A Term of
Commutative Algebra

By Allen ALTMAN
and Steven KLEIMAN

Version of September 1, 2013: `13Ed.tex`

v. edition number for publishing purposes
ISBN 978-0-9885572-1-5

Contents

Preface

There is no shortage of books on Commutative Algebra, but the present book is different. Most books are monographs, with extensive coverage. But there is one notable exception: Atiyah and Macdonald's 1969 classic [**3**]. 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. Doing so lengthened the book considerably. In particular, it led to the addition of appendices on Fitting Ideals and on Cohen–Macaulayness. (All four appendices elaborate on important issues arising in the main text.)

There are 324 exercises below. They include about half the exercises in Atiyah and Macdonald's book; eventually, all will be handled. The disposition of those exercises is indicated in a special index preceding the main index. The 324 also include many exercises that come from other publications and many that originate here. Here the exercises are tailored to provide a means for students to check, to solidify, and to expand their understanding of the material. The exercises are intentionally not difficult, tricky, or involved. Rarely do they introduce new techniques, although some introduce new concepts and many statements are used later.

Students are encouraged to try to solve each and every exercise, and to do so before looking up its solution. If they become stuck, then they should review the relevant material; if they remain stuck, then they should change tack by studying the given solution, possibly discussing it with others, but always making sure they can eventually solve the whole exercise entirely on their own. In any event, 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.

Instructors are encouraged to examine their students, possibly orally at a blackboard, possibly via written tests, on a small, randomly chosen subset of all the exercises that have been assigned over the course of the term for the students to write up in their own words. For use during each exam, instructors should provide students with a special copy of the book that does include the solutions.

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 name it this time. Below, the UMP is fundamental: there are many standard constructions; each has a UMP, which serves to characterize the resulting object 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 climbs to a higher level of abstraction. The discussion is completely elementary, but by far the most abstract in 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 treat primary decomposition in a somewhat 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 use irreducible modules. Nowadays, associated primes are normally defined as prime annihilators of elements, and studied on their own at first; sometimes, as below, irreducible modules are not considered at all in the main development.

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 over an arbitrary ring, rather than finitely generated over a Noetherian ring. Third, there is an elementary 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 of restriction of scalars.

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

Allen B. Altman and Steven L. Kleiman
31 August 2013

This page is intentionally blank!

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 unnamed 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, so that for all practical purposes, R and R' are the same — they are just copies of each other. For example, the polynomial rings $R[X]$ and $R[Y]$ in variables X and Y are canonically isomorphic when X and Y are identified. (Recognizing that an isomorphism is canonical can provide insight and obviate verifications. The notion is psychological, and depends on the context.) Otherwise, we write $R \simeq R'$.

A subset $R'' \subset R$ is a **subring** if R'' is a ring and the inclusion $R'' \hookrightarrow R$ 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) (*Boolean rings*). — The simplest nonzero ring has two elements, 0 and 1. It is unique, and denoted $\mathbb{F}_2$.

Given any ring R and any set X, let R^X denote the set of functions $f\colon X \to R$. Then R^X is, clearly, a ring under valuewise addition and multiplication.

For example, take $R := \mathbb{F}_2$. Given $f\colon X \to R$, put $S := f^{-1}\{1\}$. Then $f(x) = 1$ if $x \in S$, and $f(x) = 0$ if $x \notin S$; in other words, f is the **characteristic function** χ_S. Thus *the characteristic functions form a ring, namely,* $\mathbb{F}_2^X$.

Given $T \subset X$, clearly $\chi_S \cdot \chi_T = \chi_{S\cap T}$. Further, $\chi_S + \chi_T = \chi_{S\triangle T}$, where $S\triangle T$ is the **symmetric difference**:

$$S\triangle T := (S \cup T) - (S \cap T) = (S - T) \cup (T - S);$$

here $S - T$ denotes, as usual, the set of elements of S not in T. Thus *the subsets of X form a ring: sum is symmetric difference, and product is intersection. This ring is canonically isomorphic to* $\mathbb{F}_2^X$.

A ring B is said to be **Boolean** if $f^2 = f$ for all $f \in B$. Clearly, $\mathbb{F}_2^X$ is Boolean.

Suppose X is a topological space, and give $\mathbb{F}_2$ the **discrete** topology; that is, every subset is both open and closed. Consider the continuous functions $f\colon X \to \mathbb{F}_2$. Clearly, they are just the χ_S where S is both open and closed. Clearly, they form a Boolean subring of $\mathbb{F}_2^X$. Conversely, Stone's Theorem **(13.25)** asserts that *every Boolean ring is canonically isomorphic to the ring of continuous functions from a compact Hausdorff topological space X to $\mathbb{F}_2$, or equivalently, isomorphic to the ring of open and closed subsets of X.*

(1.3) (*Polynomial rings*). — Let R be a ring, $P := R[X_1, \ldots, X_n]$ the polynomial ring in n variables (see [**2**, pp. 352–3] or [**8**, 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:

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

In other words, P is universal among R-algebras equipped with a list of n elements: P is one, and it maps uniquely to any other.

Similarly, let $P' := R[\{X_\lambda\}_{\lambda\in\Lambda}]$ be the polynomial ring in an arbitrary list 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 $\pi(X_\lambda) = x_\lambda$.*

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

(1) $0 \in \mathfrak{a}$,
(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 $\mathfrak{a}$, or $\sum Ra_\lambda$, 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:

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

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 $\mathfrak{a}'$.

Exercise **(1.5)**. — Let $\varphi\colon R\to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Set $\mathfrak{a}^e := \varphi(\mathfrak{a})R'$ and $\mathfrak{b}^c := \varphi^{-1}(\mathfrak{b})$. Prove these statements:
(1) Then $\mathfrak{a}^{ec}\supset\mathfrak{a}$ and $\mathfrak{b}^{ce}\subset\mathfrak{b}$. (2) Then $\mathfrak{a}^{ece}=\mathfrak{a}^e$ and $\mathfrak{b}^{cec}=\mathfrak{b}^c$.
(3) If $\mathfrak{b}$ is an extension, then $\mathfrak{b}^c$ is the largest ideal of R with extension $\mathfrak{b}$.
(4) If two extensions have the same contraction, then they are equal.

(1.6) (*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**:

$$\begin{tikzcd} R \arrow[r, "\kappa"] \arrow[dr, "\varphi"'] & R/\mathfrak{a} \arrow[d, "\psi"] \\ & R' \end{tikzcd}$$

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 ψ *is an isomorphism if and only if* φ *is surjective and* $\mathfrak{a}=\operatorname{Ker}(\varphi)$. Therefore, always

$$R/\operatorname{Ker}(\varphi) \xrightarrow{\sim} \operatorname{Im}(\varphi). \tag{\textbf{1.6.1}}$$

In practice, it is usually more productive 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 universal among R-algebras R' such that $\mathfrak{a}R'=0$.

Above, if $\mathfrak{a}$ is the ideal generated by elements a_λ, then the UMP can be usefully rephrased as follows: $\kappa(a_\lambda)=0$ *for all* λ, *and given* $\varphi\colon R\to R'$ *such that* $\varphi(a_\lambda)=0$ *for all* λ, *there is a unique ring map* $\psi\colon R/\mathfrak{a}\to R'$ *such that* $\psi\kappa=\varphi$.

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

$$\begin{tikzcd} & & R/\mathfrak{a} \arrow[dl, "\psi"] \arrow[dd, bend left, "1"] \\ R \arrow[urr, "\kappa"] \arrow[r, "\varphi"] \arrow[drr, "\kappa"'] & R' \arrow[dr, "\psi'"] & \\ & & R/\mathfrak{a} \end{tikzcd}$$

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 **(1.7)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and $P:=R[X_1,\dots,X_n]$ the polynomial ring. Prove $P/\mathfrak{a}P = (R/\mathfrak{a})[X_1,\dots,X_n]$.

Proposition **(1.8)**. — *Let* R *be a ring,* $P:=R[X]$ *the polynomial ring in one variable,* $a\in R$, *and* $\pi\colon P\to R$ *the* R*-algebra map defined by* $\pi(X):=a$. *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 $\operatorname{Ker}(\pi)=\langle X-a\rangle$. Finally, **(1.6.1)** yields $R[X]/\langle X-a\rangle \xrightarrow{\sim} R$. □

(1.9) (*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

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

Clearly, φ is surjective, and $\operatorname{Ker}(\varphi)=\mathfrak{b}$. Hence, owing to **(1.6)**, φ factors through the canonical isomorphism ψ in this commutative diagram:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & R/\mathfrak{b} \arrow[d, "\psi"', "\simeq"] \\ R/\mathfrak{a} \arrow[r] & (R/\mathfrak{a})\big/(\mathfrak{b}/\mathfrak{a}) \end{tikzcd}$$

Exercise **(1.10)**. — Let R be ring, and $P := R[X_1, \ldots, X_n]$ the polynomial ring. Let $m \le n$ and $a_1, \ldots, a_m \in R$. Set $\mathfrak{p} := \langle X_1 - a_1, \ldots, X_m - a_m\rangle$. Prove that $P/\mathfrak{p} = R[X_{m+1}, \ldots, X_n]$.

(1.11) (*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 idempotents**. Conversely, if two elements $e_1, e_2 \in R$ satisfy $e_1 + e_2 = 1$ and $e_1e_2 = 0$, then they are complementary idempotents, as for each i,

$$e_i = e_i \cdot 1 = e_i(e_1 + e_2) = e_i^2.$$

We denote the set of all idempotents by $\mathrm{Idem}(R)$. Let $\varphi\colon R \to R'$ be a ring map. Then $\varphi(e)$ is idempotent. So the restriction of φ to $\mathrm{Idem}(R)$ is a map

$$\mathrm{Idem}(\varphi)\colon\ \mathrm{Idem}(R) \to \mathrm{Idem}(R').$$

Example **(1.12)**. — 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 **(1.13)**. — *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 $xye = xye^2 = (xe)(ye)$. Similarly, define $\varphi''\colon R \to R''$ by $\varphi''(x) := xe'$; then φ'' is a ring map. So 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 **(1.14)** (*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

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

(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 $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ 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 **(1.15)**. — First, given a prime number p and a $k \ge 1$, 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 **(1.16)**. — 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 $R/\mathfrak{a} = (R'/\mathfrak{a}') \times (R''/\mathfrak{a}'')$.

Exercise **(1.17)**. — Let R be a ring, and e, e' idempotents. (See **(10.7)** also.)

(1) Set $\mathfrak{a} := \langle e\rangle$. Show $\mathfrak{a}$ is **idempotent**; that is, $\mathfrak{a}^2 = \mathfrak{a}$.
(2) Let $\mathfrak{a}$ be a principal idempotent ideal. Show $\mathfrak{a}\langle f\rangle$ with f idempotent.
(3) Set $e'' := e + e' - ee'$. Show $\langle e, e'\rangle = \langle e''\rangle$ and e'' is idempotent.
(4) Let $e_1, \ldots, e_r$ be idempotents. Show $\langle e_1, \ldots, e_r\rangle = \langle f\rangle$ with f idempotent.
(5) Assume R is Boolean. Show every finitely generated ideal is principal.

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. Finally, 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) $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$.

(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 two nonzero polynomials f and g, not only is their product fg nonzero, but its leading term is the product of those of f and g; so

$$\deg(fg) = \deg(f)\deg(g). \qquad \textbf{(2.3.1)}$$

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

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

Hence the polynomial ring in an arbitrary set of variables $R[\{X_\lambda\}_{\lambda\in\Lambda}]$ is a domain, since any two elements lie in a polynomial subring in finitely many of the X_λ.

Similarly, if $f, g \in R[X]$ with $fg = 1$, then $f, g \in R$, because the product of the leading terms of f and g is constant. So by induction, if $f, g \in R[X_1, \ldots, X_n]$ with $fg = 1$, then $f, g \in R$. This reasoning can fail if R is not a domain. For example, if $a^2 = 0$ in R, then $(1 + aX)(1 - aX) = 1$ in $R[X]$.

The fraction field $\mathrm{Frac}(R[\{X_\lambda\}_{\lambda\in\Lambda}])$ is called the field of **rational functions,** and is also denoted by $K(\{X_\lambda\}_{\lambda\in\Lambda})$ 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 as a subring.

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 is a product of irreducible elements in a unique way up to order and units.

In general, prime elements are irreducible; 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 [**2**, p. 398, p. 401], [**8**, 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: Set $S := \varphi^{-1}T$. If T is multiplicative, then $1 \in S$ as $\varphi(1) = 1 \in T$, and $x, y \in S$ implies $xy \in S$ as $\varphi(xy) = \varphi(x)\varphi(y) \in T$; thus S is multiplicative.

If S is multiplicative, then $1 \in T$ as $1 \in S$ and $\varphi(1) = 1$; further, $x, y \in S$ implies $\varphi(x)$, $\varphi(y)$, $\varphi(xy) \in T$. If φ is surjective, then every $x' \in T$ is of the form $x' = \varphi(x)$ for some $x \in S$. Thus if φ is surjective, then T is multiplicative if $\varphi^{-1}T$ is. □

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)**. □

Corollary **(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 $R[X_1, \ldots, X_n]$ 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.

Exercise **(2.11)**. — Let $R := R' \times R''$ be a **product** of rings, $\mathfrak{p} \subset R$ an ideal. Show $\mathfrak{p}$ is prime if and only if either $\mathfrak{p} = \mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $\mathfrak{p} = R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime.

Exercise **(2.12)**. — Let R be a domain, and $x, y \in R$. Assume $\langle x \rangle = \langle y \rangle$. Show $x = uy$ for some unit u.

Definition **(2.13)**. — 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 **(2.14)**. — 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 $\langle X \rangle \subsetneqq \langle X, Y \rangle$. Moreover, $\langle X, Y \rangle$ is maximal if and only if R is a field by **(1.10)** and by **(2.17)** below.

Proposition **(2.15)**. — *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 **(1.4)** 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 **(1.4)**. Thus R is a field. □

Exercise **(2.16)**. — Let k be a field, R a nonzero ring, $\varphi\colon k \to R$ a ring map. Prove φ is injective.

Corollary **(2.17)**. — *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 **(1.9)**. Hence the assertion results from **(2.15)**. □

Exercise **(2.18)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal, $R[X]$ the polynomial ring. Show that $\mathfrak{p}R[X]$ and $\mathfrak{p}R[X]+\langle X\rangle$ are prime ideals of $R[X]$, and that if $\mathfrak{p}$ is maximal, then so is $\mathfrak{p}R[X]+\langle X\rangle$.

Exercise **(2.19)**. — Let B be a Boolean ring. Show that every prime $\mathfrak{p}$ is maximal, and $B/\mathfrak{p} = \mathbb{F}_2$.

Exercise **(2.20)**. — Let R be a ring. Assume that, given $x \in R$, there is $n \ge 2$ with $x^n = x$. Show that every prime $\mathfrak{p}$ is maximal.

Example **(2.21)**. — 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 **(1.10)**; so $\mathfrak{m}$ is maximal by **(2.17)**.

Exercise **(2.22)**. — Prove the following statements or give a counterexample.

(1) The complement of a multiplicative subset 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 **(1.9)**, an ideal $n' \subset R/\mathfrak{a}$ is maximal if and only if $\kappa^{-1}\mathfrak{n}' \subset R$ is maximal.

Exercise **(2.23)**. — Let k be a field, $P := k[X_1, \dots, X_n]$ the polynomial ring, $f \in P$ nonzero. Let d be the highest power of any variable appearing in f.

(1) Let $S \subset k$ have at least $d+1$ elements. Proceeding by induction on n, find $a_1, \dots, a_n \in S$ with $f(a_1, \dots, a_n) \ne 0$.

(2) Using the algebraic closure K of k, find a maximal ideal $\mathfrak{m}$ of P with $f \notin \mathfrak{m}$.

Corollary **(2.24)**. — *In a ring, every maximal ideal is prime.*

Proof: A field is a domain by **(2.3)**. So **(2.9)** and **(2.17)** yield the result. □

(2.25) (*PIDs*). — A domain R is called a **Principal Ideal Domain** (PID) if every ideal is principal. Examples include a field k, the polynomial ring $k[X]$ in one variable, and the ring $\mathbb{Z}$ of integers. Every PID is a UFD by [**2**, (2.12), p. 396], [**8**, 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 **(2.17)** implies that $R/\langle p\rangle$ is a field.

Exercise **(2.26)**. — 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 **(2.27)**. — 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 $P/\mathfrak{m} \xrightarrow{\sim} k[X]/\langle g'\rangle$ by **(1.7)** and **(1.9)**, and $k[X]/\langle g'\rangle$ is a field by **(2.25)**; hence, $\mathfrak{m}$ is maximal by **(2.17)**.

Theorem **(2.28)**. — *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 $\mathfrak{p} \ne \langle 0\rangle$. 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 $\mathfrak{p} \ne \langle f_1\rangle$. Then there is a prime $f_2 \in \mathfrak{p} - \langle f_1\rangle$. Set $K := \mathrm{Frac}(R)$. Gauss's Lemma [**2**, p. 401], [**8**, 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 **(2.25)** and **(2.26)** 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 $R \cap \mathfrak{p} \ne 0$. 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 **(2.25)**. Set $\mathfrak{q} := \mathfrak{p}/\langle p\rangle \subset k[X]$. Then $k[X]/\mathfrak{q} = P/\mathfrak{p}$ by **(1.7)** and **(1.9)**. 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 **(2.25)**. So $\mathfrak{p}$ is maximal by **(1.9)**. 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 **(2.29)**. — Preserve the setup of **(2.28)**. 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 **(2.30)**. — *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 [**11**, pp. 25, 26], [**10**, p. 880, p. 884], $\mathcal{S}$ has a maximal element, and it is the desired maximal ideal. □

Corollary **(2.31)**. — *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 **(1.4)**, x is a unit if and only if $\langle x\rangle$ is not proper. Apply **(2.30)**. □

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, $x \in R$, and $u \in R^\times$. Then $x \in \operatorname{rad}(R)$ if and only if $u - xy \in \operatorname{rad}(R)$ is a unit for all $y \in R$. In particular, the sum of an element of $\operatorname{rad}(R)$ and a unit is a unit.*

Proof: Assume $x \in \operatorname{rad}(R)$. Let $\mathfrak{m}$ be a maximal ideal. Suppose $u - xy \in \mathfrak{m}$. Since $x \in \mathfrak{m}$ too, also $u \in \mathfrak{m}$, a contradiction. Thus $u - xy$ is a unit by **(2.31)**. In particular, taking $y := -1$ yields $u + x \in R^\times$.

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 $xy + m = u$. Then $u - xy = m \in \mathfrak{m}$. So $u - xy$ is not a unit by **(2.31)**, or directly by **(1.4)**. □

Exercise **(3.3)**. — Let R be a ring, $\mathfrak{a} \subset \operatorname{rad}(R)$ an ideal, $w \in R$, and $w' \in R/\mathfrak{a}$ its residue. Prove that $w \in R^\times$ if and only if $w' \in (R/\mathfrak{a})^\times$. What if $\mathfrak{a} \not\subset \operatorname{rad}(R)$?

Corollary **(3.4)**. — *Let R be a ring, $\mathfrak{a}$ an ideal, $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Assume $\mathfrak{a} \subset \operatorname{rad}(R)$. Then $\operatorname{Idem}(\kappa)$ is injective.*

Proof: Given $e, e' \in \operatorname{Idem}(R)$ with $\kappa(e) = \kappa(e')$, set $x := e - e'$. Then

$$x^3 = e^3 - 3e^2e' + 3ee'^2 - e'^3 = e - e' = x.$$

Hence $x(1 - x^2) = 0$. But $\kappa(x) = 0$; so $x \in \mathfrak{a}$. But $\mathfrak{a} \subset \operatorname{rad}(R)$. Hence $1 - x^2$ is a unit by **(3.2)**. Thus $x = 0$. Thus $\operatorname{Idem}(\kappa)$ is injective. □

Definition **(3.5)**. — 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 **(3.6)** (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 **(2.31)**. So $\mathfrak{n} = \mathfrak{m}$. Thus $\mathfrak{n}$ is an ideal. □

Example **(3.7)**. — The product ring $R' \times R''$ is not local by **(3.6)** if both R' and R'' are nonzero. Indeed, $(1, 0)$ and $(0, 1)$ are nonunits, but their sum is a unit.

Exercise **(3.8)**. — Let A be a local ring. Find its idempotents e.

Exercise **(3.9)**. — 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 **(3.10)**. — 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 $i_j \ge 0$. The term $a_{(0)}$ where $(0) := (0, \dots, 0)$ is called the *constant term.* 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 **(1.9)** yields $P/\mathfrak{n} = R/\mathfrak{m}$.

A power series f is a unit if and only if its constant term $a_{(0)}$ is a unit. Indeed, if $ff' = 1$, then $a_{(0)}a'_{(0)} = 1$ where $a'_{(0)}$ is the constant term of f'. Conversely, if $a_{(0)}$ is a unit, then $f = a_{(0)}(1 - g)$ with $g \in \mathfrak{a}$. Set $f' := a_{(0)}^{-1}(1 + g + g^2 + \cdots)$; this sum makes sense as the component of degree d involves only the first $d + 1$ summands. Clearly $f \cdot f' = 1$.

Suppose R is a local ring with maximal ideal $\mathfrak{m}$. Given a power series $f \notin \mathfrak{n}$, its initial term lies outside $\mathfrak{m}$, so is a unit by **(2.31)**. So f itself is a unit. Hence the nonunits constitute $\mathfrak{n}$. Thus **(3.6)** implies *P is local with maximal ideal $\mathfrak{n}$.*

Example **(3.11)**. — Let k be a ring, and $A := k[[X]]$ the formal power series ring in one variable. A **formal Laurent series** is a formal sum of the form $\sum_{i=-m}^{\infty} a_i X^i$ with $a_i \in k$ and $m \in \mathbb{Z}$. These 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 $f \ne 0$, 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 $-m \ge n$. 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, $K = \operatorname{Frac}(A)$ because 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 $\mathfrak{m} := \operatorname{Ker}(\varphi)$. Then $\mathfrak{m}$ is maximal by **(2.17)** and **(1.6)**. So by **(2.28)**, $\mathfrak{m}$ 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 **(1.8)**, and so **(3.10)** 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* **(2.28)**.

Proposition **(3.12)**. — *Let R be a ring, S a multiplicative subset, and $\mathfrak{a}$ an ideal with $\mathfrak{a} \cap S = \emptyset$. Set $\mathcal{S} := \{\text{ideals } \mathfrak{b} \mid \mathfrak{b} \supset \mathfrak{a} \text{ and } \mathfrak{b} \cap S = \emptyset\}$. Then $\mathcal{S}$ has a maximal element $\mathfrak{p}$, and every such $\mathfrak{p}$ is prime.*

Proof: Clearly, $\mathfrak{a} \in \mathcal{S}$, 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 **(3.13)**. — 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 **(3.14)**. — Use Zorn's lemma to prove that any prime ideal $\mathfrak{p}$ contains a prime ideal $\mathfrak{q}$ that is minimal containing any given subset $\mathfrak{s} \subset \mathfrak{p}$.

(3.15) (*Saturated multiplicative subsets*). — Let R be a ring, and S a multiplicative subset. We say S is **saturated** if, given $x, y \in R$ with $xy \in S$, necessarily $x, y \in S$.

For example, the following statements are easy to check. The group of units $R^\times$ and the subset of nonzerodivisors $S_0 := R - \mathrm{z.div}(R)$ are saturated multiplicative subsets. Further, let $\varphi\colon R \to R'$ be a ring map, $T \subset R'$ a subset. If T is saturated multiplicative, then so is $\varphi^{-1}T$. The converse holds if φ is surjective.

Exercise **(3.16)**. — Let R be a ring, S a subset. Show that S is saturated multiplicative if and only if $R - S$ is a union of primes.

Exercise **(3.17)**. — Let R be a ring, and S a multiplicative subset. Define its **saturation** to be the subset

$$\overline{S} := \{\, x \in R \mid \text{there is } y \in R \text{ with } xy \in S\,\}.$$

(1) Show (a) that $\overline{S} \supset S$, and (b) that $\overline{S}$ is saturated multiplicative, and (c) that any saturated multiplicative subset T containing S also contains $\overline{S}$.

(2) Show that $R - \overline{S}$ is the union U of all the primes $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

(3) Let $\mathfrak{a}$ be an ideal; assume $S = 1 + \mathfrak{a}$; set $W := \bigcup_{\mathfrak{p}\in \mathbf{V}(\mathfrak{a})} \mathfrak{p}$. Show $R - \overline{S} = W$.

(4) Given $f \in R$, let $\overline{S}_f$ denote the saturation of the multiplicative subset of all powers of f. Given $f, g \in R$, show $\overline{S}_f \subset \overline{S}_g$ if and only if $\sqrt{\langle f\rangle} \supset \sqrt{\langle g\rangle}$.

Exercise **(3.18)**. — Let R be a nonzero ring, S a subset. Show S is maximal in the set $\mathfrak{S}$ of multiplicative subsets T of R with $0 \notin T$ if and only if $R - S$ is a **minimal** prime — that is, it is a prime containing no smaller prime.

Lemma **(3.19)** (Prime Avoidance). — *Let R be a ring, $\mathfrak{a}$ a subset of R that is stable under addition and multiplication, and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ ideals such that $\mathfrak{p}_3, \dots, \mathfrak{p}_n$ 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 $x_j \in \mathfrak{p}_j$. □

Exercise **(3.20)**. — Let k be a field, $\mathcal{S} \subset k$ a subset of cardinality d at least 2.

(1) Let $P := k[X_1, \dots, X_n]$ be the polynomial ring, $f \in P$ nonzero. Assume the highest power of any X_i in f is less than d. Proceeding by induction on n, show there are $a_1, \dots, a_n \in \mathcal{S}$ with $f(a_1, \dots, a_n) \neq 0$.

(2) Let V be a k-vector space, and $W_1, \dots, W_r$ proper subspaces. Assume $r < d$. Show $\bigcup_i W_i \neq V$.

(3) In (2), let $W \subset \bigcup_i W_i$ be a subspace. Show $W \subset W_i$ for some i.

