension r, and $\mathfrak{p}$ a nonzero prime. Prove that $\dim(R/\mathfrak{p}) < r$.

SOLUTION: Every chain of primes of $R/\mathfrak{p}$ is of the form $\mathfrak{p}_0/\mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p}_s/\mathfrak{p}$ where $0 \subsetneqq \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_s$ is a chain of primes of R. So $s < r$. Thus $\dim(R/\mathfrak{p}) < r$. □

EXERCISE **(15.11)**. — Let R'/R be an integral extension of rings. Prove that $\dim(R) = \dim(R')$.

SOLUTION: Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes of R. Set $\mathfrak{p}'_{-1} := 0$. Given $\mathfrak{p}'_{i-1}$ for $0 \le i \le r$, Going up, **(14.3)**(4), yields a prime $\mathfrak{p}'_i$ of R' with $\mathfrak{p}'_{i-1} \subset \mathfrak{p}'_i$ and $\mathfrak{p}'_i \cap R = \mathfrak{p}_i$. Then $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ as $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$. Thus $\dim(R) \le \dim(R')$.

Conversely, let $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ be a chain of primes of R'. Set $\mathfrak{p}_i := \mathfrak{p}'_i \cap R$. Then $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ by Incomparability, **(14.3)**(2). Thus $\dim(R) \ge \dim(R')$. □

EXERCISE **(15.16)**. — Let k be a field, R a finitely generated k-algebra, $f \in R$ nonzero. Assume R is a domain. Prove that $\dim(R) = \dim(R_f)$.

SOLUTION: Note that R_f is a finitely generated R-algebra by **(11.10)**, as R_f is, by **(11.10)**, obtained by adjoining $1/f$. So since R is a finitely generated k-algebra, R_f is one too. Moreover, R and R_f have the same fraction field K. Hence both $\dim(R)$ and $\dim(R_f)$ are equal to $\mathrm{tr.deg}_k(K)$ by **(15.12)**. □

EXERCISE **(15.17)**. — Let k be a field, $P := k[f]$ the polynomial ring in one variable f. Set $\mathfrak{p} := \langle f \rangle$ and $R := P_{\mathfrak{p}}$. Find $\dim(R)$ and $\dim(R_f)$.

SOLUTION: In P, the chain of primes $0 \subset \mathfrak{p}$ is of maximal length by **(2.6)** and **(2.20)** or **(15.12)**. So $\langle 0 \rangle$ and $\mathfrak{p}R$ are the only primes in R by **(11.16)**. Thus $\dim(R) = 1$.

Set $K := \mathrm{Frac}(P)$. Then $R_f = K$ since, if $a/(bf^n) \in K$ with $a, b \in P$ and $f \nmid b$, then $a/b \in R$ and so $(a/b)/f^n \in R_f$. Thus $\dim(R_f) = 0$. □

16. Chain Conditions

EXERCISE **(16.2)**. — Let $\mathfrak{a}$ be a finitely generated ideal in an arbitrary ring. Show every set that generates $\mathfrak{a}$ contains a finite subset that generates $\mathfrak{a}$.

SOLUTION: Say $\mathfrak{a}$ is generated by $x_1, \ldots, x_r$ and also by the y_λ for $\lambda \in \Lambda$. Write $x_i = \sum_j z_j y_{\lambda_{ij}}$. Then the $y_{\lambda_{ij}}$ generate $\mathfrak{a}$. □

EXERCISE **(16.8)**. — Let R be a ring, X a variable, $R[X]$ the polynomial ring. Prove this statement or find a counterexample: if $R[X]$ is Noetherian, then so is R.

SOLUTION: It's true. Since $R[X]$ is Noetherian, so is $R[X]/\langle X \rangle$ by **(16.7)**. But the latter ring is isomorphic to R by **(1.6)**; so R is Noetherian. □

EXERCISE **(16.14)**. — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence of R-modules, and M_1, M_2 two submodules of M. Prove or give a counterexample to this statement: if $\beta(M_1) = \beta(M_2)$ and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2)$, then $M_1 = M_2$.

SOLUTION: The statement is false: form the exact sequence

$$0 \to \mathbb{R} \xrightarrow{\alpha} \mathbb{R} \oplus \mathbb{R} \xrightarrow{\beta} \mathbb{R} \to 0$$

with $\alpha(r) := (r, 0)$ and $\beta(r, s) := s$, and take

$$M_1 := \{(t, 2t) \mid t \in \mathbb{R}\} \quad \text{and} \quad M_2 := \{(2t, t) \mid t \in \mathbb{R}\}.$$

(Geometrically, we can view M_1 as the line determined by the origin and the point $(1, 2)$, and M_2 as the line determined by the origin and the point $(2, 1)$. Then $\beta(M_1) = \beta(M_2) = \mathbb{R}$, and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2) = 0$, but $M_1 \neq M_2$ in $\mathbb{R} \oplus \mathbb{R}$.) □

EXERCISE **(16.17)**. — Let R be a ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ideals such that each $R/\mathfrak{a}_i$ is a Noetherian ring. Prove (1) that $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module, and (2) that, if $\bigcap \mathfrak{a}_i = 0$, then R too is a Noetherian ring.

SOLUTION: Any R-submodule of $R/\mathfrak{a}_i$ is an ideal of $R/\mathfrak{a}_i$. Since $R/\mathfrak{a}_i$ is a Noetherian ring, such an ideal is finitely generated as an $(R/\mathfrak{a}_i)$-module, so as an R-module as well. Thus $R/\mathfrak{a}_i$ is a Noetherian R-module. So $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module by **(16.16)**. Thus (1) holds.

To prove (2), note that the kernel of the natural map $R \to \bigoplus R/\mathfrak{a}_i$ is $\bigcap \mathfrak{a}_i$, which is 0 by hypothesis. So R can be identified with a submodule of the Noetherian R-module $\bigoplus R/\mathfrak{a}_i$. Hence R itself is a Noetherian R-module by **(16.15)**(2). So R is a Noetherian ring by **(16.12)**. □

EXERCISE **(16.20)**. — Let G be a finite group acting on a domain R, and R' the subring of invariants. Let $k \subset R'$ be a field. Using **(10.14)**, prove this celebrated theorem of E. Noether (1926): if R is algebra finite over k, then so is R'.

SOLUTION: By **(10.14)**, R is integral over R''. But it's algebra finite. So it's module finite by **(10.20)**. Hence **(16.19)** yields the assertion. □

EXERCISE **(16.24)**. — Let k be a field, R an algebra. Assume that R is finite dimensional as a k-vector space. Prove that R is Noetherian and Artinian.

SOLUTION: View R as a vector space, and ideals as subspaces. Now, by a simple dimension argument, any ascending or descending chain of subspaces of R stabilizes. Thus R is Noetherian by **(16.5)** and is Artinian by definition. □

EXERCISE **(16.25)**. — Let p be a prime number, and set $M := \mathbb{Z}[1/p]/\mathbb{Z}$. Prove that any $\mathbb{Z}$-submodule $N \subset M$ is either finite or all of M. Deduce that M is an Artinian $\mathbb{Z}$-module, and that it is not Noetherian.

SOLUTION: Given $q \in N$, write $q = n/p^e$ where n is relatively prime to p. Then there is an $m \in \mathbb{Z}$ with $nm \equiv 1 \pmod{p^e}$. Hence $N \ni m(n/p^e) = 1/p^e$, and so $1/p^r = p^{e-r}(1/p^e) \in N$ for any $0 \leq r \leq e$. Therefore, either $N = M$, or there is a largest integer $e \geq 0$ with $1/p^e \in N$. In the second case, N is finite.

Let $M \supsetneq N_1 \supset N_2 \supset \cdots$ be a descending chain. By what we just proved, each N_i is finite, say with n_i elements. Then the sequence $n_1 \geq n_2 \geq \cdots$ stabilizes; say $n_i = n_{i+1} = \cdots$. But $N_i \supset N_{i+1} \supset \cdots$, so $N_i = N_{i+1} = \cdots$. Thus M is Artinian.

Finally, suppose $m_1, \ldots, m_r$ generate M, say $m_i = n_i/p^{e_i}$. Set $e := \max e_i$. Then $1/p^e$ generates M, a contradiction since $1/p^{e+1} \in M$. Thus M is not finitely generated, and so not Noetherian. □

EXERCISE **(16.26)**. — Let R be an Artinian ring. Prove that R is a field if it is a domain. Deduce that in general every prime ideal $\mathfrak{p}$ of R is maximal.

SOLUTION: Take any nonzero element $x \in R$, and consider the chain of ideals $\langle x\rangle \supset \langle x^2\rangle \supset \cdots$. Since R is Artinian, the chain stabilizes; so $\langle x^e\rangle = \langle x^{e+1}\rangle$ for some e. Hence $x^e = ax^{e+1}$ for some $a \in R$. If R is a domain, then we can cancel to get $1 = ax$; thus R is then a field.

In general, $R/\mathfrak{p}$ is Artinian by **(16.23)**(2). Now, $R/\mathfrak{p}$ is also a domain by **(2.9)**. Hence, by what we just proved, $R/\mathfrak{p}$ is a field. Thus $\mathfrak{p}$ is maximal by **(2.16)**. □

17. Associated Primes

EXERCISE **(17.6)**. — Given modules $M_1, \dots, M_r$, set $M := M_1 \oplus \cdots \oplus M_r$. Prove

$$\operatorname{Ass}(M) = \operatorname{Ass}(M_1) \cup \cdots \cup \operatorname{Ass}(M_r).$$

SOLUTION: Set $N := M_2 \oplus \cdots \oplus M_r$. Then N, $M_1 \subset M$. Also, $M/N = M_1$. So **(17.5)** yields

$$\operatorname{Ass}(N),\ \operatorname{Ass}(M_1) \subset \operatorname{Ass}(M) \subset \operatorname{Ass}(N) \cup \operatorname{Ass}(M_1).$$

So $\operatorname{Ass}(M) = \operatorname{Ass}(N) \cup \operatorname{Ass}(M_1)$. The assertion follows by induction on r. □

EXERCISE **(17.7)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 2\rangle \oplus \mathbb{Z}$. Find $\operatorname{Ass}(M)$ and find two submodules L, $N \subset M$ with $L + N = M$ but $\operatorname{Ass}(L) \cup \operatorname{Ass}(N) \subsetneqq \operatorname{Ass}(M)$.

SOLUTION: First, we have $\operatorname{Ass}(M) = \{\langle 0\rangle, \langle 2\rangle\}$ by **(17.6)** and **(17.4)**(2). Next, take $L := R\cdot(1,1)$ and $N := R\cdot(0,1)$. Then the canonical maps $\mathbb{Z} \to L$ and $\mathbb{Z} \to N$ are isomorphisms. Hence both $\operatorname{Ass}(L)$ and $\operatorname{Ass}(N)$ are $\{\langle 0\rangle\}$ by **(17.4)**(2). Finally, $L + N = M$ because $(a, b) = a \cdot (1, 1) + (b - a) \cdot (0, 1)$. □

EXERCISE **(17.10)**. — Let R be a ring, and suppose $R_{\mathfrak{p}}$ is a domain for every prime $\mathfrak{p}$. Prove every associated prime of R is minimal.

SOLUTION: Let $\mathfrak{p} \in \operatorname{Ass}(R)$. Then $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}(R_{\mathfrak{p}})$ by **(17.9)**. By hypothesis, $R_{\mathfrak{p}}$ is a domain. So $\mathfrak{p}R_{\mathfrak{p}} = \langle 0\rangle$ by **(17.4)**. Hence $\mathfrak{p}$ is a minimal prime of R by **(11.16)**(2).

Alternatively, say $\mathfrak{p} = \operatorname{Ann}(x)$ with $x \in R$. Then $x/1 \neq 0$ in $R_{\mathfrak{p}}$; otherwise, there would be some $s \in R - \mathfrak{p}$ such that $sx = 0$, contradicting $\mathfrak{p} = \operatorname{Ann}(x)$. However, for any $y \in \mathfrak{p}$, we have $xy/1 = 0$ in $R_{\mathfrak{p}}$. Since $R_{\mathfrak{p}}$ is a domain and since $x/1 \neq 0$, we must have $y/1 = 0$ in $R_{\mathfrak{p}}$. So there exists some $t \in R - \mathfrak{p}$ such that $ty = 0$. Now, $\mathfrak{p} \supset \mathfrak{q}$ for some minimal prime $\mathfrak{q}$ by **(3.11)**. Suppose $\mathfrak{p} \neq \mathfrak{q}$. Then there is some $y \in \mathfrak{p} - \mathfrak{q}$. So there exists some $t \in R - \mathfrak{p}$ such that $ty = 0 \in \mathfrak{q}$, contradicting the primeness of $\mathfrak{q}$. Thus $\mathfrak{p} = \mathfrak{q}$; that is, $\mathfrak{p}$ is minimal. □

EXERCISE **(17.15)**. — Let R be a Noetherian ring, M a module, N a submodule, $x \in R$. Show that, if $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Ass}(M/N)$, then $xM \cap N = xN$.

SOLUTION: Trivially, $xN \subset xM \bigcap N$. Conversely, take $m \in M$ with $xm \in N$. Let m' be the residue of m in M/N. Then $xm' = 0$. By **(17.14)**, $x \notin \text{z.div}(M/N)$. So $m' = 0$. So $m \in N$. So $xm \in xN$. Thus $xM \bigcap N \subset xN$, as desired. □

EXERCISE **(17.21)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Prove the primes minimal containing $\mathfrak{a}$ are associated to $\mathfrak{a}$. Prove such primes are finite in number.