(4) Let R a k-algebra, $\mathfrak{a}, \mathfrak{a}_1, \dots, \mathfrak{a}_r$ ideals with $\mathfrak{a} \subset \bigcup_i \mathfrak{a}_i$. Show $\mathfrak{a} \subset \mathfrak{a}_i$ for some i.

Exercise **(3.21)**. — Let k be a field, $R := k[X, Y]$ the polynomial ring in two variables, $\mathfrak{m} := \langle X, Y\rangle$. Show $\mathfrak{m}$ is a union of strictly smaller primes.

(3.22) (*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 $n \geq 1$.

Note that, if $x^n = 0$ with $n \geq 1$ and if $\mathfrak{m}$ is any maximal ideal, then $x^n \in \mathfrak{m}$ and so $x \in \mathfrak{m}$ as $\mathfrak{m}$ is prime by **(2.24)**. Thus

$$\mathrm{nil}(R) \subset \mathrm{rad}(R) \qquad \textbf{(3.22.1)}$$

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

Exercise **(3.23)**. — Find the nilpotents in $\mathbb{Z}/\langle n\rangle$. In particular, take $n = 12$.

Exercise **(3.24)**. — Let R be a ring. (1) Assume every ideal not contained in $\mathrm{nil}(R)$ contains a nonzero idempotent. Prove that $\mathrm{nil}(R) = \mathrm{rad}(R)$. (2) Assume R is Boolean. Prove that $\mathrm{nil}(R) = \mathrm{rad}(R) = \langle 0\rangle$.

Exercise **(3.25)**. — 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 **(3.26)**. — Let $e, e' \in \mathrm{Idem}(R)$. Assume $\sqrt{\langle e\rangle} = \sqrt{\langle e'\rangle}$. Show $e = e'$.

Exercise **(3.27)**. — Let R be a ring, $\mathfrak{a}_1$, $\mathfrak{a}_2$ comaximal ideals with $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathrm{nil}(R)$. Show there are complementary idempotents e_1 and e_2 with $e_i \in \mathfrak{a}_i$.

Exercise **(3.28)**. — Let R be a ring, $\mathfrak{a}$ an ideal, $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Assume $\mathfrak{a} \subset \mathrm{nil}(R)$. Show $\mathrm{Idem}(\kappa)$ is bijective.

Theorem **(3.29)** (Scheinnullstellensatz). — *Let R be a ring, $\mathfrak{a}$ an ideal. Then*

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

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 $S := \{1, x, x^2, \dots\}$. Then S is multiplicative, and $\mathfrak{a} \cap S = \emptyset$. By **(3.12)**, 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 $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\supset\mathfrak{a}} \mathfrak{p}$. □

Exercise **(3.30)**. — Let R be a ring. Prove the following statements equivalent:

(1) R has exactly one prime $\mathfrak{p}$;
(2) every element of R is either nilpotent or a unit;
(3) $R/\mathrm{nil}(R)$ is a field.

Proposition **(3.31)**. — *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 $i \le n-1$ and $j \le m-1$, then $i+j \le m+n-2$. 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 **(3.29)**. □

Exercise **(3.32)**. — Let R be a ring, and $\mathfrak{a}$ an ideal. Assume $\sqrt{\mathfrak{a}}$ is finitely generated. Show $\left(\sqrt{\mathfrak{a}}\right)^n \subset \mathfrak{a}$ for all large n.

Exercise **(3.33)**. — 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 $n \ge 1$ such that $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$.

Proposition **(3.34)**. — *A ring R is reduced and has only one minimal prime $\mathfrak{q}$ if and only if R is a domain.*

Proof: Suppose R is reduced, or $\langle 0\rangle = \sqrt{\langle 0\rangle}$. Then $\langle 0\rangle$ is equal to the intersection of all the prime ideals $\mathfrak{p}$ by **(3.29)**. By **(3.14)**, every $\mathfrak{p}$ contains $\mathfrak{q}$. So $\langle 0\rangle = \mathfrak{q}$. Thus R is a domain. The converse is obvious. □

Exercise **(3.35)**. — Let R be a ring. Assume R is reduced and has finitely many minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Prove $\varphi\colon R \to \prod(R/\mathfrak{p}_i)$ is injective, and for each i, there is some $(x_1, \dots, x_n) \in \operatorname{Im}(\varphi)$ with $x_i \ne 0$ but $x_j = 0$ for $j \ne i$.

Exercise **(3.36)**. — Let R be a ring, X a variable, $f := a_0 + a_1X + \cdots + a_nX^n$ and $g := b_0 + b_1X + \cdots + b_mX^m$ polynomials with $a_n \ne 0$ and $b_m \ne 0$. Call f **primitive** if $\langle a_0, \dots, a_n\rangle = R$. Prove the following statements:

(1) Then f is nilpotent if and only if $a_0, \dots, a_n$ are nilpotent.
(2) Then f is a unit if and only if a_0 is a unit and $a_1, \dots, a_n$ are nilpotent.
(3) If f is a zerodivisor, then there is a nonzero $b \in R$ with $bf = 0$; in fact, if $fg = 0$ with m minimal, then $fb_m = 0$ (or $m = 0$).
(4) Then fg is primitive if and only if f and g are primitive.

Exercise **(3.37)**. — Generalize **(3.36)** to the polynomial ring $P := R[X_1, \dots, X_r]$. For (3), reduce to the case of one variable Y via this standard device: take d suitably large, and define $\varphi\colon P \to R[Y]$ by $\varphi(X_i) := Y^{d^i}$.

Exercise **(3.38)**. — Let R be a ring, X a variable. Show that

$$\operatorname{rad}(R[X]) = \operatorname{nil}(R[X]) = \operatorname{nil}(R)R[X].$$

Exercise **(3.39)**. — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $R[[X]]$ the formal power series ring, $\mathfrak{M} \subset R[[X]]$ be a maximal ideal, and $f := \sum a_nX^n \in R[[X]]$. Set $\mathfrak{m} := \mathfrak{M} \cap R$ and $\mathfrak{A} := \left\{ \sum b_nX^n \mid b_n \in \mathfrak{a} \right\}$. Prove the following statements:

(1) If f is nilpotent, then a_n is nilpotent for all n. The converse is false.
(2) Then $f \in \operatorname{rad}(R[[X]])$ if and only if $a_0 \in \operatorname{rad}(R)$.
(3) Assume $X \in \mathfrak{M}$. Then X and $\mathfrak{m}$ generate $\mathfrak{M}$.
(4) Assume $\mathfrak{M}$ is maximal. Then $X \in \mathfrak{M}$ and $\mathfrak{m}$ is maximal.
(5) If $\mathfrak{a}$ is finitely generated, then $\mathfrak{a}R[[X]] = \mathfrak{A}$. The converse may fail.

Example **(3.40)**. — Let R be a ring, $R[[X]]$ the formal power series ring. Then every prime $\mathfrak{p}$ of R is the contraction of a prime of $R[[X]]$. Indeed, $\mathfrak{p}R[[X]] \cap R = \mathfrak{p}$. So by **(3.13)**, there is a prime $\mathfrak{q}$ of $R[[X]]$ with $\mathfrak{q} \cap R = \mathfrak{p}$. In fact, a specific choice for $\mathfrak{q}$ is the set of series $\sum a_nX^n$ with $a_n \in \mathfrak{p}$. Indeed, the canonical map $R \to R/\mathfrak{p}$ induces a surjection $R[[X]] \to R/\mathfrak{p}$ with kernel $\mathfrak{q}$; hence, $R[[X]]/\mathfrak{q} = (R/\mathfrak{p})[[X]]$. Plainly $(R/\mathfrak{p})[[X]]$ is a domain. But **(3.39)**(5) shows $\mathfrak{q}$ may not be equal to $\mathfrak{p}R[[X]]$.

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 UMP 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 UMPs.

(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 $(x, m) \mapsto xm$, which is

(1) **distributive**, $x(m+n) = xm + xn$ and $(x+y)m = xm + xm$,
(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 **(1.4)**, 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 $\mathrm{Ann}(m)$. We call the set of $x \in R$ with $xm = 0$ for all $m \in M$ the **annihilator** of M, and denote it $\mathrm{Ann}(M)$. Clearly, $\mathrm{Ann}(m)$ and $\mathrm{Ann}(M)$ are ideals.

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

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

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

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

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 $\alpha\beta = 1_N$*, where 1_M and 1_N are the identity maps, *and then $\beta = \alpha^{-1}$*. If there is an unnamed 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 $\mathrm{Hom}_R(M, N)$ or simply $\mathrm{Hom}(M, N)$. 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

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

Show that ρ 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' 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 **(1.6)**, so if and only if $\mathfrak{a}M = 0$; as $\mathrm{End}_{\mathbb{Z}}(M)$ may be noncommutative, we must apply **(1.6)** 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, or set of residues,

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

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:

$$\begin{tikzcd} M \arrow[r, "\kappa"] \arrow[dr, "\alpha"'] & M/M' \arrow[d, "\beta"] \\ & N \end{tikzcd}$$

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*

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

In practice, it is usually more productive 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:

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

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

the isomorphism β in this commutative diagram:

$$\begin{tikzcd} N \arrow[r] \arrow[d] & N/M \arrow[d, "\beta"', "\simeq"] \\ N/L \arrow[r] & (N/L)\big/(M/L) \end{tikzcd} \qquad \textbf{(4.8.1)}$$

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:

$$\begin{tikzcd} L \arrow[r] \arrow[d] & L/(L \cap M) \arrow[d, "\beta'"', "\simeq"] \\ L + M \arrow[r] & (L + M)/M \end{tikzcd} \qquad \textbf{(4.8.2)}$$

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

$$\begin{tikzcd} M \arrow[r, "\alpha"] \arrow[dr, "0"'] & N \arrow[r, "\kappa"] \arrow[d, "\beta"] & \operatorname{Coker}(\alpha) \arrow[dl, "\gamma"] \\ & P & \end{tikzcd}$$

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 either **(5.32)**(2) or **(10.5)** below, any two free bases have the same number ℓ of elements, and we say M is **free of rank** ℓ, and we set $\operatorname{rank}(M) := \ell$.

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**, which 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 $m_1/n_1, \ldots, m_r/n_r \in M$, let d be a common multiple of $n_1, \ldots, n_r$. Then $(1/d)\mathbb{Z}$ contains every linear combination $x_1(m_1/n_1) + \cdots + x_\ell(m_\ell/n_\ell)$, but $(1/d)\mathbb{Z} \neq M$.

Moreover, $\mathbb{Q}$ is not algebra finite over $\mathbb{Z}$. Indeed, let $p \in \mathbb{Z}$ be any prime not dividing $n_1 \cdots n_r$. Then $1/p \notin \mathbb{Z}[m_1/n_1, \ldots, m_r/n_r]$.

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

Exercise **(4.13)**. — A finitely generated free module F has finite rank.

Theorem **(4.14)**. — *Let R be a* PID*, E a free module, $\{e_\lambda\}_{\lambda\in\Lambda}$ a (free) basis, and F a submodule. Then F is free, and has a basis indexed by a subset of Λ.*

Proof: Well order Λ. For all λ, let $\pi_\lambda\colon E \to R$ be the λth projection. For all μ, set $E_\mu := \bigoplus_{\lambda\le\mu} Re_\lambda$ and $F_\mu := F \cap E_\mu$. Then $\pi_\mu(F_\mu) = \langle a_\mu\rangle$ for some $a_\mu \in R$ as R is a PID. Choose $f_\mu \in F_\mu$ with $\pi_\mu(f_\mu) = a_\mu$. Set $\Lambda_0 := \{\mu \in \Lambda \mid a_\mu \neq 0\}$.

Say $\sum_{\mu\in\Lambda_0} c_\mu f_\mu = 0$ for some $c_\mu \in R$. Set $\Lambda_1 := \{\mu \in \Lambda_0 \mid c_\mu \neq 0\}$. Suppose $\Lambda_1 \neq \emptyset$. Note Λ_1 is finite. Let μ_1 be the greatest element of Λ_1. Then $\pi_{\mu_1}(f_\mu) = 0$ for $\mu < \mu_1$ as $f_\mu \in E_\mu$. So $\pi_{\mu_1}(\sum c_\mu f_\mu) = c_{\mu_1}a_{\mu_1}$. So $c_{\mu_1}a_{\mu_1} = 0$. But $c_{\mu_1} \neq 0$ and $a_{\mu_1} \neq 0$, a contradiction. Thus $\{f_\mu\}_{\mu\in\Lambda_0}$ is linearly independent.

Note $F = \bigcup_{\lambda\in\Lambda_0} F_\lambda$. Given $\lambda \in \Lambda_0$, set $\Lambda_\lambda := \{\mu \in \Lambda_0 \mid \mu \le \lambda\}$. Suppose λ is least such that $\{f_\mu\}_{\mu\in\Lambda_\lambda}$ does not generate F_λ. Given $f \in F_\lambda$, say $f = \sum_{\mu\le\lambda} c_\mu e_\mu$ with $c_\mu \in R$. Then $\pi_\lambda(f) = c_\lambda$. But $\pi_\lambda(F_\lambda) = \langle a_\lambda\rangle$. So $c_\lambda = b_\lambda a_\lambda$ for some $b_\lambda \in R$. Set $g := f - b_\lambda f_\lambda$. Then $g \in F_\lambda$, and $\pi_\lambda(g) = 0$. So $g \in F_\nu$ for some $\nu \in \Lambda_0$ with $\nu < \lambda$. Hence $g = \sum_{\mu\in\Lambda_\nu} b_\mu f_\mu$ for some $b_\mu \in R$. So $f = \sum_{\mu\in\Lambda_\lambda} b_\mu f_\mu$, a contradiction. Hence $\{f_\mu\}_{\mu\in\Lambda_\lambda}$ generates F_λ. Thus $\{f_\mu\}_{\mu\in\Lambda_0}$ is a basis of F. □

(4.15) (*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 $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$, then $\bigoplus M_\lambda$ is also denoted by $M_{\lambda_1} \oplus \cdots \oplus M_{\lambda_n}$. Further, if $M_\lambda = M$ for all λ, then $\bigoplus M_\lambda$ is also denoted by M^Λ, or by M^n if Λ has just n elements.

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 $\alpha_\kappa\colon L \to M_\kappa$, there is a unique homomorphism $\alpha\colon L \to \prod M_\lambda$ 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,

$$\operatorname{Hom}\big(L, \prod M_\lambda\big) \xrightarrow{\sim} \prod \operatorname{Hom}(L, M_\lambda). \tag{4.15.1}$$

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:

$$\operatorname{Hom}\big(\bigoplus M_\lambda, N\big) \xrightarrow{\sim} \prod \operatorname{Hom}(M_\lambda, N). \tag{4.15.2}$$

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 **(4.15.2)** and **(4.3)**.

Exercise **(4.16)**. — Let Λ be an infinite set, R_λ a nonzero 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 **(4.17)**. — Let R be a ring, M a module, and M', M'' submodules. Show that $M = M' \oplus M''$ if and only if $M = M' + M''$ and $M' \cap M'' = 0$.

Exercise **(4.18)**. — Let L, M, and N be 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 **(4.19)**. — Let L be a module, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove that the injections $\iota_\kappa \colon M_\kappa \to \bigoplus M_\lambda$ induce an injection

$$\bigoplus \mathrm{Hom}(L,\, M_\lambda) \hookrightarrow \mathrm{Hom}(L,\, \bigoplus M_\lambda),$$

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

Exercise **(4.20)**. — Let $\mathfrak{a}$ be an ideal, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove $\mathfrak{a}\big(\bigoplus M_\lambda\big) = \bigoplus \mathfrak{a}M_\lambda$. Prove $\mathfrak{a}(\prod M_\lambda) = \prod \mathfrak{a}M_\lambda$ 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.

In an appendix, we use deteminants to study free modules.

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.

Example **(5.2)**. — (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)**.

(5.3) (*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:

$$0 \to L \xrightarrow{\iota_L} L \oplus N \xrightarrow{\pi_N} N \to 0 \quad \text{where}$$
$$\iota_L(l) := (l, 0) \quad \text{and} \quad \pi_N(l, n) := n.$$

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

Proposition **(5.4)**. — *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 **(4.15)**. □

Exercise **(5.5)**. — Let M' and M'' be modules, $N \subset M'$ a submodule. Set $M := M' \oplus M''$. Using **(5.2)**(1) and **(5.3)** and **(5.4)**, 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. Prove that, if M' and M'' are finitely generated, then so is M.

Proposition **(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. □

(5.8) (*Retraction, section, splits*). — We call a linear map $\rho\colon M \to M'$ a **retraction** of another $\alpha\colon M' \to M$ if $\rho\alpha = 1_{M'}$. Then α is injective and ρ is surjective.

Dually, we call a linear map $\sigma\colon M'' \to M$ a **section** of another $\beta\colon M \to M''$ if $\beta\sigma = 1_{M''}$. Then β is surjective and σ is injective..

We say that a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ **splits** if there is an isomorphism $\varphi\colon M \xrightarrow{\sim} M' \oplus M''$ with $\varphi\alpha = \iota_{M'}$ and $\beta = \pi_{M''}\varphi$.

PROPOSITION **(5.9)**. — *Let $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ be a 3-term exact sequence. Then the following conditions are equivalent:*

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

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 plainly (2) and (3) hold.

Assume (2). Set $\sigma' := 1_M - \alpha\rho$. Then $\sigma'\alpha = \alpha - \alpha\rho\alpha$. But $\rho\alpha = 1_{M'}$ as ρ is a retraction. So $\sigma'\alpha = 0$. Hence there exists $\sigma\colon M'' \to M$ with $\sigma\beta = \sigma'$ by **(5.2)**(2) and the UMP of **(4.9)**. Thus $1_M = \alpha\rho + \sigma\beta$.

Hence $\beta = \beta\alpha\rho + \beta\sigma\beta$. But $\beta\alpha = 0$ as the sequence is exact. So $\beta = \beta\sigma\beta$. But β is surjective. Thus $1_{M''} = \beta\sigma$; that is, (3) holds.

Similarly, $\sigma = \alpha\rho\sigma + \sigma\beta\sigma$. But $\beta\sigma = 1_{M''}$ as (3) holds. So $0 = \alpha\rho\sigma$. But α is injective, as ρ is a retraction of it. Thus $\rho\sigma = 0$. Thus **(4.18)** yields (1).

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

EXAMPLE **(5.10)**. — Let R be a ring, R' an R-algebra, and M an R'-module. Set $H := \operatorname{Hom}_R(R', M)$. Define $\alpha\colon M \to H$ by $\alpha(m)(x) := xm$, and $\rho\colon H \to M$ by $\rho(\theta) := \theta(1)$. Then ρ is a retraction of α, as $\rho(\alpha(m)) = 1\cdot m$. Let $\beta\colon M \to \operatorname{Coker}(\alpha)$ be the quotient map. Then **(5.9)** implies that M is a direct summand of H with $\alpha = \iota_M$ and $\rho = \pi_M$.

EXERCISE **(5.11)**. — 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 **(5.12)**. — Criticize the following misstatement of **(5.9)**: given a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$, there is an isomorphism $M \simeq M' \oplus M''$ if and only if there is a section $\sigma\colon M'' \to M$ of β and α is injective.

LEMMA **(5.13)** (Snake). — *Consider this commutative diagram with exact rows:*

$$\begin{tikzcd}
 & M' \arrow[r, "\alpha"] \arrow[d, "\gamma'"'] & M \arrow[r, "\beta"] \arrow[d, "\gamma"'] & M'' \arrow[r] \arrow[d, "\gamma''"'] & 0 \\
0 \arrow[r] & N' \arrow[r, "\alpha'"] & N \arrow[r, "\beta'"] & N''
\end{tikzcd}$$

It yields the following exact sequence:

$$\operatorname{Ker}(\gamma') \xrightarrow{\varphi} \operatorname{Ker}(\gamma) \xrightarrow{\psi} \operatorname{Ker}(\gamma'') \xrightarrow{\partial} \operatorname{Coker}(\gamma') \xrightarrow{\varphi'} \operatorname{Coker}(\gamma) \xrightarrow{\psi'} \operatorname{Coker}(\gamma''). \tag{5.13.1}$$

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

PROOF: Clearly α restricts to a map φ, because $\alpha\big(\operatorname{Ker}(\gamma')\big) \subset \operatorname{Ker}(\gamma)$ since $\alpha'\gamma'\big(\operatorname{Ker}(\gamma')\big) = 0$. By the UMP discussed in **(4.9)**, α' factors through a unique map φ' because M' goes to 0 in $\operatorname{Coker}(\gamma)$. Similarly, β and β' induce corresponding maps ψ and ψ'. Thus all the maps in **(5.13.1)** 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 **(5.13.1)** is exact at $\operatorname{Ker}(\gamma'')$. Take $m'' \in \operatorname{Ker}(\gamma'')$. 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 $m'' \in \operatorname{Ker}(\partial)$. Then the image of n' in $\operatorname{Coker}(\gamma')$ 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 $m - \alpha(m') \in \operatorname{Ker}(\gamma)$. Since $\beta\big(m - \alpha(m')\big) = m''$, clearly $m'' = \psi(m - \alpha(m'))$; so $m'' \in \operatorname{Im}(\psi)$. Hence $\operatorname{Ker}(\partial) \subset \operatorname{Im}(\psi)$.

Conversely, suppose $m'' \in \operatorname{Im}(\psi)$. We may assume $m \in \operatorname{Ker}(\gamma)$. So $\gamma(m) = 0$ and $\alpha'(n') = 0$. Since α' is injective, $n' = 0$. Thus $\partial(m'') = 0$, and so $\operatorname{Im}(\psi) \subset \operatorname{Ker}(\partial)$. Thus $\operatorname{Ker}(\partial)$ is equal to $\operatorname{Im}(\psi)$; that is, **(5.13.1)** is exact at $\operatorname{Ker}(\gamma'')$.

The other verifications of exactness are similar or easier.

The last two assertions are clearly true. □

EXERCISE **(5.14)**. — Referring to **(4.8)**, give an alternative proof that β is an isomorphism by applying the Snake Lemma to the diagram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d, "\kappa"'] & N/M \arrow[r] \arrow[d, "\beta"'] & 0 \\
0 \arrow[r] & M/L \arrow[r] & N/L \arrow[r, "\lambda"] & (N/L)\big/(M/L) \arrow[r] & 0
\end{tikzcd}$$

EXERCISE **(5.15)** (*Five Lemma*). — Consider this commutative diagram:

$$\begin{tikzcd}
M_4 \arrow[r, "\alpha_4"] \arrow[d, "\gamma_4"'] & M_3 \arrow[r, "\alpha_3"] \arrow[d, "\gamma_3"'] & M_2 \arrow[r, "\alpha_2"] \arrow[d, "\gamma_2"'] & M_1 \arrow[r, "\alpha_1"] \arrow[d, "\gamma_1"'] & M_0 \arrow[d, "\gamma_0"'] \\
N_4 \arrow[r, "\beta_4"] & N_3 \arrow[r, "\beta_3"] & N_2 \arrow[r, "\beta_2"] & N_1 \arrow[r, "\beta_1"] & N_0
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L' \arrow[r] \arrow[d] & L \arrow[r] \arrow[d] & L'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N' \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd} \tag{5.16.1}$$

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

$$\begin{tikzcd} M' \arrow[r, "\beta"] \arrow[d, "\alpha'"'] & M \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & M'' \arrow[d, "\alpha''"'] \\ N' \arrow[r, "\beta'"] & N \arrow[r, "\gamma'"] & N'' \end{tikzcd}$$

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

$$0 \to \mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N). \qquad \textbf{(5.18.1)}$$

(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 **(5.2)**(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 **(5.18.1)** 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 **(5.18.1)** 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 **(5.19)**. — 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 **(5.20)**. — *Let R be a ring, M a module, m_λ for $\lambda \in \Lambda$ generators. Then 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, and 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 **(5.3)**. 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 **(5.21)**. — A module P is called **projective** if, given any surjective linear map $\beta\colon M \twoheadrightarrow N$, every linear map $\alpha\colon P \to N$ **lifts** to one $\gamma\colon P \to M$; namely, $\alpha = \beta\gamma$.

Exercise **(5.22)**. — Show that a free module $R^{\oplus\Lambda}$ is projective.

Theorem **(5.23)**. — *The following conditions on an R-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*

$$\mathrm{Hom}(P, N') \to \mathrm{Hom}(P, N) \to \mathrm{Hom}(P, N''). \qquad \textbf{(5.23.1)}$$

(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 **(5.20)**, 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 **(5.4)**. But by the end of **(4.15)**, that sequence is equal to this one:

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

But $K \oplus P \simeq R^{\oplus\Lambda}$. So owing to **(4.15.2)**, the latter sequence is also equal to

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

Hence **(5.23.1)** is exact by **(5.4)**. Thus (4) holds.

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

$$\mathrm{Hom}(P, M) \xrightarrow{\mathrm{Hom}(P,\beta)} \mathrm{Hom}(P, N) \to 0.$$

In other words, (5) holds.

Assume (5). Then every $\alpha \in \mathrm{Hom}(P, N)$ is the image under $\mathrm{Hom}(P, \beta)$ of some $\gamma \in \mathrm{Hom}(P, M)$. But, by definition, $\mathrm{Hom}(P, \beta)(\gamma) = \beta\gamma$. Thus (1) holds. □

Exercise **(5.24)**. — Let R be a ring, P and N finitely generated modules with P projective. Prove $\mathrm{Hom}(P, N)$ is finitely generated, and is finitely presented if N is.

Lemma **(5.25)** (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** *— namely, a commutative diagram with vertical isomorphisms:*

$$\begin{tikzcd} 0 \arrow[r] & L \oplus P' \arrow[r, "i\oplus 1_{P'}"] \arrow[d, "\beta", "\simeq"'] & P \oplus P' \arrow[r, "(\alpha\ 0)"] \arrow[d, "\gamma", "\simeq"'] & M \arrow[r] \arrow[d, "1_M", "="'] & 0 \\ 0 \arrow[r] & P \oplus L' \arrow[r, "1_P\oplus i'"] & P \oplus P' \arrow[r, "(0\ \alpha')"] & M \arrow[r] & 0 \end{tikzcd}$$

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

$$\begin{tikzcd} 0 \arrow[r] & L \oplus P' \arrow[r, "i\oplus 1_{P'}"] & P \oplus P' \arrow[r, "(\alpha\ 0)"] & M \arrow[r] & 0 \\ 0 \arrow[r] & K \arrow[r] \arrow[u, "\lambda"', "\simeq"] & P \oplus P' \arrow[r, "(\alpha\ \alpha')"] \arrow[u, "\theta"', "\simeq"] & M \arrow[r] \arrow[u, "1_M"', "="] & 0 \end{tikzcd}$$

Take $K := \mathrm{Ker}(\alpha\,\alpha')$. 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 $\theta := \begin{pmatrix} 1 & \pi \\ 0 & 1 \end{pmatrix}$.

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 $\beta := \lambda'\lambda^{-1}$. □

Exercise **(5.26)**. — Let R be a ring, and $0 \to L \to R^n \to M \to 0$ an exact sequence. Prove M is finitely presented if and only if L is finitely generated.

Exercise **(5.27)**. — Let R be a ring, $X_1, X_2, \ldots$ infinitely many variables. Set $P := R[X_1, X_2, \ldots]$ and $M := P/\langle X_1, X_2, \ldots\rangle$. Is M finitely presented? Explain.

Proposition **(5.28)**. — *Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with L finitely generated and M finitely presented. Then N is finitely presented.*

Proof: Let R be the ground ring, $\mu\colon R^m \to M$ any surjection. Set $\nu := \beta\mu$, set $K := \operatorname{Ker}\nu$, and set $\lambda := \mu|K$. Then the following diagram is commutative:

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, "\lambda"'] & R^m \arrow[r, "\nu"] \arrow[d, "\mu"'] & N \arrow[r] \arrow[d, "1_N"'] & 0 \\
0 \arrow[r] & L \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & N \arrow[r] & 0
\end{tikzcd}$$

The Snake Lemma **(5.13)** yields an isomorphism $\operatorname{Ker}\lambda \xrightarrow{\sim} \operatorname{Ker}\mu$. But $\operatorname{Ker}\mu$ is finitely generated by **(5.26)**. So $\operatorname{Ker}\lambda$ is finitely generated. Also, the Snake Lemma implies $\operatorname{Coker}\lambda = 0$ as $\operatorname{Coker}\mu = 0$; so $0 \to \operatorname{Ker}\lambda \to K \xrightarrow{\lambda} L \to 0$ is exact. Hence K is finitely generated by **(5.6)**. Thus N is finitely presented by **(5.26)**. □

Exercise **(5.29)**. — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with M finitely generated and N finitely presented. Prove L is finitely generated.

Proposition **(5.30)**. — *Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with L and N finitely presented. Then M is finitely presented too.*

Proof: Let R be the ground ring, $\lambda\colon R^\ell \to L$ and $\nu\colon R^n \twoheadrightarrow N$ any surjections. Define $\gamma\colon R^\ell \to M$ by $\gamma := \alpha\lambda$. Note R^n is projective by **(5.22)**, and define $\delta\colon R^n \to M$ by lifting ν along β. Define $\mu\colon R^\ell \oplus R^n \to M$ by $\mu := \gamma + \delta$. Then the following diagram is, plainly, commutative, where $\iota := \iota_{R^\ell}$ and $\pi := \pi_{R^n}$:

$$\begin{tikzcd}
0 \arrow[r] & R^\ell \arrow[r, "\iota"] \arrow[d, "\lambda"'] & R^\ell \oplus R^n \arrow[r, "\pi"] \arrow[d, "\mu"'] & R^n \arrow[r] \arrow[d, "\nu"'] & 0 \\
0 \arrow[r] & L \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & N \arrow[r] & 0
\end{tikzcd}$$

Since λ and ν are surjective, the Snake Lemma **(5.13)** yields an exact sequence

$$0 \to \operatorname{Ker}\lambda \to \operatorname{Ker}\mu \to \operatorname{Ker}\nu \to 0,$$

and implies $\operatorname{Coker}\mu = 0$. Also, $\operatorname{Ker}\lambda$ and $\operatorname{Ker}\nu$ are finitely generated by **(5.26)**. So $\operatorname{Ker}\mu$ is finitely generated by **(5.6)**. Thus M is finitely presented by **(5.26)**. □

5. Appendix: Fitting Ideals

(5.31) (*The Ideals of Minors*). — Let R be a ring, $\mathbf{A} := (a_{ij})$ an $m \times n$ matrix with $a_{ij} \in R$. Given $r \in \mathbb{Z}$, let $I_r(\mathbf{A})$ denote the ideal generated by the $r \times r$ minors of $\mathbf{A}$; by convention, we have

$$I_r(\mathbf{A}) = \begin{cases} \langle 0\rangle, & \text{if } r > \min\{m, n\};\\ R, & \text{if } r \le 0.\end{cases} \qquad \textbf{(5.31.1)}$$

Let $\mathbf{B} := (b_{ij})$ be an $r \times r$ submatrix of $\mathbf{A}$. Let $\mathbf{B}_{ij}$ be the $(r-1) \times (r-1)$ submatrix obtained from $\mathbf{B}$ by deleting the ith row and the jth column. For any i, expansion yields $\det(\mathbf{B}) = \sum_{j=1}^{r} (-1)^{i+j} b_{ij} \det(\mathbf{B}_{ij})$. So $I_r(\mathbf{A}) \subset I_{r-1}(\mathbf{A})$. Thus

$$R = I_0(\mathbf{A}) \supset I_1(\mathbf{A}) \supset \cdots. \qquad \textbf{(5.31.2)}$$

Let $\mathbf{U}$ be an invertible $m \times m$ matrix. Then $\det(\mathbf{U})$ is a unit, as $UV = I$ yields $\det(U)\det(V) = 1$. So $I_m(\mathbf{U}) = R$. Thus $I_r(\mathbf{U}) = R$ for all $r \le m$.

Proposition **(5.32)**. — *Let R be a nonzero ring, $\alpha\colon R^n \to R^m$ a map. (1) If α is injective, then $n \le m$. (2) If α is bijective, then $n = m$.*

Proof: For (1), assume $n > m$, and let's show α is not injective.

Let $\mathbf{A}$ be the matrix of α. Note **(5.31.1)** yields $I_n(\mathbf{A}) = \langle 0\rangle$ as $n > m$ and $I_0(\mathbf{A}) = R$. Let r be the largest integer with $\operatorname{Ann}(I_r(\mathbf{A})) = \langle 0\rangle$. Then $0 \le r < n$.

Take any nonzero $x \in I_{r+1}(\mathbf{A})$. If $r = 0$, set $z := (x, 0, \ldots, 0)$. Then $z \ne 0$ and $\alpha(z) = 0$; so α is not injective. So assume $r > 0$.

As $x \ne 0$, also $x \notin \operatorname{Ann}(I_r(\mathbf{A}))$. So there's an $r \times r$ submatrix $\mathbf{B}$ of $\mathbf{A}$ with $x\det(\mathbf{B}) \ne 0$. By renumbering, we may assume that $\mathbf{B}$ is the upper left $r \times r$ submatrix of $\mathbf{A}$. Let $\mathbf{C}$ be the upper left $(r+1) \times (r+1)$ submatrix.

Let c_i be the cofactor of $a_{(r+1)i}$ in $\det(\mathbf{C})$; so $\det(\mathbf{C}) = \sum_{i=1}^{r+1} a_{(r+1)i} c_i$. Then $c_{r+1} = \det(\mathbf{B})$. So $xc_{r+1} \ne 0$. Set $z := x(c_1, \ldots, c_{r+1}, 0, \ldots, 0)$. Then $z \ne 0$.

Let's show $\alpha(z) = 0$. Denote by $\mathbf{A}_k$ the kth row of $\mathbf{A}$, by $\mathbf{D}$ the matrix obtained by replacing the $(r+1)$st row of $\mathbf{C}$ with the first $(r+1)$ entries of $\mathbf{A}_k$, and by $z \cdot \mathbf{A}_k$ the dot product. Then $z \cdot \mathbf{A}_k = x\det(\mathbf{D})$. If $k \le r$, then $\mathbf{D}$ has two equal rows; so $z \cdot \mathbf{A}_k = 0$. If $k \ge r+1$, then $\mathbf{D}$ is an $(r+1) \times (r+1)$ submatrix of $\mathbf{A}$; so $z \cdot \mathbf{A}_k = 0$ as $xI_{r+1}(\mathbf{A}) = 0$. Thus $\alpha(z) = 0$. Thus α is not injective. Thus (1) holds.

For (2), apply (1) to α^{-1} too; thus also $m \le n$. Thus (2) holds. □

Lemma **(5.33)**. — *Let R be a ring, $\mathbf{A}$ an $m \times n$ matrix, $\mathbf{B}$ an $n \times p$ matrix, $\mathbf{U}$ be an invertible $m \times m$ matrix, and $\mathbf{V}$ an invertible $n \times n$ matrix. Then for all r*

$$(1)\ \ I_r(\mathbf{AB}) \subset I_r(\mathbf{A})I_r(\mathbf{B}) \quad \textit{and} \quad (2)\ \ I_r(\mathbf{UAV}) = I_r(\mathbf{A}).$$

Proof: As a matter of notation, given a $p \times q$ matrix $\mathbf{X} := (x_{ij})$, denote its jth column by $\mathbf{X}^j$. Given sequences $I := (i_1, \ldots, i_r)$ with $1 \le i_1 < \cdots < i_r \le p$ and $J := (j_1, \ldots, j_r)$ with $1 \le j_1 < \cdots < j_r \le q$, set

$$\mathbf{X}_{IJ} := \begin{pmatrix} x_{i_1 j_1} & \ldots & x_{i_1 j_r} \\ \vdots & & \vdots \\ x_{i_r j_1} & \ldots & x_{i_r j_r}\end{pmatrix} \quad \text{and} \quad \mathbf{X}_I := \begin{pmatrix} x_{i_1 1} & \ldots & x_{i_1 n} \\ \vdots & & \vdots \\ x_{i_r 1} & \ldots & x_{i_r n}\end{pmatrix}.$$

For (1), say $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{ij})$. Set $\mathbf{C} := \mathbf{AB}$. Given $I := (i_1, \ldots, i_r)$ with

$1 \le i_1 < \cdots < i_r \le m$ and $K := (k_1, \ldots, k_r)$ with $1 \le k_1 < \cdots < k_r \le p$, note

$$\begin{aligned}\det(\mathbf{C}_{IK}) &= \det\big(C^1_{IK}, \ldots, C^r_{IK}\big)\\ &= \det\Big(\sum_{j_1=1}^{n} \mathbf{A}_I^{j_1} b_{j_1 k_1}, \ldots, \sum_{j_r=1}^{n} \mathbf{A}_I^{j_r} b_{j_r k_r}\Big)\\ &= \sum_{j_1,\ldots,j_r=1}^{n} \det\big(\mathbf{A}_I^{j_1}, \ldots, \mathbf{A}_I^{j_r}\big) \cdot b_{j_1 k_1} \cdots b_{j_r k_r}.\end{aligned}$$

In the last sum, each term corresponds to a sequence $J := (j_1, \ldots, j_r)$ with $1 \le j_i \le n$. If two j_i are equal, then $\det\big(\mathbf{A}_I^{j_1}, \ldots, \mathbf{A}_I^{j_r}\big) = 0$ as two columns are equal. Suppose no two j_i are equal. Then J is a permutation σ of $H := (h_1, \ldots, h_r)$ with $1 \le h_1 < \cdots < h_r \le q$; so $j_i = \sigma(h_i)$. Denote the sign of σ by $(-1)^\sigma$. Then

$$\det\big(\mathbf{A}_I^{j_1}, \ldots, \mathbf{A}_I^{j_r}\big) = (-1)^\sigma \det(\mathbf{A}_{IH}).$$

But $\det(\mathbf{B}_{HK}) = \sum_\sigma (-1)^\sigma b_{\sigma(h_1)k_1} \cdots b_{\sigma(h_r)k_r}$. Hence

$$\det(\mathbf{C}_{IK}) = \textstyle\sum_H \det(\mathbf{A}_{IH}) \det(\mathbf{B}_{HK}).$$

Thus (1) holds.

For (2), note that $I_r(W) = R$ for $W = U, U^{-1}, V, V^{-1}$ by **(5.31)**. So (1) yields

$$I_r(\mathbf{A}) = I_r(\mathbf{U}^{-1}\mathbf{U}\mathbf{A}\mathbf{V}\mathbf{V}^{-1}) \subset I_r(\mathbf{U}\mathbf{A}\mathbf{V}) \subset I_r(\mathbf{A}).$$

Thus (2) holds. □

Lemma **(5.34)** (Fitting). — *Let R be a ring, M a module, r an integer, and*

$$R^n \xrightarrow{\alpha} R^m \xrightarrow{\mu} M \to 0 \quad \textit{and} \quad R^q \xrightarrow{\beta} R^p \xrightarrow{\pi} M \to 0$$

presentations. Represent α, β by matrices $\mathbf{A}$, $\mathbf{B}$. Then $I_{m-r}(\mathbf{A}) = I_{p-r}(\mathbf{B})$.

Proof: First, assume $m = p$ and $\mu = \pi$. Set $K := \mathrm{Ker}(\mu)$. Then $\mathrm{Im}(\alpha) = K$ and $\mathrm{Im}(\beta) = K$ by exactness; so $\mathrm{Im}(\alpha) = \mathrm{Im}(\beta)$. But $\mathrm{Im}(\alpha)$ is generated by the columns of $\mathbf{A}$. Hence each column of $\mathbf{B}$ is a linear combination of the columns of $\mathbf{A}$. So there's a matrix $\mathbf{C}$ such that $\mathbf{AC} = \mathbf{B}$. Set $s := m - r$.

Given k, denote by $\mathbf{I}_k$ the $k \times k$ identity matrix. Denote by $\mathbf{0}_{mq}$ the $m \times q$ zero matrix, and by $(\mathbf{A}|\mathbf{B})$ and $(\mathbf{A}|\mathbf{0}_{mq})$ the juxtapositions of $\mathbf{A}$ with $\mathbf{B}$ and with $\mathbf{0}_{mq}$. Then, therefore, there is a block triangular matrix $\mathbf{V} := \left(\begin{smallmatrix}\mathbf{I}_n & -\mathbf{C}\\ \mathbf{0}_{qn} & \mathbf{I}_q\end{smallmatrix}\right)$ such that $(\mathbf{A}|\mathbf{B})\mathbf{V} = (\mathbf{A}|\mathbf{0}_{mq})$. But $\mathbf{V}$ is invertible. So $I_s(\mathbf{A}|\mathbf{B}) = I_s(\mathbf{A}|\mathbf{0}_{mq})$ by **(5.33)**(2). But $I_s(\mathbf{A}|\mathbf{0}_{mq}) = I_s(\mathbf{A})$. Thus $I_s(\mathbf{A}|\mathbf{B}) = I_s(\mathbf{A})$. Similarly, $I_s(\mathbf{A}|\mathbf{B}) = I_s(\mathbf{B})$. Thus $I_s(\mathbf{A}) = I_s(\mathbf{B})$, as desired.

Second, assume $m = p$ and that there's an isomorphism $\gamma\colon R^m \to R^p$ with $\pi\gamma = \mu$. Represent γ by a matrix $\mathbf{G}$. Then $R^n \xrightarrow{\gamma\alpha} R^p \xrightarrow{\pi} M \to 0$ is a presentation, and $\mathbf{GA}$ represents $\gamma\alpha$. So, by the first paragraph, $I_s(\mathbf{B}) = I_s(\mathbf{GA})$. But $\mathbf{G}$ is invertible. So $I_s(\mathbf{GA}) = I_s(\mathbf{A})$ by **(5.33)**(2). Thus $I_s(\mathbf{A}) = I_s(\mathbf{B})$, as desired.

Third, assume that $q = n + t$ and $p = m + t$ for some $t \ge 1$ and that $\beta = \alpha \oplus 1_{R^t}$ and $\pi = \mu + 0$. Then $\mathbf{B} = \left(\begin{smallmatrix}\mathbf{A} & \mathbf{0}_{mt}\\ \mathbf{0}_{tn} & \mathbf{I}_t\end{smallmatrix}\right)$.

Given an $s \times s$ submatrix $\mathbf{C}$ of $\mathbf{A}$, set $\mathbf{D} := \left(\begin{smallmatrix}\mathbf{C} & \mathbf{0}_{st}\\ \mathbf{0}_{ts} & \mathbf{I}_t\end{smallmatrix}\right)$. Then $\mathbf{D}$ is an $(s+t) \times (s+t)$ submatrix of $\mathbf{B}$, and $\det(\mathbf{D}) = \det(\mathbf{C})$. Thus $I_s(\mathbf{A}) \subset I_{s+t}(\mathbf{B})$.

For the opposite inclusion, given an $(s+t) \times (s+t)$ submatrix $\mathbf{D}$ of $\mathbf{B}$, assume $\det(\mathbf{D}) \ne 0$. If $\mathbf{D}$ includes part of the $(m+i)$th row of $\mathbf{B}$, then $\mathbf{D}$ must also include part of the $(n+i)$th column, or $\mathbf{D}$ would have an all zero row. Similarly, if $\mathbf{D}$ includes part of the $(n+i)$th column, then $\mathbf{D}$ must include part of the $(m+i)$th row. So $\mathbf{D} = \left(\begin{smallmatrix}\mathbf{C} & \mathbf{0}_{hk}\\ \mathbf{0}_{kh} & \mathbf{I}_k\end{smallmatrix}\right)$ where $h := s + t - k$ for some $k \le t$ and for some $h \times h$ submatrix $\mathbf{C}$ of $\mathbf{A}$. But $\det(\mathbf{D}) = \det(\mathbf{C})$. So $\det(\mathbf{D}) \in I_h(\mathbf{A})$. But $I_h(\mathbf{A}) \subset I_s(\mathbf{A})$ by **(5.31.2)**. So $\det(\mathbf{D}) \in I_s(\mathbf{A})$. Thus $I_{s+t}(\mathbf{B}) \subset I_s(\mathbf{A})$. Thus $I_{s+t}(\mathbf{B}) = I_s(\mathbf{A})$, or $I_{m-r}(\mathbf{A}) = I_{p-r}(\mathbf{B})$, as desired.

Finally, in general, Schanuel's Lemma **(5.25)** yields the commutative diagram

$$\begin{tikzcd} R^n \oplus R^p \arrow[r, "\alpha\oplus 1_{R^p}"] & R^m \oplus R^p \arrow[r, "\mu+0"] \arrow[d, "\gamma", "\simeq"'] & M \arrow[r] \arrow[d, "1_M", "="'] & 0\\ R^m \oplus R^q \arrow[r, "1_{R^m}\oplus\beta"] & R^m \oplus R^p \arrow[r, "0+\pi"] & M \arrow[r] & 0 \end{tikzcd}$$

Thus, by the last two paragraphs, $I_{m-r}(\mathbf{A}) = I_{p-r}(\mathbf{B})$, as desired. □

(5.35) (*Fitting Ideals*). — Let R be a ring, M a finitely presented module, r an integer. Take any presentation $R^n \xrightarrow{\alpha} R^m \to M \to 0$, let $\mathbf{A}$ be the matrix of α, and define the rth **Fitting ideal** of M by

$$F_r(M) := I_{m-r}(\mathbf{A}).$$

It is independent of the choice of presentation by **(5.34)**.

By definition, $F_r(M)$ is finitely generated. Moreover, **(5.31.2)** yields

$$\langle 0 \rangle = F_{-1}(M) \subset F_0(M) \subset \cdots \subset F_m(M) = R. \qquad \textbf{(5.35.1)}$$

Exercise **(5.36)**. — Let R be a ring, and $a_1, \ldots, a_m \in R$ with $\langle a_1 \rangle \supset \cdots \supset \langle a_m \rangle$. Set $M := (R/\langle a_1 \rangle) \oplus \cdots \oplus (R/\langle a_m \rangle)$. Show that $F_r(M) = \langle a_1 \cdots a_{m-r} \rangle$.

Exercise **(5.37)**. — In the setup of **(5.36)**, assume a_1 is a nonunit.

(1) Show that m is the smallest integer such that $F_m(M) = R$.

(2) Let n be the largest integer such that $F_n(M) = \langle 0 \rangle$; set $k := m - n$. Assume R is a domain. Show (a) that $a_i \ne 0$ for $i < k$ and $a_i = 0$ for $i \ge k$, and (b) that M determines each a_i up to unit multiple.

Theorem **(5.38)** (Elementary Divisors). — *Let R be a* PID*, M a free module, N a submodule. Assume N is free of rank $n < \infty$. Then there exists a decomposition $M = M' \oplus M''$ and elements $x_1, \ldots, x_n \in M'$ and $a_1, \ldots, a_n \in R$ such that*

$$M' = Rx_1 \oplus \cdots \oplus Rx_n, \quad N = Ra_1x_1 \oplus \cdots \oplus Ra_nx_n, \quad \langle a_1 \rangle \supset \cdots \supset \langle a_n \rangle \ne 0.$$

Moreover, M and N determine M' and each a_i up to unit multiple.

Proof: Let's prove existence by induction on n. For $n = 0$, take $M' := 0$; no a_i or x_i are needed. So $M'' = M$, and the displayed conditions are trivially satisfied.

Let $\{e_\lambda\}$ be a free basis of M, and $\pi_\lambda\colon M \to R$ the λth projection.

Assume $n > 0$. Given any nonzero $z \in N$, write $z = \sum c_\lambda e_\lambda$ for some $c_\lambda \in R$. Then some $c_{\lambda_0} \ne 0$. But $c_{\lambda_0} = \pi_{\lambda_0}(z)$. Thus $\pi_{\lambda_0}(N) \ne 0$.

Consider the set $\mathcal{S}$ of nonzero ideals of the form $\alpha(N)$ where $\alpha\colon M \to R$ is a linear map. Partially order $\mathcal{S}$ by inclusion. Given a totally ordered subset $\{\alpha_\lambda(N)\}$, set $\mathfrak{b} := \bigcup \alpha_\lambda(N)$. Then $\mathfrak{b}$ is an ideal. So $\mathfrak{b} = \langle b \rangle$ for some $b \in R$ as R is a PID. Then $b \in \alpha_\lambda(N)$ for some λ. So $\alpha_\lambda(N) = \mathfrak{b}$. By Zorn's Lemma, $\mathcal{S}$ has a maximal element, say $\alpha_1(N)$. Fix $a_1 \in R$ with $\alpha_1(N) = \langle a_1 \rangle$, and fix $y_1 \in N$ with $\alpha_1(y_1) = a_1$.

Given any linear map $\beta\colon M \to R$, set $b := \beta(y_1)$. Then $\langle a_1 \rangle + \langle b \rangle = \langle c \rangle$ for some $c \in R$, as R is a PID. Write $c = da_1 + eb$ for $d, e \in R$, and set $\gamma := d\alpha_1 + e\beta$. Then $\gamma(N) \supset \langle \gamma(y_1) \rangle$. But $\gamma(y_1) = c$. So $\langle c \rangle \subset \gamma(N)$. But $\langle a_1 \rangle \subset \langle c \rangle$. Hence, by maximality, $\langle a_1\rangle = \gamma(N)$. But $\langle b\rangle \subset \langle c\rangle$. Thus $\beta(y_1) = b \in \langle a_1\rangle$.

Write $y_1 = \sum c_\lambda e_\lambda$ for some $c_\lambda \in R$. Then $\pi_\lambda(y_1) = c_\lambda$. But $c_\lambda = a_1 d_\lambda$ for some $d_\lambda \in R$ by the above paragraph with $\beta := \pi_\lambda$. Set $x_1 := \sum d_\lambda e_\lambda$. Then $y_1 = a_1 x_1$.

So $\alpha_1(y_1) = a_1\alpha_1(x_1)$. But $\alpha_1(y_1) = a_1$. So $a_1\alpha_1(x_1) = a_1$. But R is a domain and $a_1 \neq 0$. Thus $\alpha_1(x_1) = 1$.

Set $M_1 := \mathrm{Ker}(\alpha_1)$. As $\alpha_1(x_1) = 1$, clearly $Rx_1 \cap M_1 = 0$. Also, given $x \in M$, write $x = \alpha_1(x)x_1 + (x - \alpha_1(x)x_1)$; thus $x \in Rx_1 + M_1$. Hence **(4.17)** implies $M = Rx_1 \oplus M_1$. Further, M_1 is free by **(4.14)**. Set $N_1 := M_1 \cap N$.

Recall $a_1x_1 = y_1 \in N$. So $N \supset Ra_1x_1 \oplus N_1$. Conversely, given $y \in N$, write $y = bx_1 + m_1$ with $b \in R$ and $m_1 \in M_1$. Then $\alpha_1(y) = b$, so $b \in \langle a_1\rangle$. Hence $y \in Ra_1x_1 + N_1$. Thus $N = Ra_1x_1 \oplus N_1$.

Define $\varphi\colon R \to Ra_1x_1$ by $\varphi(a) = aa_1x_1$. If $\varphi(a) = 0$, then $aa_1 = 0$ as $\alpha_1(x_1) = 1$, and so $a = 0$ as $a_1 \neq 0$. Thus φ is injective, so a isomorphism.

Note $N_1 \simeq R^m$ with $m \le n$ owing to **(4.14)** with N for E. Hence $N \simeq R^{m+1}$. But $N \simeq R^n$. So **(5.32)**(2) yields $m + 1 = n$.

By induction on n, there exists a decomposition $M_1 = M_1' \oplus M''$ and elements $x_2, \dots, x_n \in M_1'$ and $a_2, \dots, a_n \in R$ such that

$$M_1' = Rx_2 \oplus \cdots \oplus Rx_n,\ \ N_1 = Ra_2x_2 \oplus \cdots \oplus Ra_nx_n,\ \ \langle a_2\rangle \supset \cdots \supset \langle a_n\rangle \neq 0.$$

Then $M = M' \oplus M''$ and $M' = Rx_1 \oplus \cdots \oplus Rx_n$ and $N = Ra_1x_1 \oplus \cdots \oplus Ra_nx_n$. Also $\langle a_1\rangle \supset \cdots \supset \langle a_n\rangle \neq 0$. Thus existence is proved.