SOLUTION: Since $\mathfrak{a} = \operatorname{Ann}(R/\mathfrak{a})$, the primes in question are the primes minimal in $\operatorname{Supp}(R/\mathfrak{a})$ by **(13.6)**(3). So they are associated to $\mathfrak{a}$ by **(17.17)**, and they are finite in number by **(17.20)**. □

EXERCISE **(17.22)**. — Take $R := \mathbb{Z}$ and $M := Z$ in **(17.19)**. Determine when a chain $0 \subset M_1 \subsetneqq M$ is acceptable, and show that then $\mathfrak{p}_2 \notin \operatorname{Ass}(M)$.

SOLUTION: If the chain is acceptable, then $M_1 \neq 0$ as $M_1/0 \simeq R/\mathfrak{p}_1$, and M_1 is a prime ideal as $M_1 = \operatorname{Ann}(M/M_1) = \mathfrak{p}_2$. Conversely, the chain is acceptable if M_1 is a nonzero prime ideal $\mathfrak{p}$, as then $M_1/0 \simeq R/0$ and $M/M_1 \simeq R/\mathfrak{p}$.

Finally, $\operatorname{Ass}(M) = 0$ by **(17.4)**. Further, as just observed, given any acceptable chain, $\mathfrak{p}_2 = M_1 \neq 0$. So $\mathfrak{p}_2 \notin \operatorname{Ass}(M)$. □

EXERCISE **(17.23)**. — Take $R := \mathbb{Z}$ and $M := Z/\langle 12\rangle$ in **(17.19)**. Find all three acceptable chains, and show that, in each case, $\{\mathfrak{p}_i\} = \operatorname{Ass}(M)$.

SOLUTION: An acceptable chain in M corresponds to chain

$$\langle 12\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle = \mathbb{Z}.$$

Here $\langle a_1\rangle/\langle 12\rangle \simeq \mathbb{Z}/\langle p_1\rangle$ with p_1 prime. So $a_1p_1 = 12$. Hence the possibilities are $p_1 = 2$, $a_1 = 6$ and $p_1 = 3$, $a_1 = 4$. Further, $\langle a_2\rangle/\langle a_1\rangle \simeq \mathbb{Z}/\langle p_2\rangle$ with p_2 prime. So $a_2p_2 = a_1$. Hence, if $a_1 = 6$, then the possibilities are $p_2 = 2$, $a_2 = 3$ and $p_2 = 3$, $a_2 = 2$; if $a_1 = 4$, then the only possibility is $p_2 = 2$ and $a_2 = 2$. In each case, a_2 is prime; hence, $n = 3$, and these three chains are the only possibilities. Conversely, each of these three possibilities, clearly, does arise.

In each case, $\{\mathfrak{p}_i\} = \{\langle 2\rangle, \langle 3\rangle\}$. Hence **(17.19.1)** yields $\operatorname{Ass}(M) \subset \{\langle 2\rangle, \langle 3\rangle\}$. For any M, if $0 \subset M_1 \subset \cdots \subset M$ is an acceptable chain, then **(17.5)** and **(17.4)**(2) yield $\operatorname{Ass}(M) \supset \operatorname{Ass}(M_1) = \{\mathfrak{p}_1\}$. Here, there's one chain with $\mathfrak{p}_1 = \langle 2\rangle$ and another with $\mathfrak{p}_1 = \langle 3\rangle$; hence, $\operatorname{Ass}(M) \supset \{\langle 2\rangle, \langle 3\rangle\}$. Thus $\operatorname{Ass}(M) = \{\langle 2\rangle, \langle 3\rangle\}$. □

18. Primary Decomposition

EXERCISE **(18.6)**. — Let R be a ring, and $\mathfrak{p} = \langle p\rangle$ a principal prime generated by a nonzerodivisor p. Show every positive power $\mathfrak{p}^n$ is $\mathfrak{p}$-primary, and conversely, if R is Noetherian, then every $\mathfrak{p}$-primary ideal $\mathfrak{q}$ is equal to some power $\mathfrak{p}^n$.

SOLUTION: Let's proceed by induction. Form the exact sequence

$$0 \to \mathfrak{p}^n/\mathfrak{p}^{n+1} \to R/\mathfrak{p}^{n+1} \to R/\mathfrak{p}^n \to 0.$$

Consider the map $R \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ given by $x \mapsto xp^n$. It is surjective, and its kernel is $\mathfrak{p}$ as p is a nonzerodivisor. Hence $R/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^n/\mathfrak{p}^{n+1}$. But $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by **(17.4)**(2). Hence **(17.5)** yields $\operatorname{Ass}(R/\mathfrak{p}^n) = \{\mathfrak{p}\}$ for every $n \geq 1$, as desired.

Conversely, $\mathfrak{p} = \sqrt{\mathfrak{q}}$ by **(18.5)**. So $p^n \in \mathfrak{q}$ for some n; take n minimal. Then $\mathfrak{p}^n \subset \mathfrak{q}$. Suppose there is an $x \in \mathfrak{q} - \mathfrak{p}^n$. Say $x = yp^m$ for some y and $m \geq 0$. Then $m < n$ as $x \notin \mathfrak{p}^n$. Take m maximal. Now, $p^m \notin \mathfrak{q}$ as n is minimal. So **(18.5)** yields $y \in \mathfrak{q} \subset \mathfrak{p}$. Hence $y = zp$ for some z. Then $x = zp^{m+1}$, contradicting the maximality of m. Thus $\mathfrak{q} = \mathfrak{p}^n$. □

EXERCISE **(18.7)**. — Let k be a field, and $k[X, Y]$ the polynomial ring. Let $\mathfrak{a}$ be the ideal $\langle X^2, XY\rangle$. Show $\mathfrak{a}$ is not primary, but $\sqrt{\mathfrak{a}}$ is prime. Show $\mathfrak{a}$ satisfies this condition: $ab \in \mathfrak{a}$ implies $a^2 \in \mathfrak{a}$ or $b^2 \in \mathfrak{a}$.

SOLUTION: First, $\langle X\rangle$ is prime by **(2.10)**. But $\langle X^2\rangle \subset \mathfrak{a} \subset \langle X\rangle$. So $\sqrt{\mathfrak{a}} = \langle X\rangle$ by **(3.20)**. On the other hand, $XY \in \mathfrak{a}$, but $X \notin \mathfrak{a}$ and $Y \notin \sqrt{\mathfrak{a}}$; thus $\mathfrak{a}$ is not primary by **(18.5)**. If $ab \in \mathfrak{a}$, then $X \mid a$ or $X \mid b$, so $a^2 \in \mathfrak{a}$ or $b^2 \in \mathfrak{a}$. □

EXERCISE **(18.8)**. — Let $\varphi\colon R \to R'$ be a homomorphism of Noetherian rings, and $\mathfrak{q} \subset R'$ a $\mathfrak{p}$-primary ideal. Show that $\varphi^{-1}\mathfrak{q} \subset R$ is $\varphi^{-1}\mathfrak{p}$-primary. Show that the converse holds if φ is surjective.

SOLUTION: Let $xy \in \varphi^{-1}\mathfrak{q}$, but $x \notin \varphi^{-1}\mathfrak{q}$. Then $\varphi(x)\varphi(y) \in \mathfrak{q}$, but $\varphi(x) \notin \mathfrak{q}$. So $\varphi(y)^n \in \mathfrak{q}$ for some $n \geq 1$ by **(18.5)**. Hence, $y^n \in \varphi^{-1}\mathfrak{q}$. So $\varphi^{-1}\mathfrak{q}$ is primary by **(18.5)**. Its radical is $\varphi^{-1}\mathfrak{p}$ as $\mathfrak{p} = \sqrt{\mathfrak{q}}$, and taking the radical commutes with taking the inverse image by **(3.21)**. The converse can be proved similarly. □

EXERCISE **(18.16)**. — Let k be a field, $R := k[X, Y, Z]$ be the polynomial ring. Set $\mathfrak{a} := \langle XY,\, X - YZ\rangle$, set $\mathfrak{q}_1 := \langle X, Z\rangle$ and set $\mathfrak{q}_2 := \langle Y^2, X - YZ\rangle$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ holds and that this expression is an irredundant primary decomposition.

SOLUTION: First, $XY = Y(X - YZ) + Y^2Z \in \mathfrak{q}_2$. Hence $\mathfrak{a} \subset \mathfrak{q}_1 \cap \mathfrak{q}_2$. Conversely, take $F \in \mathfrak{q}_1 \cap \mathfrak{q}_2$. Then $F \in \mathfrak{q}_2$, so $F = GY^2 + H(X - YZ)$ with $G, H \in R$. But $F \in \mathfrak{q}_1$, so $G \in \mathfrak{q}_1$; say $G = AX + BZ$ with $A, B \in R$. Then

$$F = (AY + B)XY + (H - BY)(X - ZY) \in \mathfrak{a}.$$

Thus $\mathfrak{a} \supset \mathfrak{q}_1 \cap \mathfrak{q}_2$. Thus $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ holds.

Finally, $\mathfrak{q}_1$ is prime by **(2.10)**. Now, using **(18.8)**, let's show $\mathfrak{q}_2$ is $\langle X, Y\rangle$-primary. Form $\varphi\colon k[X, Y, Z] \to k[Y, Z]$ with $\varphi(X) := YZ$. Clearly, $\mathfrak{q}_2 = \varphi^{-1}\langle Y^2\rangle$ and $\langle X,\, Y\rangle = \varphi^{-1}\langle Y\rangle$; also, $\langle Y^2\rangle$ is $\langle Y\rangle$-primary by **(18.2)**. Thus $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ is a primary decomposition. It is irredundant as $\mathfrak{q}_1$ and $\langle X, Y\rangle$ are distinct. □

EXERCISE **(18.17)**. — Let $R := R' \times R''$ be a product of two domains. Find an irredundant primary decomposition of $\langle 0\rangle$.

SOLUTION: Set $\mathfrak{p}' := \langle 0\rangle \times R''$ and $\mathfrak{p}'' := R'' \times \langle 0\rangle$. Then $\mathfrak{p}'$ and $\mathfrak{p}''$ are prime by **(2.11)**, so primary by **(17.4)**(2). Clearly $\langle 0\rangle = \mathfrak{p}' \cap \mathfrak{p}''$. Thus this representation is a primary decomposition; it is irredundant as both $\mathfrak{p}'$ and $\mathfrak{p}''$ are needed. □

EXERCISE **(18.21)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Consider the following submodule of M:

$$\Gamma_{\mathfrak{a}}(M) := \textstyle\bigcup_{n\geq 1}\{m \in M \mid \mathfrak{a}^n m = 0 \text{ for some } n \geq 1\}.$$

(1) For any decomposition $0 = \bigcap Q_i$ with Q_i $\mathfrak{p}_i$-primary, show $\Gamma_{\mathfrak{a}}(M) = \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$. (2) Show $\Gamma_{\mathfrak{a}}(M)$ is the set of all $m \in M$ such that $m/1 \in M_{\mathfrak{p}}$ vanishes for every prime $\mathfrak{p}$ with $\mathfrak{a} \not\subset \mathfrak{p}$. (Thus $\Gamma_{\mathfrak{a}}(M)$ is the set of all m whose support lies in $\mathbf{V}(\mathfrak{a})$.)

SOLUTION: For (1), given $m \in \Gamma_{\mathfrak{a}}(M)$, say $\mathfrak{a}^n m = 0$. Given i with $\mathfrak{a} \not\subset \mathfrak{p}_i$, take $a \in \mathfrak{a} - \mathfrak{p}_i$. Then $a^n m = 0 \in Q_i$. Hence $m \in Q_i$ by **(18.4)**. Thus $m \in \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$.

Conversely, given $m \in \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$, take any j with $\mathfrak{a} \subset \mathfrak{p}_j$. Now, $\mathfrak{p}_j = \operatorname{nil}(M/Q_j)$ by **(18.3)**. So there is n_j with $\mathfrak{a}^{n_j} m \in Q_j$. Set $n := \max\{n_j\}$. Then $a^n m \in Q_i$ for all i, if $\mathfrak{a} \subset \mathfrak{p}_i$ or not. Hence $a^n m \in \bigcap Q_i = 0$. Thus $m \in \Gamma_{\mathfrak{a}}(M)$.

For (2), given $m \in \Gamma_{\mathfrak{a}}(M)$, say $\mathfrak{a}^n m = 0$. Given a prime $\mathfrak{p}$ with $\mathfrak{a} \not\subset \mathfrak{p}$, take $a \in \mathfrak{a} - \mathfrak{p}$. Then $a^n m = 0$ and $a^n \notin \mathfrak{p}$. So $m/1 \in M_{\mathfrak{p}}$ vanishes.

Conversely, given an $m \in M$ such that $m/1 \in M_{\mathfrak{p}}$ vanishes for every prime $\mathfrak{p}$ with $\mathfrak{a} \not\subset \mathfrak{p}$, consider a decomposition $0 = \bigcap Q_i$ with Q_i $\mathfrak{p}_i$-primary; one exists by **(18.20)**. By (1), it suffices to show $m \in Q_i$ if $\mathfrak{a} \not\subset \mathfrak{p}_i$. But $m/1 \in M_{\mathfrak{p}_i}$ vanishes. So

there's an $a \in R - \mathfrak{p}_i$ with $am = 0 \in Q_i$. So **(18.4)** yields $m \in Q_i$, as desired. □

EXERCISE **(18.25)**. — Let R be a Noetherian ring, M a finitely generated module, N a submodule. Prove $N = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(M/N)} \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$.