Finally, consider the projection $\pi\colon M_1 \to R$ with $\pi(x_j) = \delta_{2j}$ for $j \le 2 \le n$ and $\pi|M'' = 0$. Define $\rho\colon M \to R$ by $\rho(ax_1 + m_1) := a + \pi(m_1)$. Then $\rho(a_1x_1) = a_1$. So $\rho(N) \supset \langle a_1\rangle = \alpha_1(N)$. By maximality, $\rho(N) = \alpha_1(N)$. But $a_2 = \rho(a_2x_2) \in \rho(N)$. Thus $\langle a_2\rangle \subset \langle a_1\rangle$, as desired.

Moreover, $M' = \{m \in M \mid xm \in N \text{ for some } x \in R\}$. Thus M' is determined. Also, by **(5.37)**(2) with M'/N for M, each a_i is determined up to unit multiple. □

Theorem **(5.39)**. — *Let A be a local ring, M a finitely presented module.*

(1) *Then M can be generated by m elements if and only if $F_m(M) = A$.*

(2) *Then M is free of rank m if and only if $F_m(M) = A$ and $F_{m-1}(M) = \langle 0\rangle$.*

Proof: For (1), assume M can be generated by m elements. Then **(4.10)**(1) and **(5.26)** yield a presentation $A^n \xrightarrow{\alpha} A^m \to M \to 0$. So $F_m(M) = A$ by **(5.34)**.

For the converse, assume also M cannot be generated by $m-1$ elements. Suppose $F_k(M) = A$ with $k < m$. Then $F_{m-1}(M) = A$ by **(5.35.1)**. Hence one entry of the matrix (a_{ij}) of α does not belong to the maximal ideal, so is a unit by **(3.6)**. By **(5.33)**(2), we may assume $a_{11} = 1$ and the other entries in the first row and first column of $\mathbf{A}$ are 0. Thus $\mathbf{A} = \left(\begin{smallmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{B}\end{smallmatrix}\right)$ where $\mathbf{B}$ is an $(m-1) \times (s-1)$ matrix. Then $\mathbf{B}$ defines a presentation $A^{s-1} \to A^{m-1} \to M \to 0$. So M can be generated by $m - 1$ elements, a contradiction. Thus $F_k(M) \neq A$ for $k < m$. Thus (1) holds.

In (2), if M is free of rank m, then there's a presentation $0 \to A^m \to M \to 0$; so $F_m(M) = A$ and $F_{m-1}(M) = \langle 0\rangle$ by **(5.35)**. Conversely, if $F_m(M) = A$, then (1) and **(5.26)** and **(4.10)**(1) yield a presentation $A^s \xrightarrow{\alpha} A^m \to M \to 0$. If also $F_{m-1}(M) = \langle 0\rangle$, then $\alpha = 0$ by **(5.35)**. Thus M is free of rank m; so (2) holds. □

Proposition **(5.40)**. — *Let R be a ring, and M a finitely presented module. Say M can be generated by m elements. Set $\mathfrak{a} := \mathrm{Ann}(M)$. Then*

$$(1)\ \ \mathfrak{a}F_r(M) \subset F_{r-1}(M) \textit{ for all } r > 0 \quad \textit{and} \quad (2)\ \ \mathfrak{a}^m \subset F_0(M) \subset \mathfrak{a}.$$

Proof: As M can be generated by m elements, **(4.10)**(1) and **(5.26)** yield a presentation $A^n \xrightarrow{\alpha} A^m \xrightarrow{\mu} M \to 0$. Say α has matrix $\mathbf{A}$.

In (1), if $r > m$, then trivially $\mathfrak{a}F_r(M) \subset F_{r-1}(M)$ owing to **(5.35.1)**. So assume $r \le m$ and set $s := m - r + 1$. Given $x \in \mathfrak{a}$, form the sequence

$$R^{n+m} \xrightarrow{\beta} R^m \xrightarrow{\mu} M \to 0 \text{ with } \beta := \alpha + x1_{R^m}.$$

Note that this sequence is a presentation. Also, the matrix of β is $(\mathbf{A}|x\mathbf{I}_m)$, obtained by juxtaposition, where $\mathbf{I}_m$ is the $m \times m$ identity matrix.

Given an $(s-1) \times (s-1)$ submatrix $\mathbf{B}$ of $\mathbf{A}$, enlarge it to an $s \times s$ submatrix $\mathbf{B}'$ of $(\mathbf{A}|x\mathbf{I}_m)$ as follows: say the ith row of $\mathbf{A}$ is not involved in $\mathbf{B}$; form the $m \times s$ submatrix $\mathbf{B}''$ of $(\mathbf{A}|x\mathbf{I}_m)$ with the same columns as $\mathbf{B}$ plus the ith column of $x\mathbf{I}_m$ at the end; finally, form $\mathbf{B}'$ as the $s \times s$ submatrix of $\mathbf{B}''$ with the same rows as $\mathbf{B}$ plus the ith row in the appropriate position.

Expanding along the last column yields $\det(\mathbf{B}') = \pm x \det(\mathbf{B})$. By constuction, $\det(\mathbf{B}') \in I_s(\mathbf{A}|x\mathbf{I}_m)$. But $I_s(\mathbf{A}|x\mathbf{I}_m) = I_s(\mathbf{A})$ by **(5.34)**. Furthermore, $x \in \mathfrak{a}$ is arbitrary, and $I_m(\mathbf{A})$ is generated by all possible $\det(\mathbf{B})$. Thus (1) holds.

For (2), apply (1) repeatedly to get $\mathfrak{a}^k F_r(M) \subset F_{r-k}(M)$ for all r and k. But $F_m(M) = R$ by **(5.35.1)**. So $\mathfrak{a}^m \subset F_0(M)$.

For the second inclusion, given any $m \times m$ submatrix $\mathbf{B}$ of $\mathbf{A}$, say $\mathbf{B} = (b_{ij})$. Let $\mathbf{e}_i$ be the ith standard basis vector of R^m. Set $m_i := \mu(\mathbf{e}_i)$. Then $\sum b_{ij}m_j = 0$ for all i. Let $\mathbf{C}$ be the matrix of cofactors of $\mathbf{B}$: the (i,j)th entry of $\mathbf{C}$ is $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the jth row and the ith column of $\mathbf{B}$. Then $\mathbf{CB} = \det(\mathbf{B})\mathbf{I}_m$. Hence $\det(\mathbf{B})m_i = 0$ for all i. So $\det(\mathbf{B}) \in \mathfrak{a}$. But $I_m(\mathbf{A})$ is generated by all such $\det(\mathbf{B})$. Thus $F_0(M) \subset \mathfrak{a}$. Thus (2) holds. □

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, 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:

$$\begin{tikzcd} F(A) \arrow[r, "F(\alpha)"] \arrow[d, "\theta(A)"'] & F(B) \arrow[d, "\theta(B)"'] \\ F'(A) \arrow[r, "F'(\alpha)"] & F'(B) \end{tikzcd}$$

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-mod)) to ((R-mod)).

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

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{C}}(B,C) \arrow[r] \arrow[d] & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \arrow[d] \\ \mathrm{Hom}_{\mathcal{C}}(A,C) \arrow[r] & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(C)\big) \end{tikzcd} \tag{6.3.1}$$

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

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{C}}(B,C) \arrow[r] \arrow[d] & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \arrow[d] \\ \mathrm{Hom}_{\mathcal{C}}(A,D) \arrow[r] & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(D)\big) \end{tikzcd}$$

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

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

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

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{C}'}(F(A),\,A') \arrow[r, phantom, "\simeq"] \arrow[d] & \mathrm{Hom}_{\mathcal{C}}(A,\,F'(A')) \arrow[d] \\ \mathrm{Hom}_{\mathcal{C}'}(F(B),\,B') \arrow[r, phantom, "\simeq"] & \mathrm{Hom}_{\mathcal{C}}(B,\,F'(B')) \end{tikzcd}$$

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:

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

Chase after $1_{F(A)}$ and $1_{F(B)}$. Both map to $F(\alpha) \in \operatorname{Hom}_{\mathcal{C}'}(F(A),\,F(B))$. So both map to the same image in $\operatorname{Hom}_{\mathcal{C}'}(G(A),\,F(B))$. 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 $\theta\theta' = 1_F$. But, by naturality, the following diagram is commutative:

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

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 $((\text{Sets}))$, since by **(4.10)**,

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

Similarly, the "polynomial ring" functor is the left adjoint of the forgetful functor from $((R\text{-alg}))$ to $((\text{Sets}))$, since by **(1.3)**,

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

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 $\varphi_{A,A'}\colon \operatorname{Hom}_{\mathcal{C}'}(FA,\,A') \xrightarrow{\sim} \operatorname{Hom}_{\mathcal{C}}(A,\,F'A')$ 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 analogous 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 to be the object of $\mathcal{C}$ universal among objects P equipped with maps $\beta_\mu\colon M_\mu \to P$, called **insertions**, that are compatible with the **transition maps** $\alpha^\kappa_\mu\colon M_\kappa \to M_\mu$, which are the images of the maps of Λ. (Note: given κ and μ, there may be more than one map $\kappa \to \mu$, and so more than one transition map α^κ_μ.) In other words, there is a unique map β such that all of the following diagrams commute:

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

To indicate 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.

Given a functor $F\colon \mathcal{C} \to \mathcal{C}'$, note that a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$ yields a functor $\lambda \mapsto F(M_\lambda)$ from Λ to $\mathcal{C}'$. Furthermore, whenever the corresponding two direct limits exist, the maps $F(\alpha_\mu)\colon F(M_\mu) \to F(\varinjlim M_\lambda)$ induce a canonical map

$$\phi\colon \varinjlim F(M_\lambda) \to F(\varinjlim M_\lambda). \qquad \textbf{(6.6.1)}$$

If ϕ is always an isomorphism, we say F **preserves direct limits**. At times, given $\varinjlim M_\lambda$, we construct $\varinjlim F(M_\lambda)$ by showing $F(\varinjlim M_\lambda)$ 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

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

To put it in another way, form the **functor category** $\mathcal{C}^\Lambda$: its objects are the functors $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$; 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 object of $\mathcal{C}$ universal among objects 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 such a P, there exists a unique map $\beta\colon \coprod M_\lambda \to P$ with $\beta\iota_\mu = \beta_\mu$ for all $\mu \in \Lambda$.

If $\Lambda = \emptyset$, then the coproduct is an object B with a unique map β to every other object P. There are no μ in Λ, so no inclusions $\iota_\mu\colon M_\mu \to B$, so no equations $\beta\iota_\mu = \beta_\mu$ to restrict β. Such a B is called an **initial object**.

For instance, suppose $\mathcal{C} = ((R\text{-mod}))$. Then the zero module is an initial object. For any Λ, the coproduct $\coprod M_\lambda$ is just the direct sum $\bigoplus M_\lambda$ (a convention if $\Lambda = \emptyset$). Next, suppose $\mathcal{C} = ((\text{Sets}))$. Then the empty set is an initial object. For any Λ, the coproduct $\coprod M_\lambda$ is the disjoint union $\bigsqcup M_\lambda$ (a convention if $\Lambda = \emptyset$).

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 $\alpha,\ \alpha'\colon M \rightrightarrows N$ be two maps in a category $\mathcal{C}$. Their **coequalizer** is defined as the object of $\mathcal{C}$ universal among objects 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 $\varphi,\ \varphi'\colon \kappa \rightrightarrows \mu$. 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 in a category $\mathcal{C}$. Their **pushout** is defined as the object of $\mathcal{C}$ universal among objects 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 ((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 all transition maps $\alpha^\lambda_\mu\colon M_\lambda \to M_\mu$. For each $\sigma := \alpha^\lambda_\mu \in \Sigma$, 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 $\iota_\mu\alpha^\lambda_\mu$. 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 $\beta_\mu\alpha^\lambda_\mu = \beta_\lambda$, 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 ((Sets)) have direct limits.*

Proof: The assertion follows from **(6.10)** because $((R\text{-mod}))$ 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

$$\begin{tikzcd}
F(M_\kappa) \arrow[r, "F(\alpha^\kappa_\mu)"] \arrow[d, "\beta'_\kappa"] & F(M_\mu) \arrow[r, "F(\alpha_\mu)"] \arrow[d, "\beta'_\mu"] & F(\varinjlim M_\lambda) \arrow[d, "\beta'"] \\
P' \arrow[r, "1"] & P' \arrow[r, "1"] & P'
\end{tikzcd} \tag{6.12.1}$$

where α^κ_μ 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:

$$\begin{tikzcd}
M_\kappa \arrow[r, "\alpha^\kappa_\mu"] \arrow[d, "\beta_\kappa"] & M_\mu \arrow[r, "\alpha_\mu"] \arrow[d, "\beta_\mu"] & \varinjlim M_\lambda \arrow[d, "\beta"] \\
F'(P') \arrow[r, "1"] & F'(P') \arrow[r, "1"] & F'(P')
\end{tikzcd}$$

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 $\lambda \mapsto M_{\sigma\lambda}$ to $\lambda \mapsto M_{\tau\lambda}$. So a map $\lambda \to \mu$ in Λ yields a commutative square

$$\begin{tikzcd}
M_{\sigma\lambda} \arrow[r] \arrow[d] & M_{\sigma\mu} \arrow[d] \\
M_{\tau\lambda} \arrow[r] & M_{\tau\mu}
\end{tikzcd} \tag{6.13.1}$$

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. After making the definitions, we study an instructive example where the limit is $\mathbb{Q}$. Then we develop an alternative construction of filtered direct 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.

(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 $\kappa \le \mu$ and $\lambda \le \mu$. Regard Λ as a category whose objects are its elements and whose sets $\operatorname{Hom}(\kappa,\lambda)$ consist of a single element if $\kappa \le \lambda$, and are empty if not; morphisms can be composed, because 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 $\lambda, \mu \in \Lambda$, 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 $M = \varinjlim M_\lambda$.

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:

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

where μ_s is the map of multiplication by s and ι_n^m is the inclusion. Thus $\mathbb{Q} = \varinjlim R_n$ where the transition maps are the 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 $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$.

Theorem **(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 set-theoretic disjoint union $\bigsqcup M_\lambda$ as follows: $m_1 \sim m_2$ for $m_i \in M_{\lambda_i}$ if there are transition maps $\alpha^{\lambda_i}_\mu \colon M_{\lambda_i} \to M_\mu$ such that $\alpha^{\lambda_1}_\mu m_1 = \alpha^{\lambda_2}_\mu m_2$. Then $\sim$ is an equivalence relation. Set $M := (\bigsqcup M_\lambda)/\!\sim$. 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 $\alpha^{\lambda_i}_\mu$ for $i = 1, 2$ and $\alpha^{\lambda_i}_\nu$ for $i = 2, 3$ with $\alpha^{\lambda_1}_\mu m_1 = \alpha^{\lambda_2}_\mu m_2$ and $\alpha^{\lambda_2}_\nu m_2 = \alpha^{\lambda_3}_\nu m_3$. Then **(7.1)**(1) yields α^μ_ρ and α^ν_ρ. Possibly, $\alpha^\mu_\rho\alpha^{\lambda_2}_\mu \neq \alpha^\nu_\rho\alpha^{\lambda_2}_\nu$, but in any case, **(7.1)**(2) yields α^ρ_σ with $\alpha^\rho_\sigma(\alpha^\mu_\rho\alpha^{\lambda_2}_\mu) = \alpha^\rho_\sigma(\alpha^\nu_\rho\alpha^{\lambda_2}_\nu)$. In sum, we have this diagram of indices:

$$\begin{tikzcd}[row sep=small]
\lambda_1 \arrow[dr] & & & \\
 & \mu \arrow[dr] & & \\
\lambda_2 \arrow[ur] \arrow[dr] & & \rho \arrow[r] & \sigma \\
 & \nu \arrow[ur] & & \\
\lambda_3 \arrow[ur] & & &
\end{tikzcd}$$

Hence, $(\alpha^\rho_\sigma\alpha^\mu_\rho)\alpha^{\lambda_1}_\mu m_1 = (\alpha^\rho_\sigma\alpha^\nu_\rho)\alpha^{\lambda_3}_\nu m_3$. Thus $m_1 \sim m_3$.

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

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

We must check that this addition is well defined.

First, consider μ. Suppose there are $\alpha^{\lambda_i}_\nu$ too. Then **(7.1)**(1) yields α^μ_ρ and α^ν_ρ. Possibly, $\alpha^\mu_\rho\alpha^{\lambda_i}_\mu \neq \alpha^\nu_\rho\alpha^{\lambda_i}_\nu$, but **(7.1)**(2) yields α^ρ_σ with $\alpha^\rho_\sigma(\alpha^\mu_\rho\alpha^{\lambda_1}_\mu)\alpha^\rho_\sigma(\alpha^\nu_\rho\alpha^{\lambda_1}_\nu)$ and then α^σ_τ with $\alpha^\sigma_\tau(\alpha^\rho_\sigma\alpha^\mu_\rho\alpha^{\lambda_2}_\mu) = \alpha^\sigma_\tau(\alpha^\rho_\sigma\alpha^\nu_\rho\alpha^{\lambda_2}_\nu)$. In sum, we have this diagram:

$$\begin{tikzcd}[row sep=small]
\lambda_1 \arrow[r, shift left] \arrow[dr] & \mu \arrow[dr] & & & \\
 & & \rho \arrow[r, shift left] \arrow[r, shift right] & \sigma \arrow[r] & \tau \\
\lambda_2 \arrow[r] \arrow[ur] & \nu \arrow[ur] & & &
\end{tikzcd}$$

Therefore, $(\alpha^\sigma_\tau\alpha^\rho_\sigma\alpha^\mu_\rho)(\alpha^{\lambda_1}_\mu m_1 + \alpha^{\lambda_2}_\mu m_2) = (\alpha^\sigma_\tau\alpha^\rho_\sigma\alpha^\nu_\rho)(\alpha^{\lambda_1}_\nu m_1 + \alpha^{\lambda_2}_\nu m_2)$. 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 $\mathcal{C} = ((R\text{-alg}))$, then we can see similarly that M is canonically an R-algebra.

Finally, let $\beta_\lambda \colon M_\lambda \to N$ be maps with $\beta_\lambda\alpha^\kappa_\lambda = \beta_\kappa$ for all α^κ_λ. 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, $\alpha^{\lambda_1}_\mu m_1 = \alpha^{\lambda_2}_\mu m_2$ for some $\alpha^{\lambda_i}_\mu$. Then $\beta_{\lambda_1}m_1 = \beta_{\lambda_2}m_2$ as $\beta_\mu\alpha^{\lambda_i}_\mu = \beta_{\lambda_i}$. So there is a unique map $\beta \colon M \to N$ with $\beta\alpha_\lambda = \beta_\lambda$ for all λ. Further, if $\mathcal{C} = ((R\text{-mod}))$ or $\mathcal{C} = ((R\text{-alg}))$, then clearly β is a homomorphism. The proof is now complete. □

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

(1) *Given $m \in \varinjlim M_\lambda$, there are λ and $m_\lambda \in M_\lambda$ 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 $\alpha^{\lambda_i}_\mu$ such that $\alpha^{\lambda_1}_\mu m_1 = \alpha^{\lambda_2}_\mu m_2$.*

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

Proof: The assertions follow directly from **(7.7)**. Specifically, (1) holds, since $\varinjlim M_\lambda$ is a quotient of the disjoint union $\bigsqcup M_\lambda$. Further, (2) holds owing to the definition of the equivalence relation involved. Finally, (3) is the special case of (2) where $m_1 := m_\lambda$ and $m_2 = 0$. □

Exercise **(7.9)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings.

(1) Prove that $R = 0$ if and only if $R_\lambda = 0$ for some λ.

(2) Assune that each R_λ is a domain. Prove that R is a domain.

(3) Assume that each R_λ is a field. Prove that R is a field.

Exercise **(7.10)**. — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha^\lambda_\mu \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$. For each λ, let $N_\lambda \subset M_\lambda$ be a submodule, and let $N \subset M$ be a submodule. Prove that $N_\lambda = \alpha_\lambda^{-1}N$ for all λ if and only if (a) $N_\lambda = (\alpha^\lambda_\mu)^{-1}N_\mu$ for all α^λ_μ and (b) $\bigcup \alpha_\lambda N_\lambda = N$.

Definition **(7.11)**. — Let R be a ring. We say an algebra R' is *finitely presented* if $R' \simeq R[X_1, \ldots, X_r]/\mathfrak{a}$ for some variables X_i and finitely generated ideal $\mathfrak{a}$.

Proposition **(7.12)**. — *Let Λ be a filtered category, R a ring, $\mathcal{C}$ either ((R-mod)) or ((R-alg)), $\lambda \mapsto M_\lambda$ a functor from Λ to $\mathcal{C}$. Given $N \in \mathcal{C}$, form the map* **(6.6.1)**,

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

(1) *If N is finitely generated, then θ is injective.*

(2) *The following conditions are equivalent:*

(a) *N is finitely presented;*

(b) *θ is bijective for all filtered categories Λ and all functors $\lambda \mapsto M_\lambda$;*

(c) *θ is surjective for all directed sets Λ and all $\lambda \mapsto M_\lambda$.*

Proof: Given a transition map $\alpha^\lambda_\mu \colon M_\lambda \to M_\mu$, set $\beta^\lambda_\mu := \operatorname{Hom}(N, \alpha^\lambda_\mu)$. Then the β^λ_μ are the transition maps of $\varinjlim \operatorname{Hom}(N, M_\lambda)$. Denote by α_λ and β_λ the insertions of $\varinjlim M_\lambda$ and $\varinjlim \operatorname{Hom}(N, M_\lambda)$.

For (1), let $n_1, \ldots, n_r$ generate N. Given φ and φ' in $\varinjlim \operatorname{Hom}(N, M_\lambda)$ with $\theta(\varphi) = \theta(\varphi')$, note that **(7.8)**(1) yields λ and $\varphi_\lambda \colon N \to M_\lambda$ and μ and $\varphi'_\mu \colon N \to M_\mu$ with $\beta_\lambda(\varphi_\lambda) = \varphi$ and $\beta_\mu(\varphi'_\mu) = \varphi'$. Then $\theta(\varphi) = \alpha_\lambda\varphi_\lambda$ and $\theta(\varphi') = \alpha_\mu\varphi'_\mu$ by construction of θ. Hence $\alpha_\lambda\varphi_\lambda = \alpha_\mu\varphi'_\mu$. So $\alpha_\lambda\varphi_\lambda(n_i) = \alpha_\mu\varphi'_\mu(n_i)$ for all i. So **(7.8)**(2) yields λ_i and $\alpha^\lambda_{\lambda_i}$ and $\alpha^\mu_{\lambda_i}$ such that $\alpha^\lambda_{\lambda_i}\varphi_\lambda(n_i) = \alpha^\mu_{\lambda_i}\varphi'_\mu(n_i)$ for all i.

Let's prove, by induction on i, that there are ν_i and $\alpha^\mu_{\nu_i}$ and $\alpha^\mu_{\nu_i}$ such that $\alpha^\lambda_{\nu_i}\varphi_\lambda(n_j) = \alpha^\mu_{\nu_i}(n_j)$ for $1 \le j \le i$. Indeed, given ν_{i-1} and $\alpha^\lambda_{\nu_{i-1}}$ and $\alpha^\mu_{\nu_{i-1}}$, by **(7.1)**(1), there are ρ_i and $\alpha^{\nu_{i-1}}_{\rho_i}$ and $\alpha^{\lambda_i}_{\rho_i}$. By **(7.1)**(2), there are ν_i and $\alpha^{\rho_i}_{\nu_i}$ such that $\alpha^{\rho_i}_{\nu_i}\alpha^{\nu_{i-1}}_{\rho_i}\alpha^\lambda_{\nu_{i-1}} = \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\lambda_{\lambda_i}$ and $\alpha^{\rho_i}_{\nu_i}\alpha^{\nu_{i-1}}_{\rho_i}\alpha^\mu_{\nu_{i-1}} = \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\mu_{\lambda_i}$. Set $\alpha^\lambda_{\nu_i} := \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\lambda_{\lambda_i}$ and $\alpha^\mu_{\nu_i} := \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\mu_{\lambda_i}$. Then $\alpha^\lambda_{\nu_i}\varphi_\lambda(n_j) = \alpha^\mu_{\nu_i}(n_j)$ for $1 \le j \le i$, as desired.

Set $\nu := \nu_r$. Then $\alpha^\lambda_\nu\varphi_\lambda(n_i) = \alpha^\mu_\nu\varphi'_\mu(n_i)$ for all i. Hence $\alpha^\lambda_\nu\varphi_\lambda = \alpha^\mu_\nu\varphi'_\mu$. But

$$\varphi = \beta_\lambda(\varphi_\lambda) = \beta_\nu\beta^\lambda_\nu(\varphi_\lambda) = \beta_\nu(\alpha^\lambda_\nu\varphi_\lambda).$$

Similarly, $\varphi' = \beta_\nu(\alpha^\mu_\nu\varphi'_\mu)$. Hence $\varphi = \varphi'$. Thus θ is injective. Notice that this proof works equally well for ((R-mod)) and ((R-alg)). Thus (1) holds.

For (2), let's treat the case $\mathcal{C} = ((R\text{-mod}))$ first. Assume (a). Say $N \simeq F/N'$ where $F := R^r$ and N' is finitely generated, say by $n_1', \ldots, n_s'$. Let n_i be the image in N of the ith standard basis vector e_i of F. Then there are homogeneous linear polynomials f_j with $f_j(e_1, \ldots, e_r) = n_j'$ for all j. So $f_j(n_1, \ldots, n_r) = 0$.

Given $\varphi\colon N \to \varinjlim M_\lambda$, set $m_i := \varphi(n_i)$ for $1 \le i \le r$. Repeated use of **(7.8)**(1) and **(7.1)**(1) yields λ and $m_{\lambda i} \in M_\lambda$ with $\alpha_\lambda m_{\lambda i} = m_i$ for all i. So for all j,

$$\alpha_\lambda(f_j(m_{\lambda 1}, \ldots, m_{\lambda r})) = f_j(m_1, \ldots, m_r) = \varphi(f_j(n_1, \ldots, n_r)) = 0.$$

Hence repeated use of **(7.8)**(2) and **(7.1)**(1), (2) yields μ and α^λ_μ with, for all j,

$$\alpha^\lambda_\mu(f_j(m_{\lambda 1}, \ldots, m_{\lambda r})) = 0.$$

Therefore, there is $\varphi_\mu\colon N \to M_\mu$ with $\varphi_\mu(n_i) := \alpha^\lambda_\mu(m_{\lambda i})$ by **(4.10)** and **(4.6)**. Set $\psi := \beta_\mu(\varphi_\mu)$. Then $\theta(\psi) = \alpha_\mu\varphi_\mu$. Hence $\theta(\psi)(n_i) = m_i := \varphi(n_i)$ for all i. So $\theta(\psi) = \varphi$. Thus θ is surjective. So (1) implies θ is bijective. Thus (b) holds.

Trivially (b) implies (c).

Finally, assume (c). Take Λ to be the directed set of finitely generated submodules N_λ of N. Then $N = \varinjlim N_\lambda$ by **(7.2)**. However, θ is surjective. So there is $\psi \in \varinjlim \operatorname{Hom}(N, N_\lambda)$ with $\theta(\psi) = 1_N$. So **(7.8)**(1) yields λ and $\psi_\lambda \in \operatorname{Hom}(N, N_\lambda)$ with $\beta_\lambda(\psi_\lambda) = \psi$. Hence $\alpha_\lambda\psi_\lambda = \theta(\psi)$. So $\alpha_\lambda\psi_\lambda = 1_N$. So α_λ is surjective. But $\alpha_\lambda\colon N_\lambda \to N$ is the inclusion. So $N_\lambda = N$. Thus N is finitely generated. Say $n_1, \ldots, n_r$ generate N. Set $F := R^r$ and let e_i be the ith standard basis vector.

Define $\kappa\colon F \to N$ by $\kappa(e_i) := n_i$ for all i. Set $N' := \operatorname{Ker}(\kappa)$. Then $F/N' \xrightarrow{\sim} N$. Let's show N' is finitely generated.

Take Λ to be the directed set of finitely generated submodules N'_λ of N'. Then $N' = \varinjlim N'_\lambda$ by **(7.2)**. Set $N_\lambda := F/N'_\lambda$. Then $N = \varinjlim N_\lambda$ by **(6.17)**. Here the α^λ_μ and the α_λ are the quotient maps. Since θ is surjective, there is $\psi \in \operatorname{Hom}(N, N_\lambda)$ with $\theta(\psi) = 1_N$. So **(7.8)**(1) yields λ and $\psi_\lambda \in \operatorname{Hom}(N, N_\lambda)$ with $\beta_\lambda(\psi_\lambda) = \psi$. Hence $\alpha_\lambda\psi_\lambda = \theta(\psi)$. So $\alpha_\lambda\psi_\lambda = 1_N$. Set $\psi_\mu := \alpha^\lambda_\mu\psi_\lambda$ for all μ; note ψ_μ is well defined as Λ is directed. Then $\alpha_\mu\psi_\mu = \alpha_\lambda\psi_\lambda = 1_N$ for all μ. Let's show there is μ with $\psi_\mu\alpha_\mu = 1_{N_\mu}$.

For all μ and i, let $n_{\mu i}$ be the image in N_μ of e_i. Then $\alpha_\lambda n_{\lambda i} = \alpha_\lambda(\psi_\lambda\alpha_\lambda n_{\lambda i})$ as $\alpha_\lambda\psi_\lambda = 1_N$. Hence repeated use of **(7.8)**(2) and **(7.1)**(1) yields μ such that $\alpha^\lambda_\mu n_{\lambda i} = \alpha^\lambda_\mu(\psi_\lambda\alpha_\lambda n_{\lambda i})$ for all i. Hence $n_{\mu i} = (\psi_\mu\alpha_\mu)n_{\mu i}$. But the $n_{\mu i}$ generate N_μ for all i. So $1_{N_\mu} = \psi_\mu\alpha_\mu$, as desired.

So $\alpha_\mu\colon N_\mu \to N$ is an isomorphism. So $N'_\mu = N'$. Thus N' is finitely generated. Thus (a) holds for $((R\text{-mod}))$.

In the case $\mathcal{C} = ((R\text{-alg}))$, replace F by a polynomial ring $R[X_1, \ldots, X_r]$, the submodule N' by the appropriate ideal $\mathfrak{a}$, and the f_j by polynomials that generate $\mathfrak{a}$. With these replacements, the above proof shows (a) implies (b). As to (c) implies (a), first take the N_λ to be the finitely generated subalgebras; then the above proof of finite generation works equally well as is. The rest of the proof works after we replace F by a polynomial ring, the e_i by the variables, N' by the appropriate ideal, and the N'_λ by the finitely generated subideals. □

(7.13) (*Finite presentations*). — Let R be a ring, R' a finitely presented algebra. The proof of **(7.12)**(2) shows that, for any presentation $R[X_1, \ldots, X_r]/\mathfrak{a}$ of R', where $R[X_1, \ldots, X_r]$ is a polynomial ring and $\mathfrak{a}$ is an ideal, necessarily $\mathfrak{a}$ is finitely generated. Similarly, for a finitely presented module M, that proof gives another solution to **(5.26)**, one not requiring Schanuel's Lemma.

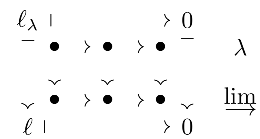
Theorem **(7.14)** (Exactness of Filtered Direct Limits). — *Let R be a ring, Λ a filtered category. Let $\mathcal{C}$ be the category of 3-term exact sequences of R-modules: its*

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

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

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^κ_λ 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 $\gamma\beta\ell = 0$. In sum, we have this figure:

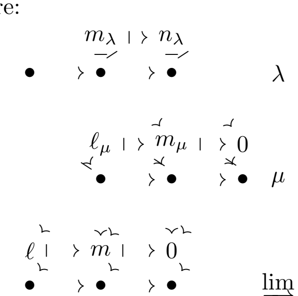


Thus $\operatorname{Im}(\beta) \subset \operatorname{Ker}(\gamma)$.

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^λ_μ with $\alpha^\lambda_\mu\gamma_\lambda m_\lambda = 0$. So $\gamma_\mu\alpha^\lambda_\mu m_\lambda = 0$ by commutativity. Hence there is $\ell_\mu \in L_\mu$ with $\beta_\mu\ell_\mu = \alpha^\lambda_\mu m_\lambda$ by exactness. Apply α_μ to get

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

In sum, we have this figure:



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

Exercise **(7.15)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings, $\mathfrak{a}_\lambda \subset R_\lambda$ an ideal for each λ. Assume $\alpha^\lambda_\mu\mathfrak{a}_\lambda \subset \mathfrak{a}_\mu$ for each transition map α^λ_μ. Set $\mathfrak{a} := \varinjlim \mathfrak{a}_\lambda$. If each $\mathfrak{a}_\lambda$ is prime, show $\mathfrak{a}$ is prime. If each $\mathfrak{a}_\lambda$ is maximal, show $\mathfrak{a}$ is maximal.

Exercise **(7.16)**. — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha^\lambda_\mu\colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda\colon M_\lambda \to M$. Let $N_\lambda \subset M_\lambda$ be a be a submodule for all λ. Assume $\alpha^\lambda_\mu N_\lambda \subset N_\mu$ for all α^λ_μ. Prove $\varinjlim N_\lambda = \bigcup \alpha_\lambda N_\lambda$.

Exercise **(7.17)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Prove that

$$\varinjlim \operatorname{nil}(R_\lambda) = \operatorname{nil}(R).$$

Exercise **(7.18)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Assume each ring R_λ is local, say with maximal ideal $\mathfrak{m}_\lambda$, and assume each transition map $\alpha^\lambda_\mu\colon R_\lambda \to R_\mu$ is local. Set $\mathfrak{m} := \varinjlim \mathfrak{m}_\lambda$. Prove that R is local with maximal ideal $\mathfrak{m}$ and that each insertion $\alpha_\lambda\colon R_\lambda \to R$ is local.

(7.19) (*Hom and direct limits again*). — Let Λ a filtered category, R a ring, N a module, and $\lambda \mapsto M_\lambda$ a functor from Λ to ((R-mod)). Here is an alternative proof that the map $\theta(N)$ of **(6.6.1)** is injective if N is finitely generated and bijective if N is finitely presented.

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:

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

The rows are exact owing to **(5.18)**, the left exactness of Hom, and to **(7.14)**, the exactness of filtered direct limits. Now, Hom preserves finite direct sums by **(4.15)**, 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 **(7.20)**. — 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 **(7.21)**. — 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 $\operatorname{Bil}_R(M, N; P)$. 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 $e_{(m,n)}$:

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

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

The above construction yields a canonical bilinear map

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

Set $m \otimes n := \beta(m,n)$.

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 bilinear map with source $M \times N$; in fact, β induces, not simply a bijection, but a module isomorphism,*

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

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. □

Exercise **(8.4)**. — Let R be a ring, R' an R- algebra, and M an R'-module. Set $M' := R' \otimes_R M$. Define $\alpha\colon M \to M'$ by $\alpha m := 1 \otimes m$, and $\rho\colon M' \to M$ by $\rho(x \otimes m) := xm$. Prove M is a direct summand of M' with $\alpha = \iota_M$ and $\rho = \pi_M$.

(8.5) (*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, compare **(9.2)**.

Proposition **(8.6)**. — *Let R be a ring, M and N modules.*

(1) *Then the switch map $(m,n) \mapsto (n,m)$ 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 b has the UMP, so (2) holds. □

Exercise **(8.7)**. — Let R be a domain, $\mathfrak{a}$ a nonzero ideal. Set $K := \operatorname{Frac}(R)$. Show that $\mathfrak{a} \otimes_R K = K$.

(8.8) (*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 **(8.5)** 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**.

In full generality, it is easy to check that $\operatorname{Hom}_R(M, N)$ is an (R, R')-bimodule under valuewise multiplication by elements of R'. Further, given an R'-module P, it is easy to check that $\operatorname{Hom}_{R'}(N, P)$ is an (R, R')-bimodule under sourcewise multiplication by elements of R.

Exercise **(8.9)**. — 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 is equal to $\operatorname{Ker}(\tau)$, and τ is surjective. Show τ is an isomorphism if R' is a quotient of R.

Theorem **(8.10)**. — *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:*

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

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

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 $\operatorname{Tril}(M, N, P;\ Q)$. 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

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

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

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

Hence each of $M \otimes_R (N \otimes_{R'} P)$ and $(M \otimes_R N) \otimes_{R'} P$ is the universal 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

$$\alpha\colon \operatorname{Hom}_{R'}(M \otimes_R N, P) \to \operatorname{Hom}_R\big(M,\ \operatorname{Hom}_{R'}(N, P)\big) \quad \text{by}$$

$$\big(\alpha(\gamma)(m)\big)(n) := \gamma(m \otimes n).$$

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

To obtain an inverse to α, given $\eta \in \operatorname{Hom}_R\big(M,\ \operatorname{Hom}_{R'}(N, P)\big)$, 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 **(8.9)** 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 **(8.11)**. — *Let R be a ring, and R' an algebra. First, let M be an R-module, and P an R'-module. Then there are two canonical R'-isomorphisms:*

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

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

Instead, let M be an R'-module, and P an R-module. Then there is a canonical R'-isomorphism:

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

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

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

Exercise **(8.12)**. — In the setup of **(8.11)**, find the unit η_M of each adjunction.

Corollary **(8.13)**. — *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 **(6.10)**. □

Example **(8.14)**. — 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 **(8.15)**. — Let M and N be nonzero k-vector spaces. Prove $M\otimes N\neq 0$.

Exercise **(8.16)**. — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module.
(1) Use **(8.13)** 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 **(8.17)**. — Show $\mathbb{Z}/\langle m\rangle\otimes_{\mathbb{Z}}\mathbb{Z}/\langle n\rangle = 0$ if m and n are relatively prime.

Theorem **(8.18)** (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's not hard to see $\theta(M)$ is natural in M and $\theta(R)=1$.

If $\theta(\bullet)$ is an isomorphism, then F preserves direct sums and cokernels by **(8.13)**.

To prove the converse, take a presentation $R^{\oplus\Sigma}\xrightarrow{\beta}R^{\oplus\Lambda}\xrightarrow{\alpha}M\to 0$; one exists by **(5.20)**. Applying θ, we get this commutative diagram:

$$\begin{tikzcd}
R^{\oplus\Sigma}\otimes N \arrow[r] \arrow[d, "\theta(R^{\oplus\Sigma})"] & R^{\oplus\Lambda}\otimes N \arrow[r] \arrow[d, "\theta(R^{\oplus\Lambda})"] & M\otimes N \arrow[r] \arrow[d, "\theta(M)"] & 0 \\
F(R^{\oplus\Sigma}) \arrow[r] & F(R^{\oplus\Lambda}) \arrow[r] & F(M) \arrow[r] & 0
\end{tikzcd} \qquad \textbf{(8.18.1)}$$

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 $\theta\colon T\to U$, 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:

$$\begin{tikzcd}
T(M_\lambda) \arrow[r, "T(\iota_\lambda)"] \arrow[d, "\theta(M_\lambda)"] & \bigoplus T(M_\lambda) \arrow[d, "\theta(\bigoplus M_\lambda)"] \\
U(M_\lambda) \arrow[r, "U(\iota_\lambda)"] & \bigoplus U(M_\lambda)
\end{tikzcd}$$

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 **(8.18.1)** are exact by **(5.2)**. Therefore, $\theta(M)$ is an isomorphism. □

Exercise **(8.19)**. — 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.

(8.20) (*Additive functors*). — Let R be a ring, M a module, and form the diagram

$$M\xrightarrow{\delta_M}M\oplus M\xrightarrow{\sigma_M}M$$

where $\delta_M:=(1_M,1_M)$ and $\sigma_M:=1_M+1_M$.

Let $\alpha,\beta\colon M\to N$ be two maps of modules. Then

$$\sigma_N(\alpha\oplus\beta)\delta_M=\alpha+\beta, \qquad \textbf{(8.20.1)}$$

because, for any $m\in M$, we have

$$(\sigma_N(\alpha\oplus\beta)\delta_M)(m)=\sigma_N(\alpha\oplus\beta)(m,m)=\sigma_N(\alpha(m),\,\beta(m))=\alpha(m)+\beta(m).$$

Let $F\colon((R\text{-mod}))\to((R\text{-mod}))$ be a functor that preserves finite direct sums. Then $F(\alpha\oplus\beta)=F(\alpha)\oplus F(\beta)$. Also, $F(\delta_M)=\delta_{F(M)}$ and $F(\sigma_M)=\sigma_{F(M)}$ as $F(1_M)=1_{F(M)}$. Hence $F(\alpha+\beta)=F(\alpha)+F(\beta)$ by **(8.20.1)**. Thus F is **additive**, that is, $\mathbb{Z}$-linear.

Conversely, every additive functor preserves finite direct sums owing to **(8.19)**.

However, not every additive functor is R-linear. For example, take $R:=\mathbb{C}$. Define $F(M)$ to be M, but with the scalar product of $x\in\mathbb{C}$ and $m\in M$ to be $\overline{x}m$ where $\overline{x}$ is the conjugate. Define $F(\alpha)$ to be α. Then F is additive, but not linear.

Lemma **(8.21)** (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 $t\in M\otimes N$ can be written as a finite sum $t=\sum m_\lambda\otimes n_\lambda$ with $m_\lambda\in M$. Further, $t=0$ 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 $m\otimes n=\sum(x_\lambda m)\otimes n_\lambda$. It follows that t can be written as a finite sum $t=\sum m_\lambda\otimes n_\lambda$ with $m_\lambda\in M$.

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 **(5.20)**, 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 **(8.13)** 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. □

(8.22) (*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 $((R\text{-alg}))$:

$$\begin{tikzcd}
 & S \arrow[dr, "\iota_S"] \arrow[drr, bend left, "\theta"] & & \\
R \arrow[ur, "\sigma"] \arrow[dr, "\tau"'] & & S \otimes_R T \arrow[r, dashed, "\psi"] & V \\
 & T \arrow[ur, "\iota_T"'] \arrow[urr, bend right, "\zeta"'] & &
\end{tikzcd}$$

Example **(8.23)**. — 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 **(1.3)**. So by **(8.22)**, 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 **(8.24)**. — Let R be a ring, M a module, X a variable. Let $M[X]$ be the set of polynomials in X with coefficients in M, that is, expressions of the form $\sum_{i=0}^{n} m_i X^i$ with $m_i \in M$. Prove $M \otimes_R R[X] = M[X]$ as $R[X]$-modules.

Exercise **(8.25)**. — Let R be a ring, $(R'_\sigma)_{\sigma\in\Sigma}$ a family of algebras. For each finite subset J of Σ, let R'_J be the tensor product of the R'_σ for $\sigma \in J$. Prove that the assignment $J \mapsto R'_J$ extends to a filtered direct system and that $\varinjlim R'_J$ exists and is the coproduct of the family $(R'_\sigma)_{\sigma\in\Sigma}$.

Exercise **(8.26)**. — 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 commutative diagram with two short exact sequences involving N'*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] & M \arrow[rr, "\alpha"] \arrow[dr, "\alpha'"'] & & N \arrow[r] & N'' \arrow[r] & 0 \\
 & & 0 \arrow[r] & N' \arrow[ur, "\alpha''"'] \arrow[r] & 0 & &
\end{tikzcd} \tag{9.1.1}$$

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

Proof: If the equations hold, then the second short sequence is exact owing to the definitions, and the first is exact since $\operatorname{Coim}(\alpha) \xrightarrow{\sim} \operatorname{Im}(\alpha)$ by **(4.9)**.

Conversely, given the commutative diagram with two short exact sequences, α'' is injective. So $\operatorname{Ker}(\alpha) = \operatorname{Ker}(\alpha')$. So $M' = \operatorname{Ker}(\alpha)$. So $N' = \operatorname{Coim}(\alpha)$ as α' is surjective. So $N' = \operatorname{Im}(\alpha)$. Hence $N'' = \operatorname{Coker}(\alpha)$. 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

$$\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{R'}(FM, FN) \tag{9.2.1}$$

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 $FM = 0$.

Call F **faithful** if **(9.2.1)** is injective, or equivalently, if $F\alpha = 0$ implies $\alpha = 0$.

Call F **exact** if it preserves exact sequences. For example, $\operatorname{Hom}(P, \bullet)$ is exact if and only if P is projective by **(5.23)**.

Call F **left exact** if it preserves kernels. When F is contravariant, 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.

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 from $((R\text{-mod}))$ to $((R'\text{-mod}))$. 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 **(5.2)**, 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, $\operatorname{Ker}(\beta) = \operatorname{Im}(\alpha)$. Now, (5) yields $\operatorname{Ker}(F(\beta)) = F(\operatorname{Ker}(\beta))$ and $\operatorname{Im}(F(\alpha)) = F(\operatorname{Im}(\alpha))$. Therefore, $\operatorname{Ker}(F(\beta)) = \operatorname{Im}(F(\alpha))$. Thus (1) holds. □

Exercise **(9.4)**. — Let R be a ring, R' an algebra, F an R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Assume F is exact. Prove the following equivalent:

(1) F is faithful.
(2) An R-module M vanishes if FM does.
(3) $F(R/\mathfrak{m}) \neq 0$ for every maximal ideal $\mathfrak{m}$ of R.
(4) A sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ is exact if $FM' \xrightarrow{F\alpha} FM \xrightarrow{F\beta} FM''$ is.

(9.5) (*Flatness*). — We say an R-module M is **flat** over R or R-**flat** if the functor $M \otimes_R \bullet$ is exact. It is equivalent by **(9.3)** that $M \otimes_R \bullet$ preserve injections since it preserves cokernels by **(8.13)**.

We say M is **faithfully flat** if $M \otimes_R \bullet$ is exact and faithful.

We say an R-algebra is **flat** or **faithfully flat** if it is so as an R-module.

Lemma **(9.6)**. — *A direct sum $M := \bigoplus M_\lambda$ is flat if and only if every M_λ is flat. Further, M is faithfully flat if every M_λ is flat and at least one is faithfully flat.*

Proof: Let $\beta\colon N' \to N$ be an injective map. Then **(8.13)** yields

$$\left(\bigoplus M_\lambda\right) \otimes \beta = \bigoplus (M_\lambda \otimes \beta);$$

see the end of the proof of **(8.18)**, taking $T(M) := M \otimes N'$ and $U(M) := M \otimes N$. But the map $\bigoplus (M_\lambda \otimes \beta)$ is injective if and only if each summand $M_\lambda \otimes \beta$ is injective by **(5.4)**. The first assertion follows.

Further, $M \otimes N = \bigoplus (M_\lambda \otimes N)$ by **(8.13)**. So if $M \otimes N = 0$, then $M_\lambda \otimes N = 0$ for all λ. If also at least one M_λ is faithfully flat, then $N = 0$, as desired. □

Proposition **(9.7)**. — *A nonzero free module is faithfully flat. Every projective module is flat.*

Proof: It's easy to extend the unitary law to maps; in other words, $R \otimes \bullet = 1$. So R is faithfully flat over R. Thus a nonzero free module is faithfully flat by **(9.6)**.

Every projective module is a direct summand of a free module by **(5.23)**, and so is flat by **(9.6)**. □

Exercise **(9.8)**. — Show that a ring of polynomials P is faithfully flat.

Example **(9.9)**. — In **(9.6)**, consider the second assertion. Its converse needn't hold. For example, take a product ring $R := R_1 \times R_2$ with $R_i \neq 0$. By **(9.7)**, R is faithfully flat over R. But neither R_i is so, as $R_1 \otimes R_2 = R_1 \otimes (R/R_1) = R_1/R_1^2 = 0$.

Exercise **(9.10)**. — Let R be a ring, M and N flat modules. Show that $M \otimes_R N$ is flat. What if "flat" is replaced everywhere by "faithfully flat"?

Exercise **(9.11)**. — Let R be a ring, M a flat module, R' an algebra. Show that $M \otimes_R R'$ is flat over R'. What if "flat" is replaced everywhere by "faithfully flat"?

Exercise **(9.12)**. — Let R be a ring, R' a flat algebra, M a flat R'-module. Show that M is flat over R. What if "flat" is replaced everywhere by "faithfully flat"?

Exercise **(9.13)**. — Let R be a ring, R' an algebra, R'' an R'-algebra, and M an R''-module. Assume that M is flat over R and faithfully flat over R'. Prove that R' is flat over R.

Exercise **(9.14)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $R/\mathfrak{a}$ is flat. Show $\mathfrak{a} = \mathfrak{a}^2$.

Exercise **(9.15)**. — Let R be a ring, R' a flat algebra. Prove equivalent:

(1) R' is faithfully flat over R.
(2) For every R-module M, the map $M \xrightarrow{\alpha} M \otimes_R R'$ by $\alpha m = m \otimes 1$ is injective.
(3) Every ideal $\mathfrak{a}$ of R is the contraction of its extension, or $\mathfrak{a} = \varphi^{-1}(\mathfrak{a}R')$.
(4) Every prime $\mathfrak{p}$ of R is the contraction of some prime $\mathfrak{q}$ of R', or $\mathfrak{p} = \varphi^{-1}\mathfrak{q}$.
(5) Every maximal ideal $\mathfrak{m}$ of R extends to a proper ideal, or $\mathfrak{m}R' \neq R'$.
(6) Every nonzero R-module M extends to a nonzero module, or $M \otimes_R R' \neq 0$.

Proposition **(9.16)**. — *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 **(5.20)**, 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:

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & M' \otimes K \arrow[r] \arrow[d] & M \otimes K \arrow[r] \arrow[d] & M'' \otimes K \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & M' \otimes R^{\oplus\Lambda} \arrow[r, "\beta"] \arrow[d] & M \otimes R^{\oplus\Lambda} \arrow[r] \arrow[d] & M'' \otimes R^{\oplus\Lambda} & \\
 & M' \otimes N \arrow[r, "\gamma"] \arrow[d] & M \otimes N \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

Here α and β are injective by Definition **(9.5)**, as M'' and $R^{\oplus\Lambda}$ are flat by hypothesis and by **(9.7)**. So the rows and columns are exact, as tensor product is right exact. Finally, the Snake Lemma, **(5.13)**, implies γ is injective. Thus (1) holds.

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

$$\begin{tikzcd}
0 \arrow[r] & M' \otimes N' \arrow[r] \arrow[d, "\alpha'"'] & M \otimes N' \arrow[r] \arrow[d, "\alpha"'] & M'' \otimes N' \arrow[r] \arrow[d, "\alpha''"'] & 0 \\
0 \arrow[r] & M' \otimes N \arrow[r] & M \otimes N \arrow[r] & M'' \otimes N \arrow[r] & 0
\end{tikzcd}$$

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. □

Exercise **(9.17)**. — Let R be a ring, $0 \to M' \xrightarrow{\alpha} M \to M'' \to 0$ an exact sequence with M flat. Assume $N \otimes M' \xrightarrow{N \otimes \alpha} N \otimes M$ is injective for all N. Prove M'' is flat.

Exercise **(9.18)**. — Prove that an R-algebra R' is faithfully flat if and only if the structure map $\varphi\colon R \to R'$ is injective and the quotient $R'/\varphi R$ is flat over R.

Proposition **(9.19)**. — *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, **(7.14)**. So $(\varinjlim M_\lambda) \otimes \beta$ is injective by **(8.13)**. Thus $\varinjlim M_\lambda$ is flat. □

Proposition **(9.20)**. — *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*

$$\theta\colon \mathrm{Hom}_R(M,\, N) \otimes_{R'} P \to \mathrm{Hom}_R(M,\, N \otimes_{R'} P). \qquad \textbf{(9.20.1)}$$

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, **(8.18)**, with R' for R, applied to $\mathrm{Hom}_R(M, N \otimes_{R'} \bullet)$. Explicitly, $\theta(\varphi \otimes p)(m) = \varphi(m) \otimes p$.

Clearly, θ is bijective if $M = R$. So θ is bijective if $M = R^n$ for any n, as $\mathrm{Hom}_R(\bullet, Q)$ preserves finite direct sums for any Q by **(4.15)**.