SOLUTION: **(18.20)** yields an irredundant primary decomposition $N = \bigcap_1^r Q_i$. Say Q_i is $\mathfrak{p}_i$-primary. Then $\{\mathfrak{p}_i\}_1^r = \mathrm{Ass}(M/N)$ by **(18.19)**. Also, **(18.23)** yields $\varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) = \bigcap_{\mathfrak{p}_j \subset \mathfrak{p}_i} Q_j$. Thus $\bigcap_1^r \varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) = \bigcap_1^r (\bigcap_{\mathfrak{p}_j \subset \mathfrak{p}_i} Q_j) = \bigcap_1^r Q_i = N$. □

EXERCISE **(18.27)**. — Let R be a Noetherian ring, $\mathfrak{m} \subset \mathrm{rad}(R)$ an ideal, M a finitely generated module, and M' a submodule. Considering M/N, show that

$$M' = \bigcap_{n \geq 0} (\mathfrak{m}^n M + M').$$

SOLUTION: Set $N := \bigcap_{n \geq 0} \mathfrak{m}^n (M/M')$. Then by **(18.26)**, there is $x \in \mathfrak{m}$ such that $(1 + x)N = 0$. By **(3.2)**, $1 + x$ is a unit since $\mathfrak{m} \subset \mathrm{rad}(R)$. Therefore, $N = (1 + x^{-1})(1 + x)N = \langle 0 \rangle$. However, $\mathfrak{m}^n(M/M') = (\mathfrak{m}^n M + M')/M'$. Thus $\bigcap (\mathfrak{m}^n M + M')/M' = 0$, as desired. □

19. Length

EXERCISE **(19.2)**. — Let R be a ring, M a module. Prove these statements:

(1) If M is simple, then any nonzero element $m \in M$ generates M.
(2) M is simple if and only if $M \simeq R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and if so, then $\mathfrak{m} = \mathrm{Ann}(M)$.
(3) If M has finite length, then M is finitely generated.

SOLUTION: Obviously, Rm is a nonzero submodule. So it is equal to M, because M is simple. Thus (1) holds.

Assume M is simple. Then M is cyclic by (1). So $M \simeq R/\mathfrak{m}$ for $\mathfrak{m} := \mathrm{Ann}(M)$ by **(4.7)**. Since M is simple, $\mathfrak{m}$ is maximal owing to the bijective correspondence of **(1.7)**. By the same token, if, conversely, $M \simeq R/\mathfrak{m}$ with $\mathfrak{m}$ maximal, then M is simple. Thus (2) holds.

Assume $\ell(M) < \infty$. Let $M = M_0 \supset M_1 \supset \cdots \supset M_m = 0$ be a composition series. If $m = 0$, then $M = 0$. Assume $m \geq 1$. Then M_1 has a composition series of length $m - 1$. So, by induction on m, we may assume M_1 is finitely generated. Further, M/M_1 is simple, so finitely generated by (1). Hence M is finitely generated by **(16.15)**(1). Thus (3) holds. □

EXERCISE **(19.4)**. — Let R be a Noetherian ring, M a finitely generated module. Prove that the following conditions are equivalent:

(1) M has finite length.
(2) $\mathrm{Supp}(M)$ consists entirely of maximal ideals.
(3) $\mathrm{Ass}(M)$ consists entirely of maximal ideals.

Prove that, if the conditions hold, then $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ are equal and finite.

SOLUTION: If (1) holds, then (2) holds owing to **(19.3)**. If (2) holds, then (1) holds owing to **(17.19)** and **(19.2)**(2). Finally, **(17.16)** and **(17.20)** imply that (2) and (3) are equivalent and that the last assertion holds. □

EXERCISE **(19.7)**. — Let k be a field, and R a finitely generated k-algebra. Prove that R is Artinian if and only if R is a finite-dimensional k-vector space.

SOLUTION: Since k is Noetherian by **(16.1)** and since R is a finitely generated k-algebra, R is Noetherian by **(16.11)**. Assume R is Artinian. Then $\ell(R) < \infty$ by **(19.5)**. So R has a composition series. The successive quotients are isomorphic to residue class fields by **(19.2)**(2). These fields are finitely generated k-algebras, since R is so. Hence these fields are finite extension fields of k by the Weak Nullstellensatz. Thus R is a finite-dimensional k-vector space. The converse holds by **(16.24)**. □

EXERCISE **(19.9)**. — Let k be a field, R a local k-algebra. Assume the map from k to the residue field is bijective. Given an R-module M, prove $\ell(M) = \dim_k(M)$.

SOLUTION: If $M = 0$, then $\ell(M) = 0$ and $\dim_k(M) = 0$. If $M \cong k$, then $\ell(M) = 1$ and $\dim_k(M) = 1$. Assume $1 \leq \ell(M) < \infty$. Then M has a submodule M' with $M/M' \cong k$. So Additivity of Length, **(19.8)**, yields $\ell(M') = \ell(M) - 1$ and $\dim_k(M') = \dim_k(M) - 1$. Hence $\ell(M') = \dim_k(M')$ by induction on $\ell(M)$. Thus $\ell(M) = \dim_k(M)$.

If $\ell(M) = \infty$, then for every $m \geq 1$, there exists a chain of submodules,

$$M = M_0 \supsetneqq M_1 \supsetneqq \cdots \supsetneqq M_m = 0.$$

Hence $\dim_k(M) = \infty$. □

EXERCISE **(19.13)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal, and R' a module-finite R-algebra. Show that R' has only finitely many primes $\mathfrak{p}'$ over $\mathfrak{p}$, as follows: reduce to the case that R is a field by localizing at $\mathfrak{p}$ and passing to the residue rings.

SOLUTION: First note that, if $\mathfrak{p}' \subset R'$ is a prime lying over $\mathfrak{p}$, then $\mathfrak{p}'R'_{\mathfrak{p}} \subset R'_{\mathfrak{p}}$ is a prime lying over the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. Hence, by **(11.16)**(2), it suffices to show that $R'_{\mathfrak{p}}$ has only finitely many such primes. Note also that $R'_{\mathfrak{p}}$ is module-finite over $R_{\mathfrak{p}}$. Hence we may replace R and R' by $R_{\mathfrak{p}}$ and $R'_{\mathfrak{p}}$, and thus assume that $\mathfrak{p}$ is the unique maximal ideal of R. Similarly, we may replace R and R' by $R/\mathfrak{p}$ and $R'/\mathfrak{p}R'$, and thus assume that R is a field.

There are a couple of ways to finish. First, R' is now Artinian by **(19.12)** or by **(16.24)**; hence, R' has only finitely many primes by **(19.10)**. Alternatively, every prime is now minimal by incomparability **(14.3)**(2). Further, R' is Noetherian by **(16.11)**; hence, R' has only finitely many minimal primes by **(17.21)**. □

EXERCISE **(19.15)**. — Let R be a Noetherian ring, and M a finitely generated module. Prove the equivalence of the following four conditions:

(1) M has finite length.
(2) M is annihilated by some finite product of maximal ideals $\prod \mathfrak{m}_i$.
(3) Every prime $\mathfrak{p}$ containing $\operatorname{Ann}(M)$ is maximal.
(4) $R/\operatorname{Ann}(M)$ is Artinian.

SOLUTION: Assume (1) holds. Let $M = M_0 \supset \cdots \supset M_m = 0$ be a composition series, and set $\mathfrak{m}_i := \operatorname{Ann}(M_{i-1}/M_i)$. Then $\mathfrak{m}_i$ is maximal by **(19.2)**(2). Further, $\mathfrak{m}_i M_{i-1} \subset M_i$. Hence $\mathfrak{m}_i \cdots \mathfrak{m}_1 M_0 \subset M_i$. Thus (2) holds.

If (2) holds, then (3) does too. Indeed, if $\mathfrak{p} \supset \operatorname{Ann}(M) \supset \prod \mathfrak{m}_i$, then $\mathfrak{p} \supset \mathfrak{m}_i$ for some i by **(2.2)** as $\mathfrak{p}$ is prime, and so $\mathfrak{p} = \mathfrak{m}_i$ as $\mathfrak{m}_i$ is maximal.

Assume (3) holds. Then $\dim(R/\operatorname{Ann}(M)) = 0$. But, by **(16.7)**, any quotient of R is Noetherian. Hence **(19.10)** yields (4).

If (4) holds, then **(19.11)** yields (1), as M is finitely generated over $R/\operatorname{Ann}(M)$ owing to **(4.5)**. □

20. Hilbert Functions

EXERCISE **(20.5)**. — Let k be a field, $k[X,Y]$ the polynomial ring. Show $\langle X, Y^2\rangle$ and $\langle X^2, Y^2\rangle$ have different Hilbert Series, but the same Hilbert Polynomial.

SOLUTION: Set $\mathfrak{m} := \langle X, Y\rangle$ and $\mathfrak{a} := \langle X, Y^2\rangle$ and $\mathfrak{b} := \langle X^2, Y^2\rangle$. They are graded by degree. So $\ell(\mathfrak{a}_1) = 1$, and $\ell(\mathfrak{a}_n) = \ell(\mathfrak{m}_n)$ for all $n \geq 2$. Further, $\ell(\mathfrak{b}_1) = 0$, $\ell(\mathfrak{b}_2) = 2$, and $\ell(\mathfrak{b}_n) = \ell(\mathfrak{m}_n)$ for $n \geq 3$. Thus the three ideals have the same Hilbert Polynomial, namely $h(n) = n + 1$, but different Hilbert Series. □

EXERCISE **(20.6)**. — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded R-module. Let $N = \bigoplus N_n$ be a **homogeneous submodule**; that is, $N_n = N \cap M_n$. Assume R_0 is Artinian, R is a finitely generated R_0-algebra, and M is a finitely generated R-module. Set

$$N' := \{\, m \in M \mid \text{there is } k_0 \text{ such that } R_k m \in N \text{ for all } k \geq k_0 \,\}.$$

(1) Prove that N' is a homogeneous submodule of M with the same Hilbert Polynomial as N, and that N' is the largest such submodule.

(2) Let $N = \bigcap Q_i$ be a decomposition with Q_i $\mathfrak{p}_i$-primary. Set $R_+ := \bigoplus_{n>0} R_n$. Prove that $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$.

SOLUTION: Given $m = \sum m_i \in N'$, say $R_k m \subset N$. Then $R_k m_i \subset N$ since N is homogeneous. Hence $m_i \in N'$. Thus N' is homogeneous.

By **(19.10)** and **(16.11)**, R is Noetherian. So N' is finitely generated by **(16.18)**. Let $n_1, \dots, n_r$ be homogeneous generators of N' with $n_i \in N_{k_i}$; set $k' := \max\{k_i\}$. There is k such that $R_k n_i \in N$ for all i. Given $\ell \geq k + k'$, take $n \in N'_\ell$, and write $n = \sum y_i n_i$ with $y_i \in R_{\ell - k_i}$. Then $y_i n_i \in N_\ell$ for all i. So $n \in N_\ell$. Thus $N'_\ell = N_\ell$ for all $\ell \geq k + k'$. Thus N and N' have the same Hilbert polynomial.

Say $N'' \supset N$, and both have the same Hilbert Polynomial. Then there is k_0 with $\ell(N''_k) = \ell(N_k)$ for all $k \geq k_0$. So $N''_k = N_k$ for all $k \geq k_0$. So, if $n \in N''$, then $R_k n \in N$ for all $k \geq k_0$. Thus $N'' \subset N'$. Thus (1) holds.

To prove (2), note $0 = \bigcap(Q_i/N)$ in M/N. By **(18.21)**,

$$\Gamma_{R_+}(M/N) = \bigcap_{\mathfrak{p}_i \not\supset R_+} (Q_i/N).$$

But clearly $\Gamma_{R_+}(M/N) = N'/N$. Thus $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$. □

EXERCISE **(20.9)**. — Let k be a field, $P := k[X,Y,Z]$ the polynomial ring in three variables, $f \in P$ a homogeneous polynomial of degree $d \geq 1$. Set $R := P/\langle f\rangle$. Find the coefficients of the Hilbert Polynomial $h(R,n)$ explicitly in terms of d.

SOLUTION: Clearly, the following sequence is exact:

$$0 \to P(-d) \xrightarrow{\mu_f} P \to R \to 0.$$

Hence, Additivity of Length, **(19.8)**, yields $h(R,n) = h(P,n) - h(P(-d),n)$. But $P(-d)_n = P(n-d)$, so $h(P(-d),n) = h(P, n-d)$. Therefore, **(20.4)** yields

$$h(R,n) = \tbinom{2+n}{2} - \tbinom{2-d+n}{2} = dn - (d-3)d/2.$$ □

EXERCISE **(20.10)**. — Under the conditions of **(20.8)**, assume there is a homogeneous nonzerodivisor $f \in R$ with $M_f = 0$. Prove $\deg\big(h(R,n)\big) > \deg\big(h(M,n)\big)$; start with the case $M := R/\langle f^k\rangle$.

SOLUTION: Suppose $M := R/\langle f^k\rangle$. Set $c := k\deg(f)$. Form the exact sequence $0 \to R(-c) \xrightarrow{\mu} R \to M \to 0$ where μ is multiplication by f^k. Then Additivity of Length **(19.8)** yields $h(M,n) = h(R,n) - h(R,n-c)$. But

$$h(R,n) = \tfrac{e(1)}{(d-1)!}n^{d-1} + \cdots \quad \text{and} \quad h(R,n-c) = \tfrac{e(1)}{(d-1)!}(n-c)^{d-1} + \cdots .$$

by **(20.8)**. Thus $\deg\bigl(h(R,n)\bigr) > \deg\bigl(h(M,n)\bigr)$.

In the general case, there is k with $f^kM = 0$ by **(12.7)**. Set $M' := R/\langle f^k\rangle$. Then generators $m_i \in M_{c_i}$ for $1 \le i \le r$ yield a surjection $\bigoplus_i M'(-c_i) \twoheadrightarrow M$. Hence $\sum_i \ell(M'_{n-c_i}) \ge \ell(M_n)$ for all n. But $\deg\bigl(h(M'(-c_i),n)\bigr) = \deg\bigl(h(M',n)\bigr)$. Hence $\deg\bigl(h(M',n)\bigr) \ge \deg\bigl(h(M,n)\bigr)$. But $\deg\bigl(h(R,n)\bigr) > \deg\bigl(h(M',n)\bigr)$ by the first case. Thus $\deg\bigl(h(R,n)\bigr) > \deg\bigl(h(M,n)\bigr)$. □

EXERCISE **(20.15)**. — Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, and M a finitely generated module. Assume $\ell(M/\mathfrak{q}M) < \infty$. Set $\mathfrak{m} := \sqrt{\mathfrak{q}}$. Show

$$\deg p_{\mathfrak{m}}(M,n) = \deg p_{\mathfrak{q}}(M,n).$$

SOLUTION: There is an m such that $\mathfrak{m} \supset \mathfrak{q} \supset \mathfrak{m}^m$ by **(3.19)**. Hence

$$\mathfrak{m}^nM \supset \mathfrak{q}^nM \supset \mathfrak{m}^{mn}M$$

for all $n \ge 0$. Dividing into M and extracting lengths yields

$$\ell(M/\mathfrak{m}^nM) \le \ell(M/\mathfrak{q}^nM) \le \ell(M/\mathfrak{m}^{mn}M).$$

Therefore, for large n, we get

$$p_{\mathfrak{m}}(M,n) \le p_{\mathfrak{q}}(M,n) \le p_{\mathfrak{m}}(M,nm).$$

The two extremes are polynomials in n with the same degree, say d, (but not the same leading coefficient). Dividing by n^d and letting $n \to \infty$, we conclude that the polynomial $p_{\mathfrak{q}}(M,n)$ also has degree d. □

EXERCISE **(20.19)**. — Derive the Krull Intersection Theorem, **(18.26)**, from the Artin–Rees Lemma, **(20.18)**.

SOLUTION: In the notation of **(18.26)**, we must prove that $N = \mathfrak{a}N$. So apply the Artin–Rees Lemma to N and the $\mathfrak{a}$-adic filtration of M; we get an m such that $\mathfrak{a}(N \cap \mathfrak{a}^mM) = N \cap \mathfrak{a}^{m+1}M$. But $N \cap \mathfrak{a}^nM = N$ for all $n \ge 0$. Thus $N = \mathfrak{a}N$. □

20. Appendix: Homogeneity

EXERCISE **(20.24)**. — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, and M a graded module. Prove that $\sqrt{\mathfrak{a}}$ and $\operatorname{Ann}(M)$ and $\operatorname{nil}(M)$ are homogeneous.

SOLUTION: Take $x = \sum_{i\ge r}^{r+n} x_i \in R$ with the x_i the homogeneous components.

First, suppose $x \in \sqrt{\mathfrak{a}}$. Say $x^k \in \mathfrak{a}$. Either x_r^k vanishes or it is the initial component of x^k. But $\mathfrak{a}$ is homogeneous. So $x_r^k \in \mathfrak{a}$. So $x_r \in \sqrt{\mathfrak{a}}$. So $x - x_r \in \sqrt{\mathfrak{a}}$ by **(3.18)**. So all the x_i are in $\sqrt{\mathfrak{a}}$ by induction on n. Thus $\sqrt{\mathfrak{a}}$ is homogeneous.

Second, suppose $x \in \operatorname{Ann}(M)$. Let $m \in M$. Then $0 = xm = \sum x_im$. If m is homogeneous, then $x_im = 0$ for all i, since M is graded. But M has a set of homogeneous generators. Thus $x_i \in \operatorname{Ann}(M)$ for all i, as desired.

Finally, $\operatorname{nil}(M)$ is homogeneous, as $\operatorname{nil}(M) = \sqrt{\operatorname{Ann}(M)}$ by **(13.7)**. □

EXERCISE **(20.25)**. — Let R be a Noetherian graded ring, M a finitely generated graded module, Q a submodule. Let $Q^* \subset Q$ be the submodule generated by the homogeneous elements of Q. Assume Q is primary. Then Q^* is primary too.

SOLUTION: Let $x \in R$ and $m \in M$ be homogeneous with $xm \in Q^*$. Assume $x \notin \operatorname{nil}(M/Q^*)$. Then, given $\ell \geq 1$, there is $m' \in M$ with $x^\ell m' \notin Q^*$. So m' has a homogeneous component m'' with $x^\ell m'' \notin Q^*$. Then $x^\ell m'' \notin Q$ by definition of Q^*. Thus $x \notin \operatorname{nil}(M/Q)$. Since Q is primary, $m \in Q$ by **(18.4)**. Since m is homogeneous, $m \in Q^*$. Thus Q^* is primary by **(20.23)**. □

EXERCISE **(20.29)**. — Under the conditions of **(20.8)**, assume that R is a domain and that its integral closure $\overline{R}$ in $\operatorname{Frac}(R)$ is a finitely generated R-module.

(1) Prove that there is a homogeneous $f \in R$ with $R_f = \overline{R}_f$.

(2) Prove that the Hilbert Polynomials of R and $\overline{R}$ have the same degree and same leading coefficient.

SOLUTION: Let $x_1, \dots, x_r$ be homogeneous generators of $\overline{R}$ as an R-module. Write $x_i = a_i/b_i$ with $a_i, b_i \in R$ homogeneous. Set $f := \prod b_i$. Then $fx_i \in R$ for each i. So $\overline{R}_f = R_f$. Thus (1) holds.

Consider the short exact sequence $0 \to R \to \overline{R} \to \overline{R}/R \to 0$. Then $(\overline{R}/R)_f = 0$ by **(12.16)**. So $\deg\bigl(h(\overline{R}/R, n)\bigr) < \deg\bigl(h(\overline{R}, n)\bigr)$ by **(20.10)** and (1). But

$$h(\overline{R}, n) = h(R, n) + h(\overline{R}/R, n)$$

by **(19.8)** and **(20.8)**. Thus (2) holds. □

21. Dimension

EXERCISE **(21.8)**. — Let R be a Noetherian ring, and $\mathfrak{p}$ be a prime minimal containing $x_1, \dots, x_r$. Given r' with $1 \leq r' \leq r$, set $R' := R/\langle x_1, \dots, x_{r'}\rangle$ and $\mathfrak{p}' := \mathfrak{p}/\langle x_1, \dots, x_{r'}\rangle$. Assume $\operatorname{ht}(\mathfrak{p}) = r$. Prove $\operatorname{ht}(\mathfrak{p}') = r - r'$.

SOLUTION: Let $x_i' \in R'$ be the residue of x_i. Then $\mathfrak{p}'$ is minimal containing $x_{r'+1}', \dots x_r'$ by **(1.7)** and **(2.7)**. So $\operatorname{ht}(\mathfrak{p}') \leq r - r'$ by **(21.7)**.

On the other hand, $R'_{\mathfrak{p}'} = R'_{\mathfrak{p}}$ by **(11.19)**, and $R'_{\mathfrak{p}} = R_{\mathfrak{p}}/\langle x_1/1, \dots, x_{r'}/1\rangle$ by **(12.18)** Hence $\dim(R'_{\mathfrak{p}'}) \geq \dim(R_{\mathfrak{p}}) - r'$ by repeated application of **(21.5)**. So $\operatorname{ht}(\mathfrak{p}') \geq r - r'$ by **(21.6.1)**, as required. □

EXERCISE **(21.10)**. — Let R be a domain. Prove that, if R is a UFD, then every height-1 prime is principal, and that the converse holds if R is Noetherian.

SOLUTION: Let $\mathfrak{p}$ be a height-1 prime. Then there's a nonzero $x \in \mathfrak{p}$. Factor x. One prime factor p must lie in $\mathfrak{p}$ as $\mathfrak{p}$ is prime. Clearly, $\langle p\rangle$ is a prime ideal as p is a prime element. But $\langle p\rangle \subset \mathfrak{p}$ and $\operatorname{ht}(p) = 1$. Thus, $\langle p\rangle = \mathfrak{p}$.

Conversely, assume every height-1 prime is principal and assume R is Noetherian. To prove R is a UFD, it suffices to prove every irreducible element p is prime (see [1, Ch. 11, Sec. 2, pp. 392–396]). Let $\mathfrak{p}$ be a prime minimal containing p. By Krull's Principal Ideal Theorem, $\operatorname{ht}(\mathfrak{p}) = 1$. So $\mathfrak{p} = \langle x\rangle$ for some x. Then x is prime by **(2.6)**. And $p = xy$ for some y as $p \in \mathfrak{p}$. But p is irreducible. So y is a unit. Thus p is prime, as desired. □

EXERCISE **(21.11)**. — (1) Let A be a Noetherian local ring with a principal prime $\mathfrak{p}$ of height at least 1. Prove that A is a domain.

(2) Let k be a field, $P := k[[X]]$ the formal power series ring in one variable. Set $R := P \times P$. Prove that P is Noetherian and semilocal, and that P contains a principal prime $\mathfrak{p}$ of height 1, but that P is not a domain.

SOLUTION: To prove (1), say $\mathfrak{p} = \langle x \rangle$, and let $\mathfrak{q} \subset \mathfrak{p}$ be a minimal prime. Take $y \in \mathfrak{q}$. Then $y = ax$ for some a. But $x \notin \mathfrak{q}$ since $\operatorname{ht}\mathfrak{p} \geq 1$. Hence $a \in \mathfrak{q}$. Thus $\mathfrak{q} = \mathfrak{q}x$. But x lies in the maximal ideal of the local ring A, and $\mathfrak{q}$ is finitely generated since A is Noetherian. Hence Nakayama's Lemma **(10.8)** yields $\mathfrak{q} = \langle 0 \rangle$. Thus $\langle 0 \rangle$ is prime, and so A is a domain.

Alternatively, as $a \in \mathfrak{q}$, also $a = a_1 x$ with $a_1 \in \mathfrak{q}$. Repeating yields an ascending chain of ideals $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$. It must stabilize as A is Noetherian: there's a k such that $a_k \in \langle a_{k-1} \rangle$. Then $a_k = ba_{k-1} = ba_k x$ for some b. So $a_k(1 - bx) = 0$. But $1 - bx$ is a unit by **(3.4)** as A is local. So $a_k = 0$. Hence $y = 0$ and so $\mathfrak{q} = \langle 0 \rangle$. Thus A is a domain.

As to (2), every nonzero ideal of P is of the form $\langle X^n \rangle$ by **(3.8)**. Hence P is Noetherian. Thus R is Noetherian by **(16.16)**.

The primes of R are of the form $\mathfrak{q} \times P$ or $P \times \mathfrak{q}$ where $\mathfrak{q}$ is a prime of P by **(2.10)**. Further, $\mathfrak{m} := \langle X \rangle$ is the unique maximal ideal by **(3.7)**. Hence R has just two maximal ideals $\mathfrak{m} \times P$ and $P \times \mathfrak{m}$. Thus R is semilocal.

Set $\mathfrak{p} := \langle (X, 1) \rangle$. Then $\mathfrak{p} = \mathfrak{m} \times P$. So $\mathfrak{p}$ is a principal prime. Further, $\mathfrak{p}$ contains just one other prime $0 \times P$. Thus $\operatorname{ht}(\mathfrak{p}) = 1$.

Finally, R is not a domain as $(1, 0) \cdot (0, 1) = 0$. □

EXERCISE **(21.12)**. — Let R be a finitely generated algebra over a field. Assume R is a domain of dimension r. Let $x \in R$ be neither 0 nor a unit. Set $R' := R/\langle x \rangle$. Prove that $r - 1$ is the length of any chain of primes in R' of maximal length.

SOLUTION: A chain of primes in R' of maximal length lifts to a chain of primes $\mathfrak{p}_i$ in R of maximal length with $\langle x \rangle \subseteq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d$. As x is not a unit, $d \geq 1$. As $x \neq 0$, also $\mathfrak{p}_1 \neq 0$. But R is a domain. So Krull's Principal Ideal Theorem, **(21.8)**, yields $\operatorname{ht}\mathfrak{p}_1 = 1$. So $0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ is of maximal length in R. But R is a finitely generated algebra over a field. Hence $d = \dim R$ by **(15.8)**. □

EXERCISE **(21.14)**. — Let A be a Noetherian local ring of dimension r. Let $\mathfrak{m}$ be the maximal ideal, and $k := A/\mathfrak{m}$ the residue class field. Prove that

$$r \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2),$$

with equality if and only if $\mathfrak{m}$ is generated by r elements.

SOLUTION: By **(21.4)**, $\dim(A)$ is the smallest number of elements that generate a parameter ideal. But $\mathfrak{m}$ is a parameter ideal, and the smallest number of generators of $\mathfrak{m}$ is $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ by **(10.9)**(2). The assertion follows. □

EXERCISE **(21.18)**. — Let A be a Noetherian local ring of dimension r, and $x_1, \ldots, x_s \in A$ with $s \leq r$. Set $\mathfrak{a} := \langle x_1, \ldots, x_s \rangle$ and $B := A/\mathfrak{a}$. Prove these two conditions are equivalent:

(1) A is regular, and there are $x_{s+1}, \ldots, x_r \in A$ with $x_1, \ldots, x_r$ a regular sop.

(2) B is regular of dimension $r - s$.

SOLUTION: Assume (1). Then $x_1, \dots, x_r$ generate the maximal ideal $\mathfrak{m}$ of A. So the residues of $x_{s+1}, \dots, x_r$ generate that $\mathfrak{n}$ of B. Hence $\dim(B) \geq r - s$ by **(21.4)**. But $\dim(B) \geq r - s$ by **(21.5)**. So $\dim(B) = r - s$. Thus (2) holds.