Assume that M is finitely generated. Then from **(5.20)**, we obtain a presentation $R^{\oplus\Sigma} \to R^n \to M \to 0$, with Σ finite if P is finitely presented. Since θ is natural, it yields this commutative diagram:

$$\begin{array}{ccccccc}
0 \to & \mathrm{Hom}_R(M,N) \otimes_{R'} P & \to & \mathrm{Hom}_R(R^n,N) \otimes_{R'} P & \to & \mathrm{Hom}_R(R^{\oplus\Sigma},N) \otimes_{R'} P \\
& \theta\big\downarrow & & \simeq\big\downarrow & & \big\downarrow \\
0 \to & \mathrm{Hom}_R(M,N \otimes_{R'} P) & \to & \mathrm{Hom}_R(R^n,N \otimes_{R'} P) & \to & \mathrm{Hom}_R(R^{\oplus\Sigma},\, N \otimes_{R'} P)
\end{array}$$

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 Σ is finite. The assertion follows. □

Exercise **(9.21)**. — Let R be a ring, R' an algebra, M and N modules. Show that there is a canonical map

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

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 **(9.22)**. — 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 **(9.23)**. — *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 $(R,\, \alpha_x)$ 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 **(9.24)** (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* **(9.20.1)** *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 **(9.20)** yields (2).

Assume (2). Consider (3). There are $\gamma_1, \dots, \gamma_n \in \mathrm{Hom}(P, R)$ and $x_1, \dots, x_n \in M$ with $\beta(p) = \sum \gamma_i(p) x_i$ by (2). 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 $\beta = \alpha\gamma$, just 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 **(9.23)**.

Assume (8). Say $M = \varinjlim M_\lambda$ with the M_λ free. Each M_λ is flat by **(9.5)**, and a filtered direct limit of flat modules is flat by **(9.19)**. Thus M is flat □

Exercise **(9.25)** (*Equational Criterion for Flatness*). — Prove that the Condition **(9.24)**(4) can be reformulated as follows: Given any 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

$$\textstyle\sum_j x_{ij}y'_j = y_i \text{ for all } i \text{ and } \sum_i x_{ij}x_i = 0 \text{ for all } j. \qquad \textbf{(9.25.1)}$$

Lemma **(9.26)** (Ideal Criterion for Flatness). — *A module N is flat if and only if, given any finitely generated ideal $\mathfrak{a}$, the inclusion $\mathfrak{a} \hookrightarrow R$ induces an isomorphism:*

$$\mathfrak{a} \otimes N \xrightarrow{\sim} \mathfrak{a}N.$$

Proof: In any case, **(8.6)**(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 **(9.25)**. Given $\sum_{i=1}^n x_iy_i = 0$ with $x_i \in R$ and $y_i \in N$, set $\mathfrak{a} := \langle x_1, \ldots, x_n \rangle$. 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 **(8.21)** yields **(9.25.1)**. Thus N is flat. □

Example **(9.27)**. — Let R be a domain, and set $K := \mathrm{Frac}(R)$. Then K is flat, but K is not projective unless $R = K$. Indeed, **(8.7)** says $\mathfrak{a} \otimes_R K = K$, with $a \otimes x = ax$, for any ideal $\mathfrak{a}$ of R. So K is flat by **(9.26)**.

Suppose K is projective. Then $K \hookrightarrow R^\Lambda$ for some Λ by **(5.23)**. 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 **(9.28)**. — Let R be a ring, M a module. Prove (1) if M is flat, then for $x \in R$ and $m \in M$ with $xm = 0$, necessarily $m \in \mathrm{Ann}(x)M$, and (2) the converse holds if R is a **Principal Ideal Ring** (PIR); that is, every ideal $\mathfrak{a}$ is principal.

10. Cayley–Hamilton Theorem

The Cayley–Hamilton Theorem says that a matrix satisfies its own characteristic polynomial. We prove it via a useful 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 integral dependence 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:

$$p_{\mathbf{M}}(T) := T^n + a_1T^{n-1} + \cdots + a_n := \det(T\mathbf{I}_n - \mathbf{M}).$$

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 $m_1, \ldots, m_n$ 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 e_i 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 $m_1, \ldots, m_n$, 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 $\mathrm{End}(M)$.*

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 the commutative subring $R[\varphi]$ of $\mathrm{End}(M)$, and $\mathbf{X}$ for the column vector (m_j). 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 $\mathbf{\Gamma\Delta X} = 0$. But $\mathbf{\Gamma\Delta} = \det(\mathbf{\Delta})\mathbf{I}_n$. So $\det(\mathbf{\Delta})m_j = 0$ for all j. Hence $\det(\mathbf{\Delta}) = 0$. But $\det(\mathbf{\Delta}) = p_{\mathbf{M}}(\varphi)$. 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 $m_1, \ldots, m_n$ 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 $p_{\mathbf{M}}(T) = T^n + a_1T^{n-1} + \cdots + a_n$. 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 a 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 $a = Xq(X)$ for some polynomial $q(X)$. Then $1_M + \varphi q(\varphi) = 0$. Set $\psi = -q(\varphi)$. Then $\varphi\psi = 1$ and $\psi\varphi = 1$. Thus φ is an isomorphism. □

Corollary **(10.5)**. — *Let R be a nonzero 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 $\varphi\colon R^n \twoheadrightarrow R^n$ 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 it can contain no zeros. Thus $n - m = 0$. □

Exercise **(10.6)**. — Let R be a nonzero ring, $\alpha\colon R^m \to R^n$ a map of free modules. Assume α is surjective. Show that $m \ge n$.

Exercise **(10.7)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a}$ is finitely generated and idempotent (or $\mathfrak{a} = \mathfrak{a}^2$). Prove there is a unique idempotent e with $\langle e \rangle = \mathfrak{a}$.

Exercise **(10.8)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Prove the following 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 finitely generated and idempotent.
(4) $\mathfrak{a}$ is generated by an idempotent.
(5) $\mathfrak{a}$ is a direct summand of R.

Exercise **(10.9)**. — Prove the following conditions on a ring R are equivalent:
(1) R is **absolutely flat**; that is, every module is flat.
(2) Every finitely generated ideal is a direct summand of R.
(3) Every finitely generated ideal is idempotent.
(4) Every principal ideal is idempotent.

Exercise **(10.10)**. — Let R be a ring.
(1) Assume R is Boolean. Prove R is absolutely flat.
(2) Assume R is absolutely flat. Prove any quotient ring R' is absolutely flat.
(3) Assume R is absolutely flat. Prove every nonunit x is a zerodivisor.
(4) Assume R is absolutely flat and local. Prove R is a field.

Lemma **(10.11)** (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 $M \ne 0$. Say $m_1, \dots, m_n$ generate M with n minimal. Then $n \ge 1$ and $m_1 = a_1m_1 + \cdots + a_nm_n$ with $a_i \in \mathfrak{m}$. By **(3.2)**, we may set $x_i := (1-a_1)^{-1}a_i$. Then $m_1 = x_2m_2 + \cdots + x_nm_n$, contradicting minimality of n. Thus $n = 0$ and so $M = 0$. □

Example **(10.12)**. — Nakayama's Lemma **(10.11)** may fail if the module is not finitely generated. For example, let A be a local domain, $\mathfrak{m}$ the maximal ideal, and K the fraction field. Assume A is not a field, so that there's a nonzero $x \in \mathfrak{m}$. Then any $z \in K$ can be written in the form $z = x(z/x)$. Thus $K = \mathfrak{m}K$, but $K \ne 0$.

Proposition **(10.13)**. — *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 **(10.11)** 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 **(10.14)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and $\alpha\colon M \to N$ a map of modules. Assume that $\mathfrak{a} \subset \mathrm{rad}(R)$, that N is finitely generated, and that the induced map $\overline{\alpha}\colon M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective. Show that α is surjective.

Exercise **(10.15)**. — Let R be a ring, $\mathfrak{m} \subset \mathrm{rad}(R)$ an ideal. Let $\alpha, \beta\colon M \rightrightarrows N$ be two maps of finitely generated modules. Assume that α is an isomorphism and that $\beta(M) \subset \mathfrak{m}N$. Set $\gamma := \alpha + \beta$. Show that γ is an isomorphism.

Exercise **(10.16)**. — 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 **(10.17)**. — 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 $M \otimes_A N \ne 0$ if $M \ne 0$ and $N \ne 0$.

(10.18) (*Local Homomorphisms*). — Let $\varphi\colon A \to B$ be a map of local rings, $\mathfrak{m}$ and $\mathfrak{n}$ their maximal ideals. Then the following three conditions are equivalent:

$$(1)\ \varphi^{-1}\mathfrak{n} = \mathfrak{m};\quad (2)\ 1 \notin \mathfrak{m}B;\quad (3)\ \mathfrak{m}B \subset \mathfrak{n}. \qquad \textbf{(10.18.1)}$$

Indeed, if (1) holds, then $\mathfrak{m}B = (\varphi^{-1}\mathfrak{n})B \subset \mathfrak{n}$; so (2) holds. If (2) holds, then $\mathfrak{m}B$ lies is some maximal ideal, but $\mathfrak{n}$ is the only one; thus (3) holds. If (3) holds, then $\mathfrak{m} \subset \varphi^{-1}(\mathfrak{m}B) \subset \varphi^{-1}\mathfrak{n}$; whence, (1) holds as $\mathfrak{m}$ is maximal.

If the above conditions hold, then we say $\varphi\colon A \to B$ is a **local homomorphism.**

Exercise **(10.19)**. — Let $A \to B$ be a local homomorphism, M a finitely generated B-module. Prove that M is faithfully flat over A if and only if M is flat over A and nonzero. Conclude that, if B is flat over A, then B is faithfully flat over A.

Proposition **(10.20)**. — *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 **(5.22)**, and a projective module is always flat by **(9.7)**. 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 **(5.23)**. 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 **(9.16)**(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 **(8.13)** 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 **(10.16)**. Therefore, $\dim_k L \otimes k = 0$; so $L \otimes k = 0$.

Assume P is finitely presented. Then L is finitely generated by **(5.26)**. Hence $L = 0$ by **(10.17)**(1). So $F = P$. Thus (3) implies (1). □

Definition **(10.21)**. — 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

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0. \qquad \textbf{(10.21.1)}$$

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 **(10.22)**. — Let G be a finite group of automorphisms of a ring R. Form the subring R^G of invariants. Show that every $x \in R$ is integral over R^G, in fact, over the subring R' generated by the elementary symmetric functions in the conjugates gx for $g \in G$.

Proposition **(10.23)**. — *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 $m \ge n$, 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 **(10.24)**. — 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 **(10.25)**. — *Let R be a ring, $P = R[X]$ 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 **(10.23)**. 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 **(10.23)** 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 **(10.26)**. — *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 **(10.27)** (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 **(10.23)**. So R_m is module finite over R by **(10.26)** 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 **(10.23)**. Hence $R_n[x]$ is module finite over R by **(10.26)**. So x is integral over R by (3)⇒(1) of **(10.23)**, as desired. □

Theorem **(10.28)**. — *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 **(10.23)**. We may assume R' is module finite over R'' by induction on n. So **(10.26)** yields (3).

If (3) holds, then R' is integral over R by (3)⇒(1) of **(10.23)**; so (1) holds. □

Exercise **(10.29)**. — 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 **(10.30)**. — 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 **(10.31)**. — 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 $x := (x_1, \ldots, x_r)$. 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.

Theorem **(10.32)**. — *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)$\Rightarrow$(1) of **(10.28)**. 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 **(10.27)**. □

Theorem **(10.33)** (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 **(10.21.1)**. 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 **(10.34)**. — (1) A polynomial ring in n variables over a field is a UFD, so normal by **(10.33)**.

(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 [**12**, p. 292]. Hence, $\mathbb{Z}[\tau]$ is a UFD, so normal by **(10.33)**; 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 [**2**, 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 **(2.17)**. Clearly $\mathfrak{p} \supset \langle Y^2 - X^3 \rangle$. Since $Y^2 - X^3$ is irreducible, **(2.28)** 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 **(10.35)**. — 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 $\mathrm{Frac}(R)$.

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 subset. The result is universal among algebras rendering all these elements units. When the multiplicative subset 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 finish by localizing algebras and then varying the set of denominators.

(11.1) (*Localization*). — Let R be a ring, and S a multiplicative subset. 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.

It is easy to check that *$S^{-1}R$ is a ring*, with $0/1$ for 0 and $1/1$ for 1. It is called the **ring of fractions with respect to** S or the **localization at** 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 subset. Prove $S^{-1}R = 0$ if and only if S contains a nilpotent element.

(11.3) (*Total quotient ring*). — Let R be a ring, and S_0 the set of nonzerodivisors. Then S_0 is a saturated multiplicative subset, as noted in **(3.15)**. The map $\varphi_{S_0}\colon R \to S_0^{-1}R$ is injective, because if $\varphi_{S_0} x = 0$, then $sx = 0$ for some $s \in S$, and so $x = 0$. We call $S_0^{-1}R$ the **total quotient ring** of R, and view R as a subring.

Let $S \subset S_0$ be a multiplicative subset. Clearly, $R \subset S^{-1}R \subset S_0^{-1}R$.

Suppose R is a domain. Then $S_0 = R - \{0\}$; so the total quotient ring is just the fraction field $\mathrm{Frac}(R)$, and φ_{S_0} is just the natural inclusion of R into $\mathrm{Frac}(R)$. Further, $S^{-1}R$ is a domain by **(2.3)** as $S^{-1}R \subset S_0^{-1}R = \mathrm{Frac}(R)$.

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 $S = \{3^i \mid i \ge 0\}$.

Theorem **(11.5)** (UMP). — *Let R be a ring, S a multiplicative subset. Then $S^{-1}R$ is the R-algebra universal among algebras rendering all the $s \in S$ 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:*

$$\begin{tikzcd} R \arrow[r, "\varphi_S"] \arrow[dr, "\psi"'] & S^{-1}R \arrow[d, "\rho"] \\ & R' \end{tikzcd}$$

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 subset. 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:

$$(x,s) \sim (y,t) \quad \text{if} \quad xt = ys.$$

Show that it is not an equivalence relation.

Exercise **(11.9)**. — Let R be a ring, $S \subset T$ a multiplicative subsets, $\overline{S}$ and $\overline{T}$ their saturations; see **(3.17)**. Set $U := (S^{-1}R)^{\times}$. Show the following:

(1) $U = \{\, x/s \mid x \in \overline{S} \text{ and } s \in S \,\}$. (2) $\varphi_S^{-1}U = \overline{S}$.
(3) $S^{-1}R = T^{-1}R$ if and only if $\overline{S} = \overline{T}$. (4) $\overline{S}^{-1}R = S^{-1}R$.

Exercise **(11.10)**. — Let R be a ring, $S \subset T \subset U$ and W multiplicative subsets.

(1) Show there's a unique R-algebra map $\varphi_T^S \colon S^{-1}R \to T^{-1}R$ and $\varphi_U^T\varphi_T^S = \varphi_U^S$.
(2) Given a map $\varphi\colon S^{-1}R \to W^{-1}R$, show $S \subset \overline{S} \subset \overline{W}$ and $\varphi = \varphi_{\overline{W}}^S$.
(3) Let Λ be a set, $S_\lambda \subset S$ a multiplicative subset for all $\lambda \in \Lambda$. Assume $\bigcup S_\lambda = S$. Assume given $\lambda, \mu \in \Lambda$, there is ν such that $S_\lambda, S_\mu \subset S_\nu$. Order Λ by inclusion: $\lambda \le \mu$ if $S_\lambda \subset S_\mu$. Using (1), show $\varinjlim S_\lambda^{-1}R = S^{-1}R$.

Exercise **(11.11)**. — Let R be a ring, S_0 the set of nonzerodivisors.

(1) Show S_0 is the largest multiplicative subset S with $\varphi_S \colon R \to S^{-1}R$ injective.
(2) Show every element x/s of $S_0^{-1}R$ is either a zerodivisor or a unit.
(3) Suppose every element of R is either a zerodivisor or a unit. Show $R = S_0^{-1}R$.

Definition **(11.12)**. — Let R be a ring, $f \in R$. Set $S := \{f^n \mid n \ge 0\}$. 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 **(11.13)**. — *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 $n \ge 0$.

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 **(11.14)**. — *Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ 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, $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = R$. Finally, 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 **(11.15)**. — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ a subset of R. 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 **(11.16)**. — *Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ 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 **(11.17)**. — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Show (1) if $\mathfrak{a} \subset \mathfrak{b}$, then $\mathfrak{a}^S \subset \mathfrak{b}^S$; (2) $(\mathfrak{a}^S)^S = \mathfrak{a}^S$; and (3) $(\mathfrak{a}^S\mathfrak{b}^S)^S = (\mathfrak{a}\mathfrak{b})^S$.

Exercise **(11.18)**. — Let R be a ring, S a multiplicative subset. Prove that

$$\mathrm{nil}(R)(S^{-1}R) = \mathrm{nil}(S^{-1}R).$$

Proposition **(11.19)**. — *Let R be a ring, S a multiplicative subset.*

(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 **(11.14)**(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), first note $\mathfrak{p}S^{-1}R \neq S^{-1}R$ as $\varphi_S^{-1}(\mathfrak{p}S^{-1}R) = \mathfrak{p}^S = \mathfrak{p}$ by (2) and (3)(a) and as $1 \notin \mathfrak{p}$. Second, 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 **(11.20)**. — *Let R be a ring, S a multiplicative subset.*

(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 **(11.19)**(1), (2); clearly, they preserve inclusions. Further, (1) implies (2) by **(11.19)**(3), by **(2.8)**, and by **(11.14)**(2). □

Definition **(11.21)**. — 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 **(11.22)**. — *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 **(11.14)**(2). Hence **(11.20)**(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 **(11.14)**(1), the nonunits of $R_{\mathfrak{p}}$ form $\mathfrak{p}R_{\mathfrak{p}}$, which is an ideal. Hence **(3.6)** yields the assertion. □

(11.23) (*Algebras*). — Let R be a ring, S a multiplicative subset, 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 $\varphi'_S : R' \to S^{-1}R'$ 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 $\psi: R' \to R''$ such that elements of S become units in R'', there is a unique R-algebra map $\rho: S^{-1}R' \to R''$ such that $\rho\varphi'_S = \psi$; that is, the following diagram is commutative:*

$$\begin{tikzcd} R' \arrow[r, "\varphi'_S"] \arrow[dr, "\psi"'] & S^{-1}R' \arrow[d, "\rho"] \\ & R'' \end{tikzcd}$$

In other words, $S^{-1}R'$ is *universal* among R'-algebras rendering the $s \in S$ units.

Let $\tau: R' \to R''$ be an R-algebra map. Then there is a commutative diagram of R-algebra maps

$$\begin{tikzcd} R' \arrow[r, "\tau"] \arrow[d, "\varphi_S"'] & R'' \arrow[d, "\varphi'_S"] \\ S^{-1}R' \arrow[r, "S^{-1}\tau"] & S^{-1}R'' \end{tikzcd}$$

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,

$$S^{-1}R' = T^{-1}R', \tag{11.23.1}$$

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 **(11.24)**. — 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 **(11.25)**. — 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 $L = \mathrm{Frac}(\overline{R})$. 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 **(11.26)**. — 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 **(11.27)**. — *Let R be a ring, S a multiplicative subset. Let T' be a multiplicative subset 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 $\psi: R \to R'$ 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 $\rho: S^{-1}R \to R'$. 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 $\rho': (T')^{-1}(S^{-1}R) \to R'$. Hence $\psi = \rho'\varphi_{T'}\varphi_S$, and ρ' is clearly unique, as required. □

Corollary **(11.28)**. — *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 **(11.20)**(2). So $S \subset T$, and **(11.27)** yields the assertion. □

Exercise **(11.29)**. — Let R be a ring, S and T multiplicative subsets.

(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

$$T^{-1}(S^{-1}R) = S^{-1}(T^{-1}R) = U^{-1}R.$$

Proposition **(11.30)**. — *Let R be a ring, S a multiplicative subset, X a variable. Then $(S^{-1}R)[X] = S^{-1}\big(R[X]\big)$.*

Proof: In spirit, the proof is like that of **(1.7)**: the two rings are equal, as each is universal among R-algebras with a distinguished element and where the $s \in S$ become units. □

Corollary **(11.31)**. — *Let R be a ring, S a multiplicative subset, 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 **(11.30)** and **(11.20)**(2). □

Exercise **(11.32)** (*Localization and normalization commute*). — Given a domain R and a multiplicative subset S with $0 \notin S$. Show that the localization of the normalization $S^{-1}\overline{R}$ is equal to the normalization of the localization $\overline{S^{-1}R}$.

12. Localization of Modules

Formally, we localize a module just as we do a ring. 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 universal among modules with those two properties. Consequently, Localization is a functor; in fact, it is the left adjoint of Restriction of Scalars from the localized ring to the base ring. So Localization preserves direct limits, or equivalently, direct sums and cokernels. Further, by uniqueness of left adjoints or by Watts's Theorem, Localization is naturally isomorphic to Tensor Product with the localized ring. Moreover, Localization is exact; so the localized ring is flat. We end the section by discussing various compatibilities and examples.

Proposition **(12.1)**. — *Let R be a ring, S a multiplicative subset. 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 $\mu_R\colon R \to \mathrm{End}_{\mathbb{Z}}(M)$ sends S into the units of $\mathrm{End}_{\mathbb{Z}}(M)$. Hence μ_R factors through a unique ring map $\mu_{S^{-1}R}\colon S^{-1}R \to \mathrm{End}_{\mathbb{Z}}(M)$ 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 subset, 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, let $\mathfrak{a}$ be an ideal. Then $S^{-1}\mathfrak{a} = \mathfrak{a}S^{-1}R$ by **(11.14)**(1). Similarly, $S^{-1}(\mathfrak{a}M) = S^{-1}\mathfrak{a}S^{-1}M = \mathfrak{a}S^{-1}M$. 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 **(11.23)**.

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 subset, and M a module. Then $S^{-1}M$ is universal among $S^{-1}R$-modules 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 subset, 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 subsets, 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 subset. Show that S becomes a filtered category when equipped as follows: given $s, t \in S$, set

$$\operatorname{Hom}(s,t) := \{x \in R \mid xs = t\}.$$

Given a module M, define a functor $S \to ((R\text{-mod}))$ as follows: for $s \in S$, set $M_s := M$; to each $x \in \operatorname{Hom}(s,t)$, 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 subset, M a module. Prove $S^{-1}M = 0$ if $\operatorname{Ann}(M) \cap S \neq \emptyset$. Prove the converse if M is finitely generated.

Exercise **(12.8)**. — Let R be a ring, M a finitely generated module, $\mathfrak{a}$ an ideal.

(1) Set $S := 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ lies in the radical of $S^{-1}R$.

(2) Use (1), Nakayama's Lemma **(10.11)**, and **(12.7)**, but not the determinant trick **(10.2)**, to prove this part of **(10.3)**: if $M = \mathfrak{a}M$, then $sM = 0$ for an $s \in S$.

(12.9) (*Functoriality*). — Let R be a ring, S a multiplicative subset, $\alpha\colon M \to N$ 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

$$(S^{-1}\alpha)(m/s) = \alpha(m)/s. \qquad \textbf{(12.9.1)}$$

Thus, canonically, we obtain the following map, and clearly, it is R-linear:

$$\operatorname{Hom}_R(M,\, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M,\, S^{-1}N). \qquad \textbf{(12.9.2)}$$

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 **(12.9.1)**. Thus $S^{-1}(\bullet)$ *is a linear functor* from $((R\text{-mod}))$ to $((S^{-1}R\text{-mod}))$.

Theorem **(12.10)**. — *Let R be a ring, S a multiplicative subset. 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 **(12.9.2)** is bijective with inverse taking $\beta\colon S^{-1}M \to N$ to $\beta\varphi_S\colon M \to N$. And **(12.9.2)** is natural in M and N by **(6.3)**. Thus the assertion holds. □

Corollary **(12.11)**. — *Let R be a ring, S a multiplicative subset. Then the functor $S^{-1}(\bullet)$ preserves direct limits, or equivalently, direct sums and cokernels.*

Proof: By **(12.10)**, 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 **(12.12)**. — Let R be a ring, S a multiplicative subset, P a projective module. Then $S^{-1}P$ is a projective $S^{-1}R$-module.

Corollary **(12.13)**. — *Let R be a ring, S a multiplicative subset. 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 **(12.11)**, the assertion is an immediate consequence of Watts Theorem **(8.18)**.

Alternatively, both functors are left adjoints of the same functor by **(12.10)** and by **(8.11)**. So they are canonically isomorphic by **(6.4)**. □

Exercise **(12.14)**. — Let R be a ring, S a multiplicative subset, M and N modules. Show $S^{-1}(M \otimes_R N) = S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} S^{-1}N = S^{-1}M \otimes_R S^{-1}N$.

Exercise **(12.15)**. — Let R be a ring, R' an algebra, S a multiplicative subset, M a finitely presented module, and r an integer. Show

$$F_r(M \otimes_R R') = F_r(M)R' \quad\text{and}\quad F_r(S^{-1}M) = F_r(M)S^{-1}R = S^{-1}F_r(M).$$

Definition **(12.16)**. — Let R be a ring, S a multiplicative subset, 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 **(12.17)**. — *Let R be a ring, M a module, N and P submodules. Let S be a multiplicative subset, 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,* $\operatorname{Ker}(\varphi_S) = 0^S$.
(4) *Then* (a) $(N^S)^S = N^S$ *and* (b) $S^{-1}(S^{-1}N) = S^{-1}N$.
(5) *If $N \subset P$, then* (a) $N^S \subset P^S$ *and* (b) $S^{-1}N \subset S^{-1}P$.
(6) *Then* (a) $(N \cap P)^S = N^S \cap P^S$ *and* (b) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.
(7) *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. Assertion (5)(b) follows by taking $M := P$. Assertion (4)(b) follows from **(12.4)** with $M := S^{-1}M$.

Assertions (1)(a), (2), (3) can be proved as in **(11.16)**(3) and **(11.19)**(1), (2). Assertions (4)(a) and (5)(a) can be proved as in **(11.16)**(1) and (2).