Assume (2). Then $\mathfrak{n}$ is generated by $r - s$ elements, say by the residues of $x_{s+1}, \dots, x_r \in A$. Hence $\mathfrak{m}$ is generated by $x_1, \dots, x_r$. Thus (1) holds. □

22. Completion

EXERCISE **(22.3)**. — In the 2-adic integers, evaluate the sum $1 + 2 + 4 + 8 + \cdots$.

SOLUTION: In the 2-adic integers, $1 + 2 + 4 + 8 + \cdots = 1/(1 - 2) = -1$. □

EXERCISE **(22.4)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Prove the following three conditions are equivalent:

(1) $\kappa\colon M \to \widehat{M}$ is injective; (2) $\bigcap \mathfrak{a}^n M = \langle 0 \rangle$; (3) M is separated.

SOLUTION: Clearly, $\operatorname{Ker}(\kappa) = \bigcap \mathfrak{a}^n M$; so (1) and (2) are equivalent. Moreover, (2) and (3) were proved equivalent in **(22.1)**. □

EXERCISE **(22.8)**. — Let A be a Noetherian semilocal ring, and $\mathfrak{m}_1, \dots, \mathfrak{m}_m$ all its maximal ideals. Prove that $\widehat{A} = \prod \widehat{A}_{\mathfrak{m}_i}$.

SOLUTION: Set $\mathfrak{m} := \operatorname{rad}(R)$. Fix $n \geq 0$. Then $A/\mathfrak{m}^n$ is Noetherian of dimension 0; so it's Artinian by **(19.15)**. Hence **(19.14)** yields

$$A/\mathfrak{m}^n = \textstyle\prod_i (A/\mathfrak{m}^n)_{(\mathfrak{m}_i/\mathfrak{m}^n)}.$$

However, $(A/\mathfrak{m}^n)_{(\mathfrak{m}_i/\mathfrak{m}^n)}$ is equal to $(A/\mathfrak{m}^n)_{\mathfrak{m}_i}$ by **(11.19)**, so to $A_{m_i}/\mathfrak{m}^n A_{m_i}$ by Exactness of Localization **(12.16)**. Furthermore, $\mathfrak{m}^n = (\prod \mathfrak{m}_i)^n = \bigcap \mathfrak{m}_i^n$ by **(1.12)**. Now, $\mathfrak{m}_i^n$ is $\mathfrak{m}_i$-primary by **(18.10)**. Hence $\mathfrak{m}^n A_{m_i} = \mathfrak{m}_i^n A_{m_i}$ by **(18.23)**. Therefore, $A/\mathfrak{m}^n = \prod_i (A_{\mathfrak{m}_i}/\mathfrak{m}_i^n A_{\mathfrak{m}_i})$. Taking inverse limits, we obtain the assertion, because inverse limit commutes with finite product by the construction of the limit. □

EXERCISE **(22.9)**. — Let R be a ring, M a module, $M = M_0 \supset M_1 \supset \cdots$ a filtration, and $N \subset M$ a submodule. Filter N by $N_n := N \cap M_n$. Assume $N \supset M_n$ for $n \geq n_0$ for some n_0. Prove $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = M/N$ and $G(\widehat{M}) = G(M)$.

SOLUTION: For each $n \geq n_0$, form this commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \to & N/M_{n+1} & \to & M/M_{n+1} & \to & M/N & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N/M_n & \longrightarrow & M/M_n & \longrightarrow & M/N & \to & 0 \end{array}$$

The left vertical map is surjective; the right is the identity. So the induced sequence

$$0 \to \widehat{N} \to \widehat{M} \to M/N \to 0$$

is exact by **(22.6)** and **(22.7)**. Thus $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = M/N$.

In particular, $\widehat{M}/\widehat{M}_n = M/M_n$ for each n. Therefore, $\widehat{M}_n/\widehat{M}_{n+1} = M_n/M_{n+1}$. Thus $G(\widehat{M}) = G(M)$. □

EXERCISE **(22.10)**. — (1) Let R be a ring, $\mathfrak{a}$ an ideal. If $G_{\mathfrak{a}}(R)$ is a domain, show $\widehat{R}$ is an domain. If also $\bigcap_{n\geq 0}\mathfrak{a}^n = 0$, show R is a domain.

(2) Use (1) to give an alternative proof that a regular local ring A is a domain.

SOLUTION: Consider (1). Let $x, y \in \widehat{R}$ be nonzero. Since $\widehat{R}$ is separated there are positive integers r and s with $x \in \widehat{\mathfrak{a}}^r - \widehat{\mathfrak{a}}^{r+1}$ and $y \in \widehat{\mathfrak{a}}^s - \widehat{\mathfrak{a}}^{s+1}$. Let $x' \in G^r_{\widehat{\mathfrak{a}}}(\widehat{R})$ and $y' \in G^s_{\widehat{\mathfrak{a}}}(\widehat{R})$ denote the images of x and y. Then $x' \neq 0$ and $y' \neq 0$. Now, $G_{\widehat{\mathfrak{a}}}(\widehat{R}) = G_{\mathfrak{a}}(R)$ by **(22.9)**. Assume $G_{\mathfrak{a}}(R)$ is a domain. Then $x'y' \neq 0$. Hence $x'y' \in G^{r+s}_{\widehat{\mathfrak{a}}}$ is the image of $xy \in \widehat{\mathfrak{a}}^{r+s}$. Hence $xy \neq 0$. Thus $\widehat{R}$ is a domain.

If $\bigcap_{n\geq 0}\mathfrak{a}^n = 0$, then $R \subset \widehat{R}$ by **(22.4)**; so R is a domain if $\widehat{R}$ is. Thus (1) holds.

As to (2), denote the maximal ideal of A by $\mathfrak{m}$. Then $\bigcap_{n\geq 0}\mathfrak{m}^n = \langle 0\rangle$ by the Krull Intersection Theorem **(18.26)**, and $G_{\mathfrak{m}}(A)$ is a polynomial ring by **(21.17)**, so a domain. Hence A is a domain, by (1). Thus (2) holds. □

EXERCISE **(22.12)**. — Let A be a semilocal ring, $\mathfrak{m}_1, \dots, \mathfrak{m}_m$ all its maximal ideals, and set $\mathfrak{m} := \operatorname{rad}(A)$. Prove that $\widehat{A}$ is a semilocal ring, that $\widehat{\mathfrak{m}}_1, \dots, \widehat{\mathfrak{m}}_m$ are all its maximal ideals, and that $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{A})$.

SOLUTION: First, **(22.9)** yields $\widehat{A}/\widehat{\mathfrak{m}} = A/\mathfrak{m}$ and $\widehat{A}/\widehat{\mathfrak{m}}_i = A/\mathfrak{m}_i$. So $\widehat{\mathfrak{m}}_i$ is maximal. By hypothesis, $\mathfrak{m} = \bigcap \mathfrak{m}_i$; so $A/\mathfrak{m} \subset \prod(A/\mathfrak{m}_i)$. Hence $\widehat{A}/\widehat{\mathfrak{m}} \subset \prod(\widehat{A}/\widehat{\mathfrak{m}}_i)$; so $\widehat{\mathfrak{m}} = \bigcap \widehat{\mathfrak{m}}_i$. So $\widehat{\mathfrak{m}} \supset \operatorname{rad}(\widehat{A})$. But $\widehat{\mathfrak{m}} \subset \operatorname{rad}(\widehat{A})$ by **(22.2)**. Thus $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{A})$.

Finally, let $\mathfrak{m}'$ be any maximal ideal of $\widehat{A}$. Then $\mathfrak{m}' \supset \operatorname{rad}(\widehat{A}) = \bigcap \widehat{\mathfrak{m}}_i$. Hence $\mathfrak{m}' \supset \widehat{\mathfrak{m}}_i$ for some i by **(2.2)**. But $\widehat{\mathfrak{m}}_i$ is maximal. So $\mathfrak{m}' = \widehat{\mathfrak{m}}_i$. Thus $\widehat{\mathfrak{m}}_1, \dots, \widehat{\mathfrak{m}}_m$ are all the maximal ideals of $\widehat{A}$, and so $\widehat{A}$ is semilocal. □

EXERCISE **(22.15)**. — Let A be a Noetherian ring, $x \in A$, and $\widehat{x} \in \widehat{A}$ its image. Prove $\widehat{x}$ is a nonzerodivisor if x is. Prove the converse holds if A is semilocal.

SOLUTION: Assume x is a nonzerodivisor. Then the multiplication map μ_x is injective on A. So by Exactness of Completion, the induced map $\widehat{\mu}_x$ is injective on $\widehat{A}$. But $\widehat{\mu}_x = \mu_{\widehat{x}}$. Thus $\widehat{x}$ is a nonzerodivisor.

Conversely, assume $\widehat{x}$ is a nonzerodivisor and A is semilocal. Then $\widehat{\mu}_x$ is injective on $\widehat{A}$. So its restriction is injective on the image of the canonical map $A \to \widehat{A}$. But this map is injective, as the completion is taken with respect to the Jacobson radical; further, $\widehat{\mu}_x$ induces μ_x. Thus x is a nonzerodivisor. □

EXERCISE **(22.17)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Show that $M \mapsto \widehat{M}$ preserves surjections, and that $\widehat{R} \otimes M \to \widehat{M}$ is surjective if M is finitely generated.

SOLUTION: The first part of the proof of **(22.14)** shows that $M \mapsto \widehat{M}$ preserves surjections. So **(8.16)** yields the desired surjectivity. □

EXERCISE **(22.20)**. — Let R be a Noetherian ring, and $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Assume $\mathfrak{a} \subset \operatorname{rad}(R)$, and use the $\mathfrak{a}$-adic toplogy. Prove $\mathfrak{b}$ is principal if $\mathfrak{b}\widehat{R}$ is.

SOLUTION: Since R is Noetherian, $\mathfrak{b}$ is finitely generated. But $\mathfrak{a} \subset \operatorname{rad}(R)$. Hence, $\mathfrak{b}$ is principal if $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ is cyclic by **(10.9)**(2). But $\mathfrak{b}/\mathfrak{a}\mathfrak{b} = \widehat{\mathfrak{b}}\big/(\mathfrak{a}\mathfrak{b})\widehat{\ }$ by **(22.9)**, and $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$ by **(22.18)**(2). Hence, if $\mathfrak{b}\widehat{R}$ is principal, then $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ is cyclic, as desired. □

EXERCISE **(22.23)** (*Nakayama's Lemma for a complete ring*). — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Assume R is complete, and M separated. Show $m_1, \dots, m_n \in M$ generate if their images in $M/\mathfrak{a}M$ generate.

SOLUTION: Note that the images of $m_1, \dots, m_n$ in $G(M)$ generate over $G(R)$. Therefore, $m_1, \dots, m_n \in M$ generate over R by the proof of **(22.22)**.

Alternatively, M is finitely generated over R and complete by the statement of **(22.22)**. Since M is also separated, $M = \widehat{M}$. Hence M is also an $\widehat{R}$-module. Since R is complete, $\kappa_R \colon R \to \widehat{R}$ is surjective. Now, $\mathfrak{a}$ is closed by **(22.1)**; so $\mathfrak{a}$ is complete; whence, $\kappa_{\mathfrak{a}} \colon \mathfrak{a} \to \widehat{\mathfrak{a}}$ is surjective too. Hence $\mathfrak{a}M = \widehat{\mathfrak{a}}M$. Thus $M/\mathfrak{a}M = M/\widehat{\mathfrak{a}}M$. So the m_i generate $M/\widehat{\mathfrak{a}}M$. But $\widehat{\mathfrak{a}} \subset \operatorname{rad}(\widehat{R})$ by **(22.2)**. So by Nakayama's Lemma **(10.9)**(2), the m_i generate M over $\widehat{R}$, so also over R as κ_R is surjective. □

EXERCISE **(22.27)**. — Let A be a Noetherian local ring, $\mathfrak{m}$ the maximal ideal. Prove (1) that $\widehat{A}$ is a Noetherian local ring with $\widehat{\mathfrak{m}}$ as maximal ideal, (2) that $\dim(A) = \dim(\widehat{A})$, and (3) that A is regular if and only if $\widehat{A}$ is regular.

SOLUTION: First, $\widehat{A}$ is Noetherian by **(22.25)**, and local with $\widehat{\mathfrak{m}}$ as maximal ideal by **(22.8)**; thus (1) holds.

Second, $A/\mathfrak{m}^n = \widehat{A}/\widehat{\mathfrak{m}}^n$ by **(22.9)**. So $d(A) = d(\widehat{A})$ by **(20.13)**. Thus (2) holds by **(21.4)**.

Third, $\mathfrak{m}/\mathfrak{m}^2 = \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2$ by **(22.9)**. So $\mathfrak{m}$ and $\widehat{\mathfrak{m}}$ have the same number of generators by **(10.10)**. Thus (3) holds. □

23. Discrete Valuation Rings

EXERCISE **(23.5)**. — Let R be a ring, M a module, and $x, y \in R$.

(1) Prove that, if x, y form an M-sequence, then, given any $m, n \in M$ such that $xm = yn$, there exists $p \in M$ such that $m = yp$ and $n = xp$.

(2) Prove the converse of (1) if R is local, and x, y lie in its maximal ideal $\mathfrak{m}$, and M is Noetherian.

SOLUTION: Consider (1). Let n_1 be the residue of n in $M_1 := M/xM$. Then $yn_1 = 0$, but $y \notin \operatorname{z.div}(M_1)$. Hence $n_1 = 0$. So there exists $p \in M$ such that $n = xp$. So $x(m - yp) = 0$. But $x \notin \operatorname{z.div}(M)$. Thus $m = yp$.

Consider (2). Given $m \in M$ such that $xm = 0$, take $n := 0$. Then $xm = yn$; so there exists $p \in M$ such that $m = yp$ and $n = xp$. Repeat with p in place of m, obtaining $p_1 \in M$ such that $p = yp_1$ and $0 = xp_1$. Induction yields $p_i \in M$ for $i \geq 2$ such that $p_{i-1} = yp_i$ and $0 = xp_i$.

Then $Rp_1 \subset Rp_2 \subset \cdots$ is an ascending chain. It stabilizes as M is Noetherian. Say $Rp_n = Rp_{n+1}$. So $p_{n+1} = zp_n$ for some $z \in R$. Then $p_n = yp_{n+1} = yzp_n$. So $(1 - yz)p_n = 0$. But $y \in \mathfrak{m}$. So $1 - yz$ is a unit. Hence $p_n = 0$. But $m = y^{n+1}p_n$. Thus $m = 0$. Thus $x \notin \operatorname{z.div}(M)$.

Given $n_1 \in M_1 := M/xM$ such that $yn_1 = 0$, take $n \in M$ with n_1 as residue. Then $yn = xm$ for some $m \in M$. So there exists $p \in M$ such that $m = yp$ and $n = xp$. Thus $n_1 = 0$. Thus $y \notin \operatorname{z.div}(M_1)$. Thus x, y form an M-sequence. □

EXERCISE **(23.6)**. — Let R be a local ring, $\mathfrak{m}$ its maximal ideal, M a Noetherian module, $x_1, \dots, x_n \in \mathfrak{m}$, and σ a permutation of $1, \dots, n$. Assume $x_1, \dots, x_n$ form an M-sequence, and prove $x_{\sigma 1}, \dots, x_{\sigma n}$ do too; first, say σ transposes i and $i + 1$.

SOLUTION: Say σ transposes i and $i+1$. Set $M_j := M/\langle x_1, \dots, x_j\rangle$. Then x_i, x_{i+1} form an M_{i-1}-sequence; so x_{i+1}, x_i do too owing to **(23.5)**. So

$$x_1, \dots, x_{i-1}, x_{i+1}, x_i$$

form an M-sequence. But $M/\langle x_1, \dots, x_{i-1}, x_{i+1}, x_i\rangle = M_{i+1}$. Hence $x_{\sigma 1}, \dots, x_{\sigma n}$ form an M-sequence. In general, σ is a composition of transpositions of successive integers; hence, the general assertion follows. □

EXERCISE **(23.7)**. — Prove that a Noetherian local ring A of dimension $r \geq 1$ is regular if and only if its maximal ideal $\mathfrak{m}$ is generated by an A-sequence.

SOLUTION: Assume A is regular. Given a regular sop $x_1, \dots, x_r$, let's show it's an A-sequence. Set $A_1 := A/\langle x_1\rangle$. Then A_1 is regular of dimension $r-1$ by **(21.18)**. So $x_1 \neq 0$. But A is a domain by **(21.19)**. So $x_1 \notin \text{z.div}(A)$. Further, if $r \geq 2$, then the residues of $x_2, \dots, x_r$ form a regular sop of A_1; so we may assume they form an A_1-sequence by induction on r. Thus $x_1, \dots, x_r$ is an A-sequence.

Conversely, if $\mathfrak{m}$ is generated by an A-sequence $x_1, \dots, x_n$, then $n \leq \text{depth}(A) \leq r$ by **(23.3)** and **(23.4)**(3), and $n \geq r$ by **(21.14)**; thus $n = r$, and A is regular. □

EXERCISE **(23.9)**. — Let A be a DVR with fraction field K, and $f \in A$ a nonzero nonunit. Prove A is a maximal proper subring of K. Prove $\dim(A) \neq \dim(A_f)$.

SOLUTION: Let R be a ring, $A \subsetneqq R \subset K$. Then there's an $x \in R - A$. Say $x = ut^n$ where $u \in A^\times$ and t is a uniformizing parameter. Then $n < 0$. Set $y := u^{-1}t^{-n-1}$. Then $y \in A$. So $t^{-1} = xy \in R$. Hence $wt^m \in R$ for any $w \in A^\times$ and $m \in \mathbb{Z}$. Thus $R = K$, as desired.

Since f is a nonzero nonunit, $A \subsetneqq A_f \subset K$. Hence $A_f = K$ by the above. So $\dim(A_f) = 0$. But $\dim(A) = 1$ by **(23.8)**. □

EXERCISE **(23.10)**. — Let k be a field, $P := k[X, Y]$ the polynomial ring in two variables, $f \in P$ an irreducible polynomial. Say $f = \ell(X, Y) + g(X, Y)$ with $\ell(X, Y) = aX + bY$ for $a, b \in k$ and with $g \in \langle X, Y\rangle^2$. Set $R := P/\langle f\rangle$ and $\mathfrak{p} := \langle X, Y\rangle/\langle f\rangle$. Prove that $R_\mathfrak{p}$ is a DVR if and only if $\ell \neq 0$. (Thus $R_\mathfrak{p}$ is a DVR if and only if the plane curve $C : f = 0 \subset k^2$ is nonsingular at $(0, 0)$.)

SOLUTION: Set $A := R_\mathfrak{p}$ and $\mathfrak{m} := \mathfrak{p}A$. Then **(12.18)** and **(12.4)** yield

$$A/\mathfrak{m} = (R/\mathfrak{p})_\mathfrak{p} = k \quad \text{and} \quad \mathfrak{m}/\mathfrak{m}^2 = \mathfrak{p}/\mathfrak{p}^2.$$

First, assume $\ell \neq 0$. Now, the k-vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by the images x and y of X and Y in A. Clearly, the image of f is 0 in $\mathfrak{m}/\mathfrak{m}^2$. Also, $g \in (X, Y)^2$; so its image in $\mathfrak{m}/\mathfrak{m}^2$ is also 0. Hence, the image of ℓ is 0 in $\mathfrak{m}/\mathfrak{m}^2$; that is, x and y are linearly dependent. Now, f cannot generate $\langle X, Y\rangle$, so $\mathfrak{m} \neq 0$; hence, $\mathfrak{m}/\mathfrak{m}^2 \neq 0$ by Nakayama's Lemma, **(10.8)**. Therefore, $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional over k; hence, $\mathfrak{m}$ is principal by **(10.9)**(2). Now, since f is irreducible, A is a domain. Hence, A is a DVR by **(23.8)**.

Conversely, assume $\ell = 0$. Then $f = g \in (X, Y)^2$. So

$$\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{p}/\mathfrak{p}^2 = \langle X, Y\rangle/\langle X, Y\rangle^2.$$

Hence, $\mathfrak{m}/\mathfrak{m}^2$ is 2-dimensional. Therefore, A is not a DVR by **(23.9)**. □

EXERCISE **(23.11)**. — Let k be a field, A a ring intermediate between the polynomial ring and the formal power series ring in one variable: $k[X] \subset A \subset k[[X]]$. Suppose that A is local with maximal ideal $\langle X \rangle$. Prove that A is a DVR. (Such local rings arise as rings of power series with curious convergence conditions.)

SOLUTION: Let's show that the ideal $\mathfrak{a} := \bigcap_{n \geq 0} \langle X^n \rangle$ of A is zero. Clearly, $\mathfrak{a}$ is a subset of the corresponding ideal $\bigcap_{n \geq 0} \langle X^n \rangle$ of $k[[X]]$, and the latter ideal is clearly zero. Hence **(23.2)** implies A is a DVR. □

EXERCISE **(23.12)**. — Let L/K be an algebraic extension of fields, $X_1, \ldots, X_n$ variables, P and Q the polynomial rings over K and L in $X_1, \ldots, X_n$.

(1) Let $\mathfrak{q}$ be a prime of Q, and $\mathfrak{p}$ its contraction in P. Prove $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q})$.
(2) Let $f, g \in P$ be two polynomials with no common prime factor in P. Prove that f and g have no common prime factor $q \in Q$.

SOLUTION: Since L/K is algebraic, Q/P is integral. Furthermore, P is normal, and Q is a domain. Hence we may apply the Going Down Theorem **(14.9)**. So given any chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{p}$, we can proceed by descending induction on i for $0 \leq i \leq r$, and thus construct a chain of primes $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r = \mathfrak{q}$ with $\mathfrak{q}_i \cap P = \mathfrak{p}_i$. Thus $\operatorname{ht} \mathfrak{p} \leq \operatorname{ht} \mathfrak{q}$. Conversely, any chain of primes $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r = \mathfrak{q}$ contracts to a chain of primes $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{p}$, and $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$ by Incomparability, **(14.3)**; whence, $\operatorname{ht} \mathfrak{p} \geq \operatorname{ht} \mathfrak{q}$. Hence $\operatorname{ht} \mathfrak{p} = \operatorname{ht} \mathfrak{q}$. Thus (1) holds.

Alternatively, by **(15.13)**, $\operatorname{ht}(\mathfrak{p}) + \dim(P/\mathfrak{p}) = n$ and $\operatorname{ht}(\mathfrak{q}) + \dim(Q/\mathfrak{q}) = n$ as both P and Q are polynomial rings in n variables over a field. However, by **(15.12)**, $\dim P/\mathfrak{p} = \operatorname{tr.deg}_K \operatorname{Frac}(P/\mathfrak{p})$ and $\dim Q/\mathfrak{q} = \operatorname{tr.deg}_L \operatorname{Frac}(Q/\mathfrak{q})$, and these two transcendence degrees are equal as Q/P is an integral extension. Thus again, (1) holds.

Suppose f and g have a common prime factor $q \in Q$, and set $\mathfrak{q} := Qq$. Then the maximal ideal $\mathfrak{q}Q_{\mathfrak{q}}$ of $Q_{\mathfrak{q}}$ is principal and nonzero. Hence $Q_{\mathfrak{q}}$ is a DVR by **(23.8)**. Thus $\operatorname{ht}(\mathfrak{q}) = 1$. Set $\mathfrak{p} := \mathfrak{q} \cap P$. Then $\mathfrak{p}$ contains f; whence, $\mathfrak{p}$ contains some prime factor p of f. Then $\mathfrak{p} \supseteq Pp$, and Pp is a nonzero prime. Hence $\mathfrak{p} = Pp$ since $\operatorname{ht} \mathfrak{p} = 1$ by (1). However, $\mathfrak{p}$ contains g too. Therefore, $p \mid g$, contrary to the hypothesis. Thus (2) holds. (Caution: if $f := X_1$ and $g := X_2$, then f and g have no common factor, yet there are no φ and ψ such that $\varphi f + \psi g = 1$.) □

EXERCISE **(23.14)**. — Let R be a Noetherian ring. Show that R is reduced if and only if (R_0) and (S_1) hold.

SOLUTION: Assume (R_0) and (S_1) hold. Consider an irredundant primary decomposition $\langle 0 \rangle = \bigcap \mathfrak{q}_i$. Set $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$. Then $\mathfrak{p}_i$ is minimal by (S_1), and $\mathfrak{p}_i = \mathfrak{q}_i$ by (R_0) and **(18.22)**. So $\langle 0 \rangle = \bigcap \mathfrak{p}_i = \sqrt{\langle 0 \rangle}$. Thus R is reduced.

Conversely, assume R is reduced. Then $R_{\mathfrak{p}}$ is reduced for any prime $\mathfrak{p}$ by **(13.15)**. So if $\mathfrak{p}$ is minimal, then $R_{\mathfrak{p}}$ is a field. Thus (R_0) holds. But $\langle 0 \rangle = \bigcap_{\mathfrak{p} \text{ minimal}} \mathfrak{p}$. So $\mathfrak{p}$ is minimal whenever $\mathfrak{p} \in \operatorname{Ass}(R)$ by **(18.19)**. Thus R satisfies (S_1). □

EXERCISE **(23.19)**. — Prove that a Noetherian domain R is normal if and only if, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_{\mathfrak{p}}$ is principal.

SOLUTION: Assume R normal. Say $\mathfrak{p} \in \operatorname{Ass}(R/\langle x \rangle)$. Then $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}(R_{\mathfrak{p}}/\langle x/1 \rangle)$ by **(17.9)**. So $\operatorname{depth}(R_{\mathfrak{p}}) = 1$. But $R_{\mathfrak{p}}$ is normal by **(11.28)**. Hence $\mathfrak{p}R_{\mathfrak{p}}$ is principal by **(23.8)**.

Conversely, assume that, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_{\mathfrak{p}}$ is principal. Given any prime $\mathfrak{p}$ of height 1, take a nonzero $x \in \mathfrak{p}$. Then $\mathfrak{p}$ is minimal containing $\langle x \rangle$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x \rangle)$ by **(17.17)**. So, by hypothesis, $\mathfrak{p}R_{\mathfrak{p}}$ is principal. So $R_{\mathfrak{p}}$ is a DVR by **(23.8)**. Thus R satisfies (R_1).

Given any prime $\mathfrak{p}$ with $\operatorname{depth}(R_{\mathfrak{p}}) = 1$, say $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}(R_{\mathfrak{p}}/\langle x/s \rangle)$ with $x \neq 0$. Then $\langle x/s \rangle = \langle x/1 \rangle \subset R_{\mathfrak{p}}$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x \rangle)$ by **(17.9)**. So, by hypothesis, $\mathfrak{p}R_{\mathfrak{p}}$ is principal. So $\dim(R_{\mathfrak{p}}) = 1$ by **(23.8)**. Thus R also satisfies (S_2). So R is normal by Serre's Criterion, **(23.17)**. □

Exercise **(23.20)**. — Let R be a Noetherian ring, K its total quotient ring, Set

$$\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\} \quad \text{and} \quad \Sigma := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{depth}(R_{\mathfrak{p}}) = 1 \,\}.$$

Assuming (S_1) holds in R, prove $\Phi \subset \Sigma$, and prove $\Phi = \Sigma$ if and only if (S_2) holds.