As to (6)(a), clearly $(N \cap P)^S \subset N^S \cap P^S$. Conversely, given $n \in N^S \cap P^S$, there are $s, t \in S$ with $sn \in N$ and $tn \in P$. Then $stn \in N \cap P$ and $st \in S$. So $n \in (N \cap P)^S$. Thus (a) holds. Alternatively, (6)(b) and (3) yield (6)(a).

As to (6)(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 $n/s = p/t \in S^{-1}N \cap S^{-1}P$, there is a $u \in S$ with $utn = usp \in N \cap P$. Hence $utn/uts = usp/uts \in S^{-1}(N \cap P)$. Thus (b) holds.

As to (7)(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 (7)(a) holds.

As to (7)(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 (7)(b) holds. □

Exercise **(12.18)**. — Let R be a ring, S a multiplicative subset.

(1) Let $M_1 \xrightarrow{\alpha} M_2$ be a map of modules, which restricts to a map $N_1 \to N_2$ of submodules. Show $\alpha(N_1^S) \subset N_2^S$; that is, there is an induced map $N_1^S \to N_2^S$.

(2) Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$ be a left exact sequence, which restiсts to a left exact sequence $0 \to N_1 \to N_2 \to N_3$ of submodules. Show there is an induced left exact sequence of saturations: $0 \to N_1^S \to N_2^S \to N_3^S$.

Exercise **(12.19)**. — Let R be a ring, M a module, and S a multiplicative subset. Set $T^S M := \langle 0\rangle^S$. We call it the **$S$-torsion submodule of** M. Prove the following:

(1) $T^S(M/T^S M) = 0$. (2) $T^S M = \mathrm{Ker}(\varphi_S)$.

(3) Let $\alpha\colon M \to N$ be a map. Then $\alpha(T^S M) \subset T^S N$.

(4) Let $0 \to M' \to M \to M''$ be exact. Then so is $0 \to T^S M' \to T^S M \to T^S M''$.

(5) Let $S_1 \subset S$ be a multiplicative subset. Then $T^S(S_1^{-1}M) = S_1^{-1}(T^S M)$.

Theorem **(12.20)** (Exactness of Localization). — *Let R be a ring, and S a multiplicative subset. Then the functor $S^{-1}(\bullet)$ is exact.*

Proof: As $S^{-1}(\bullet)$ preserves injections by **(12.17)**(1) and cokernels by **(12.11)**, 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 **(7.14)**, 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 **(12.21)**. — *Let R be a ring, S a multiplicative subset. Then $S^{-1}R$ is flat over R.*

Proof: The functor $S^{-1}(\bullet)$ is exact by **(12.20)**, and is isomorphic to $S^{-1}R\otimes_R\bullet$ by **(12.13)**. 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 **(9.7)**. Thus $S^{-1}R$ is flat by **(9.19)**. □

Corollary **(12.22)**. — *Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal, and M a module. Then $S^{-1}(M/\mathfrak{a}M) = S^{-1}M\big/S^{-1}(\mathfrak{a}M) = S^{-1}M\big/\mathfrak{a}S^{-1}M$.*

Proof: The assertion results from **(12.20)** and **(12.2)**. □

Corollary **(12.23)**. — *Let R be a ring, $\mathfrak{p}$ a prime. Then $\mathrm{Frac}(R/\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$.*

Proof: We have $\mathrm{Frac}(R/\mathfrak{p}) = (R/\mathfrak{p})_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ by **(11.23)** and **(12.22)**. □

Proposition **(12.24)**. — *Let R be a ring, M a module, S a multiplicative subset.*

(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 $C := \mathrm{Coker}(\alpha)$. Then $S^{-1}C = \mathrm{Coker}(S^{-1}\alpha)$ by **(12.11)**. 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 **(12.11)**. 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 $K := \mathrm{Ker}(\alpha)$. Then **(12.20)** yields $S^{-1}K = \mathrm{Ker}(S^{-1}\alpha)$ and $S^{-1}C = \mathrm{Coker}(S^{-1}\alpha)$. 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 **(12.20)**. Take a finite presentation $R^p \to R^q \to M \to 0$. By **(12.20)**, 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 **(5.26)**.

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 **(12.25)**. — *Let R be a ring, S a multiplicative subset, M and N modules. Then there is a canonical homomorphism*

$$\sigma\colon S^{-1}\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

Further, σ is injective if M is finitely generated, and σ is an isomorphism if M is finitely presented.

Proof: The assertions result from **(9.21)** with $R' := S^{-1}R$, since $S^{-1}R$ is flat by **(12.21)** and since $S^{-1}R \otimes P = S^{-1}P$ for every R-module P by **(12.13)**. □

Example **(12.26)**. — 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, $\mu_R\colon R \to \mathrm{Hom}_R(M, M)$ is injective. But $S^{-1}R = \mathbb{Q}$. So **(12.20)** yields $S^{-1}\mathrm{Hom}_R(M, M) \neq 0$. 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 **(12.25)** is not injective. Thus **(12.25)**(2) can fail if M is not finitely generated.

Example **(12.27)**. — 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 $S^{-1}\big(\prod M_n\big)$ as the kth component of $m \cdot (1, 1, \dots)$ is nonzero in $\prod M_n$ for $k > m$ if m is nonzero. Thus $S^{-1}\big(\prod M_n\big) \neq \prod(S^{-1}M_n)$.

Also $S^{-1}\mathbb{Z} = \mathbb{Q}$. So **(12.13)** yields $\mathbb{Q} \otimes \big(\prod M_n\big) \neq \prod(\mathbb{Q} \otimes M_n)$, whereas **(8.13)** yields $\mathbb{Q} \otimes \big(\bigoplus M_n\big) = \bigoplus(\mathbb{Q} \otimes M_n)$.

Exercise **(12.28)**. — 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 **(12.25)** is not injective.

13. Support

The spectrum of a ring is the following topological space: its points are the prime ideals, and each closed set consists of those primes containing a given ideal. The support of a module is the following 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 every maximal ideal. We end this section by proving that the following conditions on a module ar equivalent: it is finitely generated and projective; it is finitely presented and flat; and 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 $\mathrm{Spec}(R)$, and is called the (prime) **spectrum** of R.

Let $\mathfrak{a}$ be an ideal. Let $\mathbf{V}(\mathfrak{a})$ denote the subset of $\mathrm{Spec}(R)$ consisting of those primes that contain $\mathfrak{a}$. We call $\mathbf{V}(\mathfrak{a})$ the **variety** of $\mathfrak{a}$.

Let $\mathfrak{b}$ be a second ideal. Obviously, if $\mathfrak{a} \subset \mathfrak{b}$, then $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$. Conversely, if $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$, then $\mathfrak{a} \subset \sqrt{\mathfrak{b}}$, owing to the Scheinnullstellensatz **(3.29)**. Therefore, $\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{b})$ 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,

$$\bigcap \mathbf{V}(\mathfrak{a}_\lambda) = \mathbf{V}\big(\sum \mathfrak{a}_\lambda\big).$$

Finally, $\mathbf{V}(R) = \emptyset$, and $\mathbf{V}(\langle 0\rangle) = \mathrm{Spec}(R)$. Thus the subsets $\mathbf{V}(\mathfrak{a})$ of $\mathrm{Spec}(R)$ are the closed sets of a topology; it is called the **Zariski topology**.

Given an element $f \in R$, we call the open set

$$\mathbf{D}(f) := \mathrm{Spec}(R) - \mathbf{V}(\langle f\rangle)$$

a **principal open set**. These sets form a basis for the topology of $\mathrm{Spec}(R)$; indeed, given any prime $\mathfrak{p} \not\supset \mathfrak{a}$, there is an $f \in \mathfrak{a} - \mathfrak{p}$, and so $\mathfrak{p} \in \mathbf{D}(f) \subset \mathrm{Spec}(R) - \mathbf{V}(\mathfrak{a})$. Further, $f, g \notin \mathfrak{p}$ if and only if $fg \notin \mathfrak{p}$, for any $f, g \in R$ and prime $\mathfrak{p}$; in other words,

$$\mathbf{D}(f) \cap \mathbf{D}(g) = \mathbf{D}(fg). \qquad \textbf{(13.1.1)}$$

A ring map $\varphi\colon R \to R'$ induces a set map

$$\mathrm{Spec}(\varphi)\colon \mathrm{Spec}(R') \to \mathrm{Spec}(R) \quad \text{by} \quad \mathrm{Spec}(\varphi)(\mathfrak{p}') := \varphi^{-1}(\mathfrak{p}'). \qquad \textbf{(13.1.2)}$$

Notice $\varphi^{-1}(\mathfrak{p}') \supset \mathfrak{a}$ if and only if $\mathfrak{p}' \supset \mathfrak{a}R'$; so $\mathrm{Spec}(\varphi)^{-1}\,\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{a}R')$. Hence $\mathrm{Spec}(\varphi)$ is continuous. Thus $\mathrm{Spec}(\bullet)$ is a contravariant functor from ((Rings)) to ((Top spaces)).

For example, the quotient map $R \to R/\mathfrak{a}$ induces a topological embedding

$$\mathrm{Spec}(R/\mathfrak{a}) \hookrightarrow \mathrm{Spec}(R), \qquad \textbf{(13.1.3)}$$

whose image is $\mathbf{V}(\mathfrak{a})$, owing to **(1.9)** and **(2.8)**. Furthermore, the localization map $R \to R_f$ induces a topological embedding

$$\mathrm{Spec}(R_f) \hookrightarrow \mathrm{Spec}(R), \qquad \textbf{(13.1.4)}$$

whose image is $\mathbf{D}(f)$, owing to **(11.20)**.

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.

Exercise **(13.3)**. — Let R be a ring, and set $X := \mathrm{Spec}(R)$. Let $X_1, X_2 \subset X$ be closed subsets. Show that the following three conditions are equivalent:

(1) $X_1 \cup X_2 = X$ and $X_1 \cap X_2 = \emptyset$.
(2) There are complementary idempotents $e_1, e_2 \in R$ with $\mathbf{V}(\langle e_i\rangle) = X_i$.
(3) There are comaximal ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1\mathfrak{a}_2 = 0$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.
(4) There are ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = R$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.

Finally, given any e_i and $\mathfrak{a}_i$ satisfying (2) and either (3) or (4), necessarily $e_i \in \mathfrak{a}_i$.

Exercise **(13.4)**. — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Prove these two statements:

(1) Every prime of R is a contraction of a prime if and only if φ^* is surjective.
(2) If every prime of R' is an extension of a prime, then φ^* is injective.

Is the converse of (2) true?

Exercise **(13.5)**. — Let R be a ring, S a multiplicative subset. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(S^{-1}R)$. Set $\varphi_S^* := \mathrm{Spec}(\varphi_S)$ and $S^{-1}X := \mathrm{Im}\,\varphi_S^* \subset X$. Show (1) that $S^{-1}X$ consists of the primes $\mathfrak{p}$ of R with $\mathfrak{p} \cap S = \emptyset$ and (2) that φ_S^* is a homeomorphism of Y onto $S^{-1}X$.

Exercise **(13.6)**. — Let $\theta\colon R \to R'$ be a ring map, $S \subset R$ a multiplicative subset. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$ and $\theta^* := \mathrm{Spec}(\theta)$. Via **(13.5)**(2) and **(11.23)**, identify $\mathrm{Spec}(S^{-1}R)$ and $\mathrm{Spec}(S^{-1}R')$ with their images $S^{-1}X \subset X$ and $S^{-1}Y \subset Y$. Show (1) $S^{-1}Y = \theta^{*-1}(S^{-1}X)$ and (2) $\mathrm{Spec}(S^{-1}\theta) = \theta^*\big|S^{-1}Y$.

Exercise **(13.7)**. — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{a} \subset R$ an ideal. Set $\mathfrak{b} := \mathfrak{a}R'$. Let $\overline{\theta}\colon R/\mathfrak{a} \to R'/\mathfrak{b}$ be the induced map. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$. Set $\theta^* := \mathrm{Spec}(\theta)$ and $\overline{\theta}^* := \mathrm{Spec}(\overline{\theta})$. Via **(13.1)**, identify $\mathrm{Spec}(R/\mathfrak{a})$ and $\mathrm{Spec}(R'/\mathfrak{b})$ with $\mathbf{V}(\mathfrak{a}) \subset X$ and $\mathbf{V}(\mathfrak{b}) \subset Y$. Show (1) $\mathbf{V}(\mathfrak{b}) = \theta^{*-1}(\mathbf{V}(\mathfrak{a}))$ and (2) $\overline{\theta}^* = \theta^*\big|\,\mathbf{V}(\mathfrak{b})$.

Exercise **(13.8)**. — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{p} \subset R$ a prime, k the residue field of $R_\mathfrak{p}$. Set $\theta^* := \mathrm{Spec}(\theta)$. Show (1) that $\theta^{*-1}(\mathfrak{p})$ is canonically homeomorphic to $\mathrm{Spec}(R' \otimes_R k)$ and (2) that $\mathfrak{p} \in \mathrm{Im}\,\theta^*$ if and only if $R' \otimes_R k \neq 0$.

Exercise **(13.9)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal. Show that the image of $\mathrm{Spec}(R_\mathfrak{p})$ in $\mathrm{Spec}(R)$ is the intersection of all open neighborhoods of $\mathfrak{p}$ in $\mathrm{Spec}(R)$.

Exercise **(13.10)**. — Let $\varphi\colon R \to R'$ and $\psi\colon R \to R''$ be ring maps, and define $\theta\colon R \to R' \otimes_R R''$ by $\theta(x) := \varphi(x) \otimes \psi(x)$. Show

$$\mathrm{Im}\,\mathrm{Spec}(\theta) = \mathrm{Im}\,\mathrm{Spec}(\varphi) \bigcap \mathrm{Im}\,\mathrm{Spec}(\psi).$$

Exercise **(13.11)**. — Let R be a filtered direct limit of rings R_λ with transition maps α^λ_μ and insertions α_λ. For each λ, let $\varphi_\lambda\colon R' \to R_\lambda$ be a ring map with $\varphi_\mu = \alpha^\lambda_\mu\varphi_\lambda$ for all α^λ_μ, so that $\varphi := \alpha_\lambda\varphi_\lambda$ is independent of λ. Show

$$\mathrm{Im}\,\mathrm{Spec}(\varphi) = \textstyle\bigcap_\lambda \mathrm{Im}\,\mathrm{Spec}(\varphi_\lambda).$$

Exercise **(13.12)**. — Let A be a domain with just one nonzero prime $\mathfrak{p}$. Set $K := \mathrm{Frac}(A)$ and $R := (A/\mathfrak{p}) \times K$. Define $\varphi\colon A \to R$ by $\varphi(x) := (x', x)$ with x' the residue of x. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Show φ^* is bijective, but not a homeomorphism.

Exercise **(13.13)**. — Let $\varphi\colon R \to R'$ be a ring map, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Show (1) that the closure $\overline{\varphi^*(\mathbf{V}(\mathfrak{b}))}$ in $\operatorname{Spec}(R)$ is equal to $\mathbf{V}(\varphi^{-1}\mathfrak{b})$ and (2) that $\varphi^*(\operatorname{Spec}(R'))$ is dense in $\operatorname{Spec}(R)$ if and only if $\operatorname{Ker}(\varphi) \subset \operatorname{nil}(R)$.

Exercise **(13.14)**. — Let R be a ring, R' a flat algebra with structure map φ. Show that R' is faithfully flat if and only if $\operatorname{Spec}(\varphi)$ is surjective.

Exercise **(13.15)**. — Let $\varphi\colon R \to R'$ be a flat map of rings, $\mathfrak{q}$ a prime of R', and $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Show that the induced map $\operatorname{Spec}(R'_{\mathfrak{q}}) \to \operatorname{Spec}(R_{\mathfrak{p}})$ is surjective.

Exercise **(13.16)**. — Let R be a ring. Given $f \in R$, set $S_f := \{f^n \mid n \ge 0\}$, and let $\overline{S}_f$ denote its saturation; see **(3.17)**. Given $f, g \in R$, show that the following conditions are equivalent:

(1) $\mathbf{D}(g) \subset \mathbf{D}(f)$. (2) $\mathbf{V}(\langle g\rangle) \supset \mathbf{V}(\langle f\rangle)$. (3) $\sqrt{\langle g\rangle} \subset \sqrt{\langle f\rangle}$.
(4) $\overline{S}_f \subset \overline{S}_g$. (5) $g \in \sqrt{\langle f\rangle}$. (6) $f \in \overline{S}_g$.
(7) there is a unique R-algebra map $\varphi^f_g\colon \overline{S}_f^{-1}R \to \overline{S}_g^{-1}R$.
(8) there is an R-algebra map $R_f \to R_g$.

Show that, if these conditions hold, then the map in (8) is equal to φ^f_g.

Exercise **(13.17)**. — Let R be a ring. (1) Show that $\mathbf{D}(f) \mapsto R_f$ is a well-defined contravariant functor from the category of principal open sets and inclusions to ((R-alg)). (2) Given $\mathfrak{p} \in \operatorname{Spec}(R)$, show $\varinjlim_{\mathbf{D}(f)\ni\mathfrak{p}} R_f = R_{\mathfrak{p}}$.

Exercise **(13.18)**. — A topological space is called **irreducible** if it's nonempty and if every pair of nonempty open subsets meet. Let R be a ring. Set $X := \operatorname{Spec}(R)$ and $\mathfrak{n} := \operatorname{nil}(R)$. Show that X is irreducible if and only if $\mathfrak{n}$ is prime.

Exercise **(13.19)**. — Let X be a topological space, Y an irreducible subspace.

(1) Show that the closure $\overline{Y}$ of Y is also irreducible.

(2) Show that Y is contained in a maximal irreducible subspace.

(3) Show that the maximal irreducible subspaces of X are closed, and cover X. They are called its **irreducible components**. What are they if X is Hausdorff?

(4) Let R be a ring, and take $X := \operatorname{Spec}(R)$. Show that its irreducible components are the closed sets $\mathbf{V}(\mathfrak{p})$ where $\mathfrak{p}$ is a minimal prime.

Proposition **(13.20)**. — *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 $U_\lambda = X - \mathbf{V}(\mathfrak{a}_\lambda)$. As $X = \bigcup_{\lambda\in\Lambda} U_\lambda$, then $\emptyset = \bigcap \mathbf{V}(\mathfrak{a}_\lambda) = \mathbf{V}\bigl(\sum \mathfrak{a}_\lambda\bigr)$. So $\sum \mathfrak{a}_\lambda$ lies in no prime ideal. Hence there are $\lambda_1, \dots, \lambda_n \in \Lambda$ and $f_{\lambda_i} \in \mathfrak{a}_{\lambda_i}$ with $1 = \sum f_{\lambda_i}$. So $R = \sum \mathfrak{a}_{\lambda_i}$. So $\emptyset = \bigcap \mathbf{V}(\mathfrak{a}_{\lambda_i}) = \mathbf{V}\bigl(\sum \mathfrak{a}_{\lambda_i}\bigr)$. Thus $X = \bigcup U_{\lambda_i}$. □

Exercise **(13.21)**. — Let R be a ring, $X := \operatorname{Spec}(R)$, and U an open subset. Show U is quasi-compact if and only if $X - U = \mathbf{V}(\mathfrak{a})$ where $\mathfrak{a}$ is finitely generated.

Exercise **(13.22)**. — Let R be a ring, M a module, $m \in M$. Set $X := \operatorname{Spec}(R)$. Assume $X = \bigcup \mathbf{D}(f_\lambda)$ for some f_λ, and $m/1 = 0$ in M_{f_λ} for all λ. Show $m = 0$.

Exercise **(13.23)**. — Let R be a ring; set $X := \operatorname{Spec}(R)$. Prove that the four following conditions are equivalent:

(1) $R/\operatorname{nil}(R)$ is absolutely flat.
(2) X is Hausdorff.
(3) X is T_1; that is, every point is closed.
(4) Every prime $\mathfrak{p}$ of R is maximal.

Assume (1) holds. Prove that X is **totally disconnected**; namely, no two distinct points lie in the same connected component.

Exercise **(13.24)**. — Let B be a Boolean ring, and set $X := \operatorname{Spec}(B)$. Show a subset $U \subset X$ is both open and closed if and only if $U = \mathbf{D}(f)$ for some $f \in B$. Further, show X is a compact Hausdorff space. (Following Bourbaki, we shorten "quasi-compact" to "compact" when the space is Hausdorff.)

Exercise **(13.25)** (*Stone's Theorem*). — Show every Boolean ring B is isomorphic to the ring of continuous functions from a compact Hausdorff space X to $\mathbb{F}_2$ with the discrete topology. Equivalently, show B is isomorphic to the ring R of open and closed subsets of X; in fact, $X := \operatorname{Spec}(B)$, and $B \xrightarrow{\sim} R$ is given by $f \mapsto \mathbf{D}(f)$.

Definition **(13.26)**. — Let R be a ring, M a module. Its **support** is the set

$$\operatorname{Supp}(M) := \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \ne 0 \,\}.$$

Proposition **(13.27)**. — *Let R be a ring, M a module.*

(1) *Let $0 \to L \to M \to N \to 0$ be exact. Then $\operatorname{Supp}(L) \bigcup \operatorname{Supp}(N) = \operatorname{Supp}(M)$.*
(2) *Let M_λ be submodules with $\sum M_\lambda = M$. Then $\bigcup \operatorname{Supp}(M_\lambda) = \operatorname{Supp}(M)$.*
(3) *Then $\operatorname{Supp}(M) \subset \mathbf{V}(\operatorname{Ann}(M))$, 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 **(12.20)**. So $M_{\mathfrak{p}} \ne 0$ if and only if $L_{\mathfrak{p}} \ne 0$ or $N_{\mathfrak{p}} \ne 0$. 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 **(12.11)**. 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 $\operatorname{Ann}(M) \cap (R - \mathfrak{p}) \ne \emptyset$, and the converse holds if M is finitely generated. But $\operatorname{Ann}(M) \bigcap (R - \mathfrak{p}) \ne \emptyset$ if and only if $\operatorname{Ann}(M) \not\subset \mathfrak{p}$. Thus (3) holds. □

Definition **(13.28)**. — Let R be a ring, $x \in R$. We say x is **nilpotent** on a module M if there is $n \ge 1$ with $x^n m = 0$ for all $m \in M$; that is, $x \in \sqrt{\operatorname{Ann}(M)}$. We denote the set of nilpotents on M by $\operatorname{nil}(M)$; that is, $\operatorname{nil}(M) := \sqrt{\operatorname{Ann}(M)}$.

Proposition **(13.29)**. — *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 **(3.29)**. But $\mathfrak{p} \supset \operatorname{Ann}(M)$ if and only if $\mathfrak{p} \in \operatorname{Supp}(M)$ by **(13.27)**(3). □

Proposition **(13.30)**. — *Let R be a ring, M and N modules. Then*

$$\operatorname{Supp}(M \otimes_R N) \subset \operatorname{Supp}(M) \cap \operatorname{Supp}(N), \qquad \textbf{(13.30.1)}$$

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 **(12.14)**; whence, **(13.30.1)** holds. The opposite inclusion follows from **(10.17)** if M and N are finitely generated. □

Exercise **(13.31)**. — Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Prove that
$$\operatorname{Supp}(M/\mathfrak{a}M) \subset \operatorname{Supp}(M) \cap \mathbf{V}(\mathfrak{a}),$$
with equality if M is finitely generated.

Exercise **(13.32)**. — Let $\varphi\colon R \to R'$ be a map of rings, M an R-module. Prove
$$\operatorname{Supp}(M \otimes_R R') \subset \operatorname{Spec}(\varphi)^{-1}(\operatorname{Supp}(M)),$$
with equality if M is finitely generated.

Exercise **(13.33)**. — Let R be a ring, M a module, $\mathfrak{p} \in \operatorname{Supp}(M)$. Prove
$$\mathbf{V}(\mathfrak{p}) \subset \operatorname{Supp}(M).$$

Exercise **(13.34)**. — 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 **(13.35)**. — *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 subset 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 **(13.36)**. — Let R be a domain, and M a module. Set $S := R - 0$ and $T(M) := T^S(M)$. We call $T(M)$ the **torsion submodule** of M, and we say M is **torsionfree** if $T(M) = 0$.

Prove M is torsionfree if and only if $M_{\mathfrak{m}}$ is torsionfree for all maximal ideals $\mathfrak{m}$.

Exercise **(13.37)**. — Let R be a ring, P a module, M, N submodules. Assume $M_{\mathfrak{m}} = N_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Show $M = N$. First assume $M \subset N$.

Exercise **(13.38)**. — Let R be a ring, M a module, and $\mathfrak{a}$ an ideal. Suppose $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \supset \mathfrak{a}$. Show that $M = \mathfrak{a}M$.

Exercise **(13.39)**. — Let R be a ring, P a module, M a submodule, and $p \in P$ an element. Assume $p/1 \in M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Show $p \in M$.

Exercise **(13.40)**. — Let R be a domain, $\mathfrak{a}$ an ideal. Show $\mathfrak{a} = \bigcap_{\mathfrak{m}} \mathfrak{a}R_{\mathfrak{m}}$ where $\mathfrak{m}$ runs through the maximal ideals and the intersection takes place in $\operatorname{Frac}(R)$.

Exercise **(13.41)**. — Prove these three conditions on a ring R are equivalent:
(1) R is reduced.
(2) $S^{-1}R$ is reduced for all multiplicative subsets S.
(3) $R_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$.

If $R_{\mathfrak{m}}$ is a domain for all maximal ideals $\mathfrak{m}$, is R necessarily a domain?

Exercise **(13.42)**. — 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 **(13.43)**. — *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 **(12.20)**.

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 **(12.20)** and **(9.3)**. Hence $\operatorname{Im}(\beta\alpha) = 0$ by **(13.35)**. So $\beta\alpha = 0$. Thus $\operatorname{Im}(\alpha) \subset \operatorname{Ker}(\beta)$.