Further, without assuming (S_1) holds, prove this canonical sequence is exact:

$$R \to K \to \textstyle\prod_{\mathfrak{p} \in \Sigma} K_{\mathfrak{p}}/R_{\mathfrak{p}}. \tag{23.20.1}$$

Solution: Assume (S_1) holds. Then, given $\mathfrak{p} \in \Phi$, there exists a nonzerodivisor $x \in \mathfrak{p}$. Clearly, $\mathfrak{p}$ is minimal containing $\langle x \rangle$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x \rangle)$ by **(17.17)**. Hence $\operatorname{depth}(R_{\mathfrak{p}}) = 1$ by **(23.4)**(2). Thus $\Phi \subset \Sigma$.

However, as (S_1) holds, (S_2) holds if and only if $\Phi \supset \Sigma$. Thus $\Phi = \Sigma$ if and only if R satisfies (S_2).

Further, without assuming (S_1), consider **(23.20.1)**. Trivially, the composition is zero. Conversely, take an $x \in K$ that vanishes in $\prod_{\mathfrak{p} \in \Sigma} K_{\mathfrak{p}}/R_{\mathfrak{p}}$. Say $x = a/b$ with $a, b \in R$ and b a nonzerodivisor. Then $a/1 \in bR_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Sigma$. But $b/1 \in R_{\mathfrak{p}}$ is, clearly, a nonzerodivisor for any prime $\mathfrak{p}$. Hence, if $\mathfrak{p} \in \operatorname{Ass}(R_{\mathfrak{p}}/bR_{\mathfrak{p}})$, then $\mathfrak{p} \in \Sigma$ by **(23.4)**(2). Therefore, $a \in bR$ by **(18.25)**. Thus $x \in R$. Thus **(23.20.1)** is exact. □

Exercise **(23.21)**. — Let R be a Noetherian ring, and K its total quotient ring. Set $\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\}$. Prove these three conditions are equivalent:

(1) R is normal.
(2) (R_1) and (S_2) hold.
(3) (R_1) and (S_1) hold, and $R \to K \to \prod_{\mathfrak{p} \in \Phi} K_{\mathfrak{p}}/R_{\mathfrak{p}}$ is exact.

Solution: Assume (1). Then R is reduced by **(14.15)**. So **(23.14)** yields (R_0) and (S_1). But $R_{\mathfrak{p}}$ is normal for any prime $\mathfrak{p}$ by **(14.14)**. Thus (2) holds by **(23.8)**.

Assume (2). Then (R_1) and (S_1) hold trivially. Thus **(23.20)** yields (3).

Assume (3). Let $x \in K$ be integral over R. Then $x/1 \in K$ is integral over $R_{\mathfrak{p}}$ for any prime $\mathfrak{p}$. Now, $R_{\mathfrak{p}}$ is a DVR for all $\mathfrak{p}$ of height 1 as R satisfies (R_1). Hence, $x/1 \in R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Phi$. So $x \in R$ by the exactness of the sequence in (3). But R is reduced by **(23.14)**. Thus **(14.15)** yields (1). □

24. Dedekind Domains

Exercise **(24.5)**. — Let R be a domain, S a multiplicative set.

(1) Assume $\dim(R) = 1$. Prove $\dim(S^{-1}R) = 1$ if and only if there is a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

(2) Assume $\dim(R) \geq 1$. Prove $\dim(R) = 1$ if and only if $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero prime $\mathfrak{p}$.

SOLUTION: Consider (1). Suppose $\dim(S^{-1}R) = 1$. Then there's a chain of primes $0 \subsetneqq \mathfrak{p}' \subset S^{-1}R$. Set $\mathfrak{p} := \mathfrak{p}' \cap R$. Then $\mathfrak{p}$ is as desired by **(11.16)**(2).

Conversely, suppose there's a nonzero $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $0 \subsetneqq \mathfrak{p}S^{-1}R$ is a chain of primes by **(11.16)**(2); so $\dim(S^{-1}R) \geq 1$. Now, given a chain of primes $0 = \mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r \subset S^{-1}R$, set $\mathfrak{p}_i := \mathfrak{p}'_i \cap R$. Then $0 = \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \subset R$ is a chain of primes by **(11.16)**(2). So $r \leq 1$ as $\dim(R) = 1$. Thus $\dim(S^{-1}R) = 1$.

Consider (2). If $\dim(R) = 1$, then (1) yields $\dim(R_\mathfrak{p}) = 1$ for every nonzero $\mathfrak{p}$.

Conversely, let $0 = \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \subset R$ be a chain of primes. Set $\mathfrak{p}'_i := \mathfrak{p}_i R_{\mathfrak{p}_i}$. Then $0 = \mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ is a chain of primes by **(11.16)**(2). So if $\dim(R_{\mathfrak{p}_i}) = 1$, then $r \leq 1$. Thus, if $\dim(R_\mathfrak{p}) = 1$ for every nonzero $\mathfrak{p}$, then $\dim(R) \leq 1$, as desired. □

EXERCISE **(24.6)**. — Let R be a Dedekind domain, S a multiplicative set. Prove $S^{-1}R$ is a Dedekind domain if and only if there's a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

SOLUTION: Suppose there's a prime nonzero $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $0 \notin S$. So $S^{-1}R$ is a domain by **(11.3)**. And $S^{-1}R$ is normal by **(11.28)**. Further, $S^{-1}R$ is Noetherian by **(16.7)**. Also, $\dim(S^{-1}R) = 1$ by **(24.5)**(1). Thus $S^{-1}R$ is Dedekind.

The converse results directly from **(24.5)**(1). □

EXERCISE **(24.8)**. — Let R be a Dedekind domain, and $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ideals. By first reducing to the case that R is local, prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}),$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

SOLUTION: By **(13.14)**, it suffices to establish the two equations after localizing at each maximal ideal $\mathfrak{p}$. But localization commutes with sum and intersection by **(12.15)**(4), (5). So the localized equations look like the original ones, but with $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ replaced by $\mathfrak{a}_\mathfrak{p}$, $\mathfrak{b}_\mathfrak{p}$, $\mathfrak{c}_\mathfrak{p}$. Thus we may replace R by $R_\mathfrak{p}$, and so assume R is a DVR.

Referring to **(23.1)**, take a uniformizing parameter t, and say $\mathfrak{a} = \langle t^i \rangle$ and $\mathfrak{b} = \langle t^j \rangle$ and $\mathfrak{c} = \langle t^k \rangle$. Then the two equations in questions are equivalent to these two:

$$\max\bigl\{i, \min\{j,k\}\bigr\} = \min\bigl\{\max\{i,j\}, \max\{i,k\}\bigr\},$$
$$\min\bigl\{i, \max\{j,k\}\bigr\} = \max\bigl\{\min\{i,j\}, \min\{i,k\}\bigr\}.$$

However, these two equations are easy to check for any integers i, j, k. □

EXERCISE **(24.12)**. — Prove that a semilocal Dedekind domain A is a PID. Begin by proving that each maximal ideal is principal.

SOLUTION: Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the maximal ideals of A. Let's prove they are principal, starting with $\mathfrak{p}_1$. By Nakayama's lemma **(10.8)**, $\mathfrak{p}_1 A_{\mathfrak{p}_1} \neq \mathfrak{p}_1^2 A_{\mathfrak{p}_1}$; so $\mathfrak{p}_1 \neq \mathfrak{p}_1^2$. Take $y \in \mathfrak{p}_1 - \mathfrak{p}_1^2$. The ideals $\mathfrak{p}_1^2$, $\mathfrak{p}_2$, …, $\mathfrak{p}_r$ are pairwise comaximal because no two of them lie in the same maximal ideal. Hence, by the Chinese Remainder Theorem, **(1.12)**, there is an $x \in A$ with $x \equiv y \bmod \mathfrak{p}_1^2$ and $x \equiv 1 \bmod \mathfrak{p}_i$ for $i \geq 2$.

The Main Theorem of Classical Ideal Theory, **(24.10)**, yields $\langle x \rangle = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$ with $n_i \geq 0$. But $x \notin \mathfrak{p}_i$ for $i \geq 2$; so $n_i = 0$ for $i \geq 2$. Further, $x \in \mathfrak{p}_1 - \mathfrak{p}_1^2$; so $n_1 = 1$. Thus $\mathfrak{p}_1 = \langle x \rangle$. Similarly, all the other $\mathfrak{p}_i$ are principal.

Finally, let $\mathfrak{a}$ be any nonzero ideal. Then the Main Theorem, **(24.10)**, yields $\mathfrak{a} = \prod \mathfrak{p}_i^{m_i}$ for some m_i. Say $\mathfrak{p}_i = \langle x_i \rangle$. Then $\mathfrak{a} = \prod x_i^{m_i}$, as desired. □

EXERCISE **(24.13)**. — Let R be a Dedekind domain, $\mathfrak{a}$ and $\mathfrak{b}$ two nonzero ideals. Prove (1) every ideal in $R/\mathfrak{a}$ is principal, and (2) $\mathfrak{b}$ is generated by two elements.

SOLUTION: To prove (1), let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the associated primes of $\mathfrak{a}$, and set $S := \bigcap_i (R - \mathfrak{p}_i)$. Then S is multiplicative. Set $R' := S^{-1}R$. Then R' is Dedekind by **(24.6)**. Let's prove R' is semilocal.

Let $\mathfrak{q}$ be a maximal ideal of R', and set $\mathfrak{p} := \mathfrak{q} \cap R$. Then $\mathfrak{q} = \mathfrak{p}R'$ by **(11.16)**. So $\mathfrak{p}$ is nonzero, whence maximal since R has dimension 1. Suppose $\mathfrak{p}$ is distinct from all the $\mathfrak{p}_i$. Then $\mathfrak{p}$ and the $\mathfrak{p}_i$ are pairwise comaximal. So, by the Chinese Remainder Theorem, **(1.12)**, there is a $u \in R$ that is congruent to 0 modulo $\mathfrak{p}$ and to 1 modulo each $\mathfrak{p}_i$. Hence, $u \in \mathfrak{p} \cap S$, but $\mathfrak{q} = \mathfrak{p}R'$, a contradiction. Thus $\mathfrak{p}_1 R', \dots, \mathfrak{p}_r R'$ are all the maximal ideals of R'.

So R' is a PID by **(24.12)**; so every ideal in $R'/\mathfrak{a}R'$ is principal. But by **(12.18)**, $R'/\mathfrak{a}R' = S^{-1}(R/\mathfrak{a})$. Finally, $S^{-1}(R/\mathfrak{a}) = R/\mathfrak{a}$ by **(11.6)** because every $u \in S$ maps to a unit in $R/\mathfrak{a}$ since the image lies in no maximal ideal of $R/\mathfrak{a}$. Thus (1) holds.

Alternatively, we can prove (1) without using **(24.12)**, as follows. The Main Theorem of Classical Ideal Theory, **(24.10)**, yields $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$ for distinct maximal ideals $\mathfrak{p}_i$. The $\mathfrak{p}_i^{n_i}$ are pairwise comaximal. So, by the Chinese Remainder Theorem, **(1.12)**, there's a canonical isomorphism:

$$R/\mathfrak{a} \xrightarrow{\sim} R/\mathfrak{p}_1^{n_1} \times \cdots \times R/\mathfrak{p}_k^{n_k}.$$

Next, let's prove each $R/\mathfrak{p}_i^{n_i}$ is a **Principal Ideal Ring (PIR)**; that is, every ideal is principal. Set $S := R - \mathfrak{p}_i$. Then $S^{-1}(R/\mathfrak{p}_i^{n_i}) = R_{\mathfrak{p}_i}/\mathfrak{p}_i^{n_i} R_{\mathfrak{p}_i}$, and the latter ring is a PIR because $R_{\mathfrak{p}_i}$ is a DVR. However, $R/\mathfrak{p}_i^{n_i} = S^{-1}(R/\mathfrak{p}_i^{n_i})$ by **(11.6)**, because every $u \in S$ maps to a unit in $R/\mathfrak{p}_i^{n_i}$ since $\mathfrak{p}/\mathfrak{p}_i^{n_i}$ is the only prime in $R/\mathfrak{p}_i^{n_i}$.

Finally, given finitely many PIRs $R_1, \dots, R_k$, we must prove their product is a PIR. Consider an ideal $\mathfrak{b} \subset R_1 \times \cdots \times R_k$. Then $\mathfrak{b} = \mathfrak{b}_1 \times \cdots \times \mathfrak{b}_k$ where $\mathfrak{b}_i \subset R_i$ is an ideal by **(1.14)**. Say $\mathfrak{b}_i = \langle a_i \rangle$. Then $\mathfrak{b} = \big\langle (a_1, \dots, a_k) \big\rangle$. Thus again, (1) holds.

Consider (2). Let $x \in \mathfrak{b}$ be nonzero. By (1), there is a $y \in \mathfrak{b}$ whose residue generates $\mathfrak{b}/\langle x \rangle$. Then $\mathfrak{b} = \langle x, y \rangle$. □

25. Fractional Ideals

EXERCISE **(25.2)**. — Let R be a domain, M and N nonzero fractional ideals. Prove that M is principal if and only if there exists some isomorphism $M \simeq R$. Construct the following canonical surjection and canonical isomorphism:

$$\pi\colon M \otimes N \twoheadrightarrow MN \quad \text{and} \quad \varphi\colon (M : N) \xrightarrow{\sim} \operatorname{Hom}(N, M).$$

SOLUTION: If $M \simeq R$, let x correspond to 1; then $M = Rx$. Conversely, assume $M = Rx$. Then $x \neq 0$ as $M \neq 0$. Form the map $R \to M$ with $a \mapsto ax$. It's surjective as $M = Rx$. It's injective as $x \neq 0$ and $M \subset \operatorname{Frac}(R)$.

Form the canonical $M \times N \to MN$ with $(x, y) \mapsto xy$. It's bilinear. So it induces a map $\pi\colon M \otimes N \to MN$, and clearly π is surjective.

Define φ as follows: given $z \in (M : N)$, define $\varphi(z)\colon N \to M$ by $\varphi(z)(y) := yz$. Clearly, φ is R-linear. Say $y \neq 0$. Then $yz = 0$ implies $z = 0$; thus, φ is injective.

Finally, given $\theta\colon N \to M$, fix a nonzero $n \in N$, and set $z := \theta(n)/n$. Given $y \in N$, say $y = a/b$ and $n = c/d$ with $a, b, c, d \in R$. Then $bcy = adn$. So

$bc\theta(y) = ad\theta(n)$. Hence $\theta(y) = yz$. Thus, φ is surjective, as desired. □

EXERCISE **(25.6)**. — Let R be a domain, M and N fractional ideals. Prove that the map $\pi\colon M \otimes N \to MN$ is an isomorphism if M is locally principal.

SOLUTION: By **(13.17)**, it suffices to prove that, for each maximal ideal $\mathfrak{m}$, the localization $\pi_{\mathfrak{m}}\colon (M \otimes N)_{\mathfrak{m}} \to (MN)_{\mathfrak{m}}$ is bijective. But $(M \otimes N)_{\mathfrak{m}} = M_{\mathfrak{m}} \otimes N_{\mathfrak{m}}$ by **(12.13)**, and $(MN)_{\mathfrak{m}} = M_{\mathfrak{m}}N_{\mathfrak{m}}$ by **(25.4)**. By hypothesis, $M_{\mathfrak{m}} = R_{\mathfrak{m}}x$ for some x. Clearly $R_{\mathfrak{m}}x \simeq R_{\mathfrak{m}}$. And $R_{\mathfrak{m}} \otimes N_{\mathfrak{m}} = N_{\mathfrak{m}}$ by **(8.5)**(2). Thus $\pi_{\mathfrak{m}} \simeq 1_{N_{\mathfrak{m}}}$. □

EXERCISE **(25.11)**. — Let R be a UFD. Show that a fractional ideal M is invertible if and only if M is principal and nonzero.

SOLUTION: By **(25.7)**, a nonzero principal ideal is always invertible.

Conversely, assume M is invertible. Then trivially $M \neq 0$. Say $1 = \sum m_i n_i$ with $m_i \in M$ and $n_i \in M^{-1}$. Fix a nonzero $m \in M$.

Then $m = \sum m_i n_i m$. But $n_i m \in R$ as $m \in M$ and $n_i \in M^{-1}$. Set

$$d := \gcd\{n_i m\} \in R \quad \text{and} \quad x := \textstyle\sum (n_i m/d) m_i \in M.$$

Then $m = dx$.

Given $m' \in M$, write $m'/m = a/b$ where $a, b \in R$ are relatively prime. Then

$$d' := \gcd\{n_i m'\} = \gcd\{n_i ma/b\} = a \gcd\{n_i m\}/b = ad/b.$$

So $m' = (a/b)m = (ad/b)x = d'x$. But $d' \in R$. Thus $M = Rx$. □

EXERCISE **(25.14)**. — Show that a ring is a PID if and only if it's a Dedekind domain and a UFD.

SOLUTION: A PID is Dedekind by **(24.2)**, and is a UFD by **(2.20)**.

Conversely, let R be a Dedekind UFD. Then every nonzero fractional ideal is invertible by **(25.3)** and **(25.13)**, so is principal by **(25.11)**. Thus R is a PID.

Alternatively and more directly, every nonzero prime is of height 1 as $\dim R = 1$, so is principle by **(21.10)**. But, by **(24.10)**, every nonzero ideal is a product of nonzero prime ideals. Thus again, R is a PID. □

EXERCISE **(25.16)**. — Let R be an ring, M an invertible module. Prove that M is finitely generated, and that, if R is local, then M is free of rank 1.

SOLUTION: Say $\alpha\colon M \otimes N \xrightarrow{\sim} R$ and $1 = \alpha(\sum m_i \otimes n_i)$ with $m_i \in M$ and $n_i \in N$. Given $m \in M$, set $a_i := \alpha(m \otimes n_i)$. Form this composition:

$$\beta\colon M = M \otimes R \xrightarrow{\sim} M \otimes M \otimes N = M \otimes N \otimes M \xrightarrow{\sim} R \otimes M = M.$$

Then $\beta(m) = \sum a_i m_i$. But β is an isomorphism. Thus the m_i generate M.

Suppose R is local. Then $R - R^\times$ is an ideal. So $u := \alpha(m_i \otimes n_i) \in R^\times$ for some i. Set $m := u^{-1}m_i$ and $n := n_i$. Then $\alpha(m \otimes n) = 1$. Define $\nu\colon M \to R$ by $\nu(m') := \alpha(m' \otimes n)$. Then $\nu(m) = 1$; so ν is surjective. Define $\mu\colon R \to M$ by $\mu(x) := xm$. Then $\mu\nu(m') = \nu(m')m = \beta(m')$, or $\mu\nu = \beta$. But β is an isomorphism. So ν is injective. Thus ν is an isomorphism, as desired. □

EXERCISE **(25.17)**. — Show these conditions on an R-module M are equivalent:

(1) M is invertible.
(2) M is finitely generated, and $M_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ at each maximal ideal $\mathfrak{m}$.
(3) M is locally free of rank 1.

Assuming the conditions, show M is finitely presented and $M \otimes \operatorname{Hom}(M, R) = R$.

SOLUTION: Assume (1). Then M is finitely generated by **(25.16)**. Further, say $M \otimes N \simeq R$. Let $\mathfrak{m}$ be a maximal ideal. Then $M_\mathfrak{m} \otimes N_\mathfrak{m} \simeq R_\mathfrak{m}$. Hence $M_\mathfrak{m} \simeq R_\mathfrak{m}$ again by **(25.16)**. Thus (2) holds.

Conditions (2) and (3) are equivalent by **(13.23)**.

Assume (3). Then (2) holds; so $M_\mathfrak{m} \simeq R_\mathfrak{m}$ at any maximal ideal $\mathfrak{m}$. Also, M is finitely presented by **(13.22)**; so $\operatorname{Hom}_R(M, R)_\mathfrak{m} = \operatorname{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m}, R_\mathfrak{m})$ by **(12.21)**.

Consider the evaluation map

$$\operatorname{ev}(M, R)\colon M \otimes \operatorname{Hom}(M, R) \to R \quad \text{defined by} \quad \operatorname{ev}(M, R)(m, \alpha) := \alpha(m).$$

Clearly $\operatorname{ev}(M, R)_\mathfrak{m} = \operatorname{ev}(M_\mathfrak{m}, R_\mathfrak{m})$. Clearly $\operatorname{ev}(R_\mathfrak{m}, R_\mathfrak{m})$ is bijective. Hence $\operatorname{ev}(M, R)$ is bijective by **(13.17)**. Thus the last assertions hold; in particular, (1) holds. □

26. Arbitrary Valuation Rings

EXERCISE **(26.3)**. — Let V be a domain. Show that V is a valuation ring if and only if, given any two ideals $\mathfrak{a}$ and $\mathfrak{b}$, either $\mathfrak{a}$ lies in $\mathfrak{b}$ or $\mathfrak{b}$ lies in $\mathfrak{a}$.

SOLUTION: First, suppose V is a valuation ring. Suppose also $\mathfrak{a} \not\subset \mathfrak{b}$; say $x \in \mathfrak{a}$, but $x \notin \mathfrak{b}$. Take $y \in \mathfrak{b}$. Then $x/y \notin V$; else $x = (x/y)y \in \mathfrak{b}$. So $y/x \in V$. Hence $y = (y/x)x \in \mathfrak{a}$. Thus $\mathfrak{b} \subset \mathfrak{a}$.

Conversely, let $x, y \in V - \{0\}$, and suppose $x/y \notin V$. Then $\langle x \rangle \not\subset \langle y \rangle$; else, $x = wy$ with $w \in V$. Hence $\langle y \rangle \subset \langle x \rangle$ by hypothesis. So $y = zx$ for some $z \in V$; in other words, $y/x \in V$. Thus V is a valuation ring. □

EXERCISE **(26.4)**. — Let V be a valuation ring, $\mathfrak{m}$ its maximal ideal, and $\mathfrak{p} \subset \mathfrak{m}$ another prime ideal. Prove that $V_\mathfrak{p}$ is a valuation ring, that its maximal ideal $\mathfrak{p}V_\mathfrak{p}$ is equal to $\mathfrak{p}$, and that $V/\mathfrak{p}$ is a valuation ring of the field $V_\mathfrak{p}/\mathfrak{p}$.

SOLUTION: First, set $K := \operatorname{Frac}(V_\mathfrak{p})$. So $K = \operatorname{Frac}(V)$. Let $x \in K - V_\mathfrak{p}$. Then $1/x \in V \subset V_\mathfrak{p}$. Thus $V_\mathfrak{p}$ is a valuation ring.

Second, let $r/s \in \mathfrak{p}V_\mathfrak{p}$ where $r \in \mathfrak{p} - \{0\}$ and $s \in V - \mathfrak{p}$. Then $s/r \notin V$, else $s = (s/r)r \in \mathfrak{p}$. Hence $r/s \in V$. Now, $(r/s)s = r \in \mathfrak{p}$, but $s \notin \mathfrak{p}$; since $\mathfrak{p}$ is prime, $r/s \in \mathfrak{p}$. Thus $\mathfrak{p}V_\mathfrak{p} = \mathfrak{p}$.

Third, to prove $V/\mathfrak{p}$ is a valuation ring of $V_\mathfrak{p}/\mathfrak{p}V_\mathfrak{p}$, we need only show that, whenever $x \in V_\mathfrak{p} - V$, then $x^{-1} \in V$. But, V is a valuation ring; hence, $x^{-1} \in V$. □

EXERCISE **(26.5)**. — Prove that a valuation ring V is normal.

SOLUTION: Set $K := \operatorname{Frac}(V)$, and let $\mathfrak{m}$ be the maximal ideal. Take $x \in K$ integral over V, say $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in V$. Then

$$1 + a_1 x^{-1} + \cdots + a_n x^{-n} = 0. \qquad \textbf{(26.5.1)}$$

If $x \notin V$, then $x^{-1} \in \mathfrak{m}$ by **(26.2)**. So **(26.5.1)** yields $1 \in \mathfrak{m}$, a contradiction. Hence $x \in V$. Thus V is normal. □

EXERCISE **(26.10)**. — Let K be a field, $\mathcal{S}$ the set of local subrings with fraction field K, ordered by domination. Show its maximal elements are the valuation rings.

Solution: Let V be maximal in $\mathcal{S}$. By **(26.9)**, V is dominated by a valuation ring V' of K. By maximality, $V = V'$.

Conversely, let V be a valuation ring of K. Then V lies in $\mathcal{S}$ by **(26.2)**. Let $V' \in \mathcal{S}$ dominate V. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the maximal ideals of V and V'. Take any nonzero $x \in V'$. Then $1/x \notin \mathfrak{m}'$ as $1 \notin \mathfrak{m}'$; so also $1/x \notin \mathfrak{m}$. So $x \in V$ by **(26.2)**. Hence, $V' = V$. Thus V is maximal in $\mathcal{S}$. □

Exercise **(26.15)**. — Let V be a valuation ring, such as a DVR, whose value group Γ is **Archimedean**; that is, given any nonzero $\alpha, \beta \in \Gamma$, there's $n \in \mathbb{Z}$ such that $n\alpha > \beta$. Show that V is a maximal proper subring of its fraction field K.

Solution: Let R be a subring of K strictly containing V, and fix $a \in R - V$. Given $b \in K$, let α and β be the values of a and b. Then $\alpha < 0$. So, as Γ is Archimedean, there's $n > 0$ such that $-n\alpha > -\beta$. Then $v(b/a^n) > 0$. So $b/a^n \in V$. So $b = (b/a^n)a^n \in R$. Thus $R = K$. □

Exercise **(26.16)**. — Let V be a valuation ring. Show that

(1) every finitely generated ideal $\mathfrak{a}$ is principal, and

(2) V is Noetherian if and only if V is a DVR.

Solution: To prove (1), say $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$ with $x_i \neq 0$ for all i. Let v be the valuation. Suppose $v(x_1) \leq v(x_i)$ for all i. Then $x_i/x_1 \in V$ for all i. So $x_i \in \langle x_1 \rangle$. Hence $\mathfrak{a} = \langle x_1 \rangle$. Thus (1) holds.

To prove (2), first assume V is Noetherian. Then V is local by **(26.2)**, and by (1) its maximal ideal $\mathfrak{m}$ is principal. Hence V is a DVR by **(23.8)**. Conversely, assume V is a DVR. Then V is a PID by **(23.1)**, so Noetherian. Thus (2) holds. □

References

[1] Artin, M., "Algebra," Prentice-Hall, 1991.

[2] Atiyah, M., and Macdonald, I., "Introduction to Commutative Algebra," Addison-Wesley, 1969.

[3] Eisenbud, D., "Commutative Algebra with a View Toward Algebraic Geomertry," Springer-Verlag, 1999.

[4] Judson, T., "Abstract Algebra: theory and Applications," Open source, Electronic Book, `http://abstract.ips.edu`, 2011/11/08.

[5] Lang, S., "Undergraduate Analysis," Springer-Verlag, 1997.

[6] Lang, S., "Algebra" Graduate Texts in Mathematics **211**, Springer-Verlag, 2002.

[7] Reid, M., "Undergraduate Commutative Algebra," Cambridge University Press, 1995.

[8] Stark H., "An Introduction to Number Theory," MIT Press, 1978.