Set $H := \operatorname{Ker}(\beta)\big/\operatorname{Im}(\alpha)$. Then $H_{\mathfrak{m}} = \operatorname{Ker}(\beta_{\mathfrak{m}})\big/\operatorname{Im}(\alpha_{\mathfrak{m}})$ by **(12.20)** and **(9.3)**. So $H_{\mathfrak{m}} = 0$ owing to the hypothesis. Hence $H = 0$ by **(13.35)**, as required. □

Exercise **(13.44)**. — 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 **(13.45)**. — *Let A be a semilocal ring, $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ its maximal ideals, M, N finitely presented modules. Assume $M_{\mathfrak{m}_i} \simeq N_{\mathfrak{m}_i}$ for each i. Then $M \simeq N$.*

Proof: For each i, take an isomorphism $\psi_i\colon M_{\mathfrak{m}_i} \xrightarrow{\sim} N_{\mathfrak{m}_i}$. Then **(12.25)** yields $s_i \in A - \mathfrak{m}_i$ and $\varphi_i\colon M \to N$ with $(\varphi_i)_{\mathfrak{m}_i} = s_i\psi_i$. However, **(2.2)** implies $\bigcap_{j\neq i}\mathfrak{m}_j \not\subset \mathfrak{m}_i$; so there's $x_i \in \bigcap_{j\neq i}\mathfrak{m}_j$ with $x_i \notin \mathfrak{m}_i$. Set $\gamma := \sum_i x_i s_i \varphi_i$.

For each j, set $\alpha_j := x_j s_j \psi_j$. Then $\alpha_{\mathfrak{m}_j}\colon M_{\mathfrak{m}_j} \xrightarrow{\sim} N_{\mathfrak{m}_j}$ as x_j and s_j are units. Set $\beta_j := \sum_{i\neq j}\alpha_i$. Then $\beta_j(M_{\mathfrak{m}_j}) \subset \mathfrak{m}_j N_{\mathfrak{m}_j}$ as $x_i \in \mathfrak{m}_j$ for $i \neq j$. Further, $\gamma = \alpha_j + \beta_j$. So $\gamma_{\mathfrak{m}_j}$ is an isomorphism by **(10.15)**. Hence **(13.43)** implies $\gamma\colon M \xrightarrow{\sim} N$. □

Proposition **(13.46)**. — *Let R be a ring, M a module. Then M is flat over R if and only if, at every maximal ideal $\mathfrak{m}$, the localization $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$.*

Proof: If M is flat over R, then $M \otimes_R R_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$ by **(9.11)**. But $M \otimes_R R_{\mathfrak{m}} = M_{\mathfrak{m}}$ by **(12.13)**. Thus $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$.

Conversely, assume $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$ for every $\mathfrak{m}$. Let $\alpha\colon N' \to N$ be an injection of R-modules. Then $\alpha_{\mathfrak{m}}$ is injective by **(13.43)**. Hence $M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} \alpha_{\mathfrak{m}}$ is injective. But that map is equal to $(M \otimes \alpha)_{\mathfrak{m}}$ by **(12.14)**. So $(M \otimes \alpha)_{\mathfrak{m}}$ is injective. Hence $M \otimes \alpha$ is injective by **(13.43)**. Thus M is flat over R. □

Exercise **(13.47)**. — Let R be a ring, R' a flat algebra, $\mathfrak{p}'$ a prime in R', and $\mathfrak{p}$ its contraction in R. Prove that $R'_{\mathfrak{p}'}$ is a faithfully flat $R_{\mathfrak{p}}$-algebra.

Exercise **(13.48)**. — Let R be a ring, S a multiplicative subset.
(1) Assume R is absolutely flat. Show $S^{-1}R$ is absolutely flat.
(2) Show R is absolutely flat if and only if $R_{\mathfrak{m}}$ is a field for each maximal $\mathfrak{m}$.

Definition **(13.49)**. — 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. It is enough that an f exist for each maximal ideal $\mathfrak{m}$ as every $\mathfrak{p}$ lies in some $\mathfrak{m}$ by **(2.30)**. Similarly, we define the properties **locally finitely presented**, **locally free of finite rank**, and **locally free of rank** n.

Proposition **(13.50)**. — *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 **(13.20)**, 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_i be the image of $R - \mathfrak{m}$ in R_{f_i}. Then **(12.5)** yields $M_{\mathfrak{m}} = S_i^{-1}(M_{f_i})$. Hence the $m_{i,j}/1$ generate

$M_{\mathfrak{m}}$. Thus **(13.44)** 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 **(5.26)**. 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 **(13.51)**. — *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 **(10.20)**.

Let $\mathfrak{m}$ be a maximal ideal. Then $R_{\mathfrak{m}}$ is local by **(11.22)**. If P is finitely presented, then $P_{\mathfrak{m}}$ is finitely presented, because localization preserves direct sums and cokernels by **(12.11)**.

Assume (2). Then $P_{\mathfrak{m}}$ is flat by **(13.46)**, so free by **(10.20)**. 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 **(5.23)** and **(5.22)**. But $\operatorname{Hom}(P_{\mathfrak{m}}, \alpha_{\mathfrak{m}}) = \operatorname{Hom}(P, \alpha)_{\mathfrak{m}}$ by **(12.25)** as P is finitely presented. Further, $\mathfrak{m}$ is arbitrary. Hence $\operatorname{Hom}(P, \alpha)$ is surjective by **(13.43)**. Therefore, P is projective by **(5.23)**. 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 **(12.24)**(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 **(13.50)**(2). Further, given $\mathfrak{p} \in \operatorname{Spec}(R)$, there are $f \in R - \mathfrak{p}$ and n such that P_f is free of rank n over R_f. Given $\mathfrak{q} \in \mathbf{D}(f)$, let S be the image of $R - \mathfrak{q}$ in R_f. Then **(12.5)** yields $P_{\mathfrak{q}} = S^{-1}(P_f)$. Hence $P_{\mathfrak{q}}$ is 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, **(12.24)**(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 **(13.43)** with R_h for R. Thus (4) holds. □

EXERCISE **(13.52)**. — 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 $\mathfrak{m}$.

EXERCISE **(13.53)**. — Let A be a semilocal ring, P a locally free module of rank n. Show that P is free of rank n.

EXERCISE **(13.54)**. — Let R be a ring, M a finitely presented module, $n \ge 0$. Show that M is locally free of rank n if and only if $F_{n-1}(M) = \langle 0 \rangle$ and $F_n(M) = R$.

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 $n \ge 1$ 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 $n \ge 1$ and $a_i \in R$. Rewriting the equation, we obtain

$$y(y^{n-1} + \cdots + a_{n-1}) = -a_n.$$

Take n minimal. Then $a_n \ne 0$ as R' is a domain. So dividing by $-a_n y$, we obtain

$$1/y = (-1/a_n)(y^{n-1} + \cdots + a_{n-1}) \in R'.$$ □

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:

$$\begin{tikzcd} R' \arrow[r] & R'_{\mathfrak{p}} \\ R \arrow[u] \arrow[r] & R_{\mathfrak{p}} \arrow[u] \end{tikzcd}$$

Here $R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$ is injective by **(12.17)**(1), and the extension is integral by **(11.24)**.

Here $\mathfrak{p}'R'_{\mathfrak{p}}$ and $\mathfrak{q}'R'_{\mathfrak{p}}$ are nested primes of $R'_{\mathfrak{p}}$ by **(11.20)**(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 **(11.22)**. 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 2.30; 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 $1, x_1, x_1^2, \ldots$ form a free basis of R_1 over R' by **(10.25)** 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 with R normal, $\mathfrak{p} \subsetneqq \mathfrak{q}$ nested primes of R, and $\mathfrak{q}'$ a prime of R' lying over $\mathfrak{q}$. Then there is a prime $\mathfrak{p}'$ lying over $\mathfrak{p}$ and contained in $\mathfrak{q}'$.*

PROOF: First, let us show $\mathfrak{p}R'_{\mathfrak{q}'} \cap R = \mathfrak{p}$. Given $y \in \mathfrak{p}R'_{\mathfrak{q}'} \cap R$, 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 $R'' := R[x_1, \ldots, x_m]$. Then R'' is module finite by **(10.28)** 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 $K := \mathrm{Frac}(R)$. 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 $\mathrm{Frac}(R/\mathfrak{p})[X]$. 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

$$s^n + b_1 s^{n-1} + \cdots + b_n = 0 \quad \text{with} \quad b_i := a_i/y^i \in K. \tag{14.9.1}$$

Conversely, any such equation yields one of the same degree for x as $y \in R \subset K$. So **(14.9.1)** is the minimal polynomial of s over K. So all b_i are in R by **(14.8)**.

Suppose $y \notin \mathfrak{p}$. Then $b_i \in \mathfrak{p}$ as $a_i = b_i y^i \in \mathfrak{p}$. 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 **(3.13)**. Then p'' lies in $\mathfrak{q}'R'_{\mathfrak{q}'}$ as it is the only maximal ideal. Set $\mathfrak{p}' := \mathfrak{p}'' \cap R'$. Then $\mathfrak{p}' \cap R = \mathfrak{p}$, and $\mathfrak{p}' \subset \mathfrak{q}'$ by **(11.20)**(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 **(11.20)**(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 Algebras). — *Let R be a ring, R' a flat algebra, $\mathfrak{p} \subsetneqq \mathfrak{q}$ nested primes of R, and $\mathfrak{q}'$ a prime of R' lying over $\mathfrak{q}$. Then there is a prime $\mathfrak{p}'$ lying over $\mathfrak{p}$ and contained in $\mathfrak{q}'$.*

PROOF: The canonical map $R_{\mathfrak{q}} \to R'_{\mathfrak{q}'}$ is faithfully flat by **(13.47)**. Therefore, $\mathrm{Spec}(R'_{\mathfrak{q}'}) \to \mathrm{Spec}(R_{\mathfrak{q}})$ is surjective by **(13.14)**. Thus **(11.20)** yields the desired $\mathfrak{p}'$.

Alternatively, $R' \otimes_R (R/\mathfrak{p})$ is flat over $R/\mathfrak{p}$ by **(9.11)**. Also, $R'/\mathfrak{p}R' = R' \otimes_R R/\mathfrak{p}$ by **(8.16)**(1). Hence, owing to **(1.9)**, 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 **(3.14)**, $\mathfrak{q}'$ 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 $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$ and that $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ 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) $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$, and $R_{\mathfrak{p}}\, \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$.
(3) $K/\mathfrak{p}K = \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$, and $K = \prod_{\mathfrak{p} \in \Sigma} K/\mathfrak{p}K$.

Exercise **(14.14)**. — Let A be a reduced local ring with residue field k and finite set Σ of minimal primes. For each $\mathfrak{p} \in \Sigma$, set $K(\mathfrak{p}) := \mathrm{Frac}(A/\mathfrak{p})$. Let P be a finitely generated module. Show that P is free of rank r if and only if $\dim_k(P \otimes_A k) = r$ and $\dim_{K(\mathfrak{p})}(P \otimes_A K(\mathfrak{p})) = r$ for each $\mathfrak{p} \in \Sigma$.

Exercise **(14.15)**. — Let A be a reduced local ring with residue field k and a finite set of minimal primes. Let P be a finitely generated module, B an A-algebra with $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ surjective. Show that P is a free A-module of rank r if and only if $P \otimes B$ is a free B-module of rank r.

(14.16) (*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 **(10.30)**, owing to **(11.32)**.

Exercise **(14.17)**. — Let R be a ring, $\mathfrak{p}_1 \dots, \mathfrak{p}_r$ 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 $\mathfrak{a}'_0 := \mathrm{Ker}\,\varphi$ 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 **(1.10)**, 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 **(10.28)** yields (1).

Further, by the theory of transcendence bases [**2**, (8.3), p. 526], [**10**, 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 $x' \in R \cap \mathrm{Frac}(P)$. Also, $R \cap \mathrm{Frac}(P) = P$, for P is normal by **(10.34)** 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 $P[x_1] = R$. Now, say $t_1 = H_d + \cdots + H_0$ where $H_d \neq 0$ and where H_i is **homogeneous of degree** i in $x_1, \ldots, x_n$; that is, H_i is a linear combination of monomials of degree i. Then $d > 0$ as $t_1 \notin k$. As k is infinite, **(3.20)** yields $a_i \in k$ with $H_d(a_1, a_2, \ldots, a_n) \neq 0$. Since H_d is homogeneous, $a_i \neq 0$ for some i; reordering the x_i, we may assume $a_1 \neq 0$. Again since H_d is homogeneous, we may replace a_i by a_i/a_1. Then $H_d(1, a_2, \ldots, a_n) \neq 0$. But $H_d(1, a_2, \ldots, a_n)$ is the coefficient of x_1^d in $H_d(x_1, t_2 + a_2x_1, \ldots, t_n + a_nx_1)$. So after we collect like powers of x_1, the equation

$$H_d(x_1, t_2 + a_2x_1, \ldots, t_n + a_nx_1) + \cdots + H_0(x_1, t_2 + a_2x_1, \ldots, t_n + a_nx_1) + t_1 = 0$$

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_1R. 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 **(10.27)**. 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 **(10.27)**. 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 $f := X^qY - XY^q$ 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 $a = 0$.

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)** (Zariski Nullstellensatz). — *Let k be a field, R an algebra-finite extension. Assume R is a field. Then R/k is finite.*

Proof: By the Noether Normalization Lemma **(15.1)**, R is module finite over a polynomial subring $P := k[t_1, \ldots, t_\nu]$. Then R/P is integral by **(10.23)**. As R is a field, so is P by **(14.1)**. Hence $\nu = 0$. So $P = k$. Thus R/k is finite, as asserted.

Alternatively, here's a short proof, not using **(15.1)**. Say $R = k[x_1, \ldots, x_n]$. Set $P := k[x_1]$ and $K := \mathrm{Frac}(P)$. Then $R = K[x_2, \ldots, x_n]$. By induction on n, assume R/K is finite. Suppose x_1 is transcendental over k, so P is a polynomial ring.

Note $R = P[x_2, \ldots, x_n]$. Hence **(11.26)** yields $f \in P$ with R_f/P_f module finite, so integral by **(10.28)**. But $R_f = R$. Thus P_f is a field by **(14.1)**. So $f \notin k$.

Set $g := 1 + f$. Then $1/g \in P_f$. So $1/g = h/f^r$ for some $h \in P$ and $r \geq 1$. Then $f^r = gh$. But f and g are relatively prime, a contradiction. Thus x_1 is algebraic over k. Hence $P = K$, and K/k is finite. But R/K is finite. Thus R/k is too. □

Corollary **(15.5)**. — *Let k be a field, $R := k[x_1, \ldots, x_n]$ an algebra-finite extension, and $\mathfrak{m}$ a maximal ideal of R. Assume k is algebraically closed. Then there are $a_1, \ldots, a_n \in k$ such that $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.*

Proof: Set $K := R/\mathfrak{m}$. Then K is a finite extension field of k by the Zariski Nullstellensatz **(15.4)**. But k is algebraically closed. Hence $k = K$. Let $a_i \in k$ be the residue of x_i, and set $\mathfrak{n} := \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Then $\mathfrak{n} \subset \mathfrak{m}$.

Let $R' := k[X_1, \ldots, X_n]$ be the polynomial ring, and $\varphi\colon R' \to R$ the k-algebra map with $\varphi X_i := x_i$. Set $\mathfrak{n}' := \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Then $\varphi(\mathfrak{n}') = \mathfrak{n}$. But $\mathfrak{n}'$ is maximal by **(2.21)**. So $\mathfrak{n}$ is maximal. Hence $\mathfrak{n} = \mathfrak{m}$, as desired. □

Corollary **(15.6)**. — *Let k be any field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, and $\mathfrak{m}$ a maximal ideal of P. Then $\mathfrak{m}$ is generated by n elements.*

Proof: Set $K := P/\mathfrak{m}$. Then K is a field. So K/k is finite by **(15.4)**.

Induct on n. If $n = 0$, then $\mathfrak{m} = 0$. Assume $n \geq 1$. Set $R := k[X_1]$ and $\mathfrak{p} := \mathfrak{m} \cap R$. Then $\mathfrak{p} = \langle f_1 \rangle$ for some $f_1 \in R$ as R is a PID. Set $k_1 := R/\mathfrak{p}$. Then k_1 is isomorphic to the image of R in K. But K is a finite-dimensional k-vector space. So k_1 is too. So $k \subset k_1$ is an integral extension by **(10.23)**. Since k is a field, so is k_1 by **(14.1)**.

Note $P/\mathfrak{p}P = k_1[X_2, \ldots, X_n]$ by **(1.7)**. But $\mathfrak{m}/\mathfrak{p}$ is a maximal ideal. So by induction $\mathfrak{m}/\mathfrak{p}$ is generated by $n - 1$ elements, say the residues of $f_2, \ldots, f_n \in \mathfrak{m}$. Then $\mathfrak{m} = \langle f_1, \ldots, f_n \rangle$, as desired. □

Theorem **(15.7)** (Hilbert Nullstellensatz). — *Let k be a field, and R a finitely generated k-algebra. Let $\mathfrak{a}$ be a proper ideal of R. Then*

$$\sqrt{\mathfrak{a}} = \bigcap\nolimits_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$$

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 **(2.30)**. 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 **(11.13)**. 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 **(10.23)**. 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 **(15.8)**. — Let k be a field, K an algebraically closed extension field. (So K contains a copy of every finite extension field.) Let $P := k[X_1, \ldots, X_n]$ be the polynomial ring, and $f, f_1, \ldots, f_r \in P$. Assume f vanishes at every zero in K^n of $f_1, \ldots, f_r$; in other words, if $(a) := (a_1, \ldots, a_n) \in K^n$ and $f_1(a) = 0, \ldots, f_r(a) = 0$, then $f(a) = 0$ too. Prove that there are polynomials $g_1, \ldots, g_r \in P$ and an integer N such that $f^N = g_1 f_1 + \cdots + g_r f_r$.

LEMMA **(15.9)**. — *Let k be a field, R a finitely generated k-algebra. Assume R is a domain. Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes. Set $K := \operatorname{Frac}(R)$ and $d := \operatorname{tr.deg}_k K$. Then $r \le d$, with equality if and only if the chain is* **maximal**, *that is, it is not a proper subchain of a longer chain.*

PROOF: By the Noether Normalization Lemma **(15.1)**, R is module finite over a polynomial subring $P := k[t_1, \ldots, t_\nu]$ such that $\mathfrak{p}_i \cap P = \langle t_1, \ldots, t_{h_i} \rangle$ for suitable h_i. Set $L := \operatorname{Frac}(P)$. Then $\nu = \operatorname{tr.deg}_k L$. But $P \subset R$ is an integral extension by **(10.23)**. So $L \subset K$ is algebraic. Hence $\nu = d$. Now, Incomparability **(14.3)**(2) yields $h_i < h_{i+1}$ for all i. Hence $r \le h_r$. But $h_r \le \nu$ and $\nu = d$. 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 $\mathfrak{p}_0 = \langle 0 \rangle$ 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 $h_r = \nu$.

Suppose there is an i such that $h_i + 1 < h_{i+1}$. Then

$$(\mathfrak{p}_i \cap P) \subsetneqq \langle t_1, \ldots, t_{h_i+1} \rangle \subsetneqq (\mathfrak{p}_{i+1} \cap P).$$

Now, $P/(\mathfrak{p}_i \cap P)$ is, by **(1.10)**, equal to $k[t_{h_i+1}, \ldots, t_\nu]$; the latter is a polynomial ring, so normal by **(10.34)**(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 $\mathfrak{p} \cap P = \langle t_1, \ldots, t_{h_i+1} \rangle$. 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 $h_r = \nu$ and $\nu = d$. Thus $r = d$, as desired. □

(15.10) (*Krull Dimension*). — Given a ring R, its (Krull) **dimension** $\dim(R)$ is the supremum of the **lengths** r of all strictly ascending chains of primes:

$$\dim(R) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \text{ in } R \,\}.$$

For example, if R is a field, then $\dim(R) = 0$; more generally, $\dim(R) = 0$ if and only if every minimal prime is maximal. If R is a PID, but not a field, then $\dim(R) = 1$, as every nonzero prime is maximal by **(2.25)**.

EXERCISE **(15.11)**. — Let R be a domain of (finite) dimension r, and $\mathfrak{p}$ a nonzero prime. Prove that $\dim(R/\mathfrak{p}) < r$.

EXERCISE **(15.12)**. — Let R'/R be an integral extension of rings. Prove that $\dim(R) = \dim(R')$.

THEOREM **(15.13)**. — *Let k be a field, R a finitely generated k-algebra. If R is a domain, then $\dim(R) = \operatorname{tr.deg}_k(\operatorname{Frac}(R))$.*

PROOF: The assertion is an immediate consequence of **(15.9)**. □

THEOREM **(15.14)**. — *Let k be a field, R a finitely generated k-algebra, $\mathfrak{p}$ a prime ideal, and $\mathfrak{m}$ a maximal ideal. Suppose R is a domain. Then*

$$\dim(R_\mathfrak{p}) + \dim(R/\mathfrak{p}) = \dim(R) \quad \textit{and} \quad \dim(R_\mathfrak{m}) = \dim(R).$$

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 **(11.20)** and to **(1.9)** and **(2.7)**; conversely, every such pair arises from a unique chain in R through $\mathfrak{p}$. But by **(15.9)**, every maximal strictly ascending chain through $\mathfrak{p}$ is of length $\dim(R)$. The first equation follows.

Clearly $\dim(R/\mathfrak{m}) = 0$, and so $\dim(R_\mathfrak{p}) = \dim(R)$. □

DEFINITION **(15.15)**. — We call a ring **catenary** if, given any two nested primes, all maximal chains of primes between the two have the same (finite) length.

THEOREM **(15.16)**. — *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 **(15.14)** shows that any maximal chain of primes $\langle 0 \rangle \subsetneqq \cdots \subsetneqq \mathfrak{p}$ is of length $\dim(R) - \dim(R/\mathfrak{p})$. □

EXERCISE **(15.17)**. — 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 **(15.18)**. — 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 $\dim(R_f)$.

EXERCISE **(15.19)**. — Let R be a ring, $R[X]$ the polynomial ring. Prove

$$1 + \dim(R) \le \dim(R[X]) \le 1 + 2\dim(R).$$

(In particular, $\dim(R[X]) = \infty$ if and only if $\dim(R) = \infty$.)

15. Appendix: Jacobson Rings

(15.20) (*Jacobson Rings*). — We call a ring R **Jacobson** if, given any ideal $\mathfrak{a}$, its radical is equal to the intersection of all maximal ideals containing it; that is,

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m}\supset\mathfrak{a}} \mathfrak{m}. \qquad \textbf{(15.20.1)}$$

Plainly, the nilradical of a Jacobson ring is equal to its Jacobson radical. Also, any quotient ring of a Jacobson ring is Jacobson too. In fact, a ring is Jacobson if and only if the the nilradical of every quotient ring is equal to its Jacobson radical.

In general, the right-hand side of **(15.20.1)** contains the left. So **(15.20.1)** holds if and only if every f outside $\sqrt{\mathfrak{a}}$ lies outside some maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.

Recall the Scheinnullstellensatz, **(3.29)**: 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 $\mathfrak{p} = \bigcap_{\mathfrak{m}\supset\mathfrak{p}} \mathfrak{m}$ for every prime $\mathfrak{p}$.

For example, a field k is Jacobson; in fact, a local ring A is Jacobson if and only if its maximal ideal is its only prime. Further, a Boolean ring B is Jacobson, as every prime is maximal by **(2.16)**, and so trivially $\mathfrak{p} = \bigcap_{\mathfrak{m}\supset\mathfrak{p}} \mathfrak{m}$ for every prime $\mathfrak{p}$. Finally, owing to **(15.10)** and **(2.6)** and the next lemma, a PID is Jacobson.

Lemma **(15.21)**. — *Let R be a 1-dimensional domain, $\{\mathfrak{m}_\lambda\}_{\lambda\in\Lambda}$ its set of maximal ideals. Assume every nonzero element lies in only finitely many $\mathfrak{m}_\lambda$. Then R is Jacobson if and only if Λ is infinite.*

Proof: If Λ is finite, take a nonzero $x_\lambda \in \mathfrak{m}_\lambda$ for each λ, and 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 Λ is infinite, then $\bigcap \mathfrak{m}_\lambda = \langle 0\rangle$ by hypothesis. But every nonzero prime is maximal as R is 1-dimensional. Thus $\mathfrak{p} = \bigcap_{\mathfrak{m}_\lambda\supset\mathfrak{p}} \mathfrak{m}_\lambda$ for every prime $\mathfrak{p}$. □

Proposition **(15.22)**. — *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 **(11.20)**.

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 **(12.22)** 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 hypothesis. Thus R is Jacobson. □

Exercise **(15.23)**. — Let X be a topological space. We say a subset Y is **locally closed** if Y is the intersection of an open set and a closed set; equivalently, Y is open in its closure $\overline{Y}$; equivalently, Y is closed in an open set containing it.

We say a subset X_0 of X is **very dense** if X_0 meets every nonempty locally closed subset Y. We say X is **Jacobson** if its set of closed points is very dense.

Show that the following conditions on a subset X_0 of X are equivalent:

(1) X_0 is very dense.
(2) Every closed set F of X satisfies $\overline{F \cap X_0} = F$.
(3) The map $U \mapsto U \cap X_0$ from the open sets of X to those of X_0 is bijective.

Exercise **(15.24)**. — Let R be a ring, $X := \operatorname{Spec}(R)$, and X_0 the set of closed points of X. Show that the following conditions are equivalent:

(1) R is a Jacobson ring.
(2) X is a Jacobson space.
(3) If $y \in X$ is a point such that $\{y\}$ is locally closed, then $y \in X_0$.

Lemma **(15.25)**. — *Let $R \subset R'$ be domains. Assume that $R' = R[x]$ for some $x \in R'$ and that there is $y \in R'$ with R'_y a field. Then there is $z \in R$ with R_z a field and x algebraic over R_z. Further, if R is Jacobson, then R and R' are fields.*

Proof: Set $Q := \operatorname{Frac}(R)$. Then $Q \subset R'_y$, so $R'_y = R[x]_y \subset Q[x]_y \subset R'_y$. Hence $Q[x]_y = R'_y$. So $Q[x]_y$ is a field. Now, if x is transcendental over Q, then $Q[x]$ is a polynomial ring, so Jacobson by **(15.20)**; whence, $Q[x]_y$ is not a field by **(15.22)**, a contradiction. Thus x is algebraic over Q. Hence y is algebraic over Q too.

Let $a_0x^n + \cdots + a_n = 0$ and $b_0y^m + \cdots + b_m = 0$ be equations of minimal degree with $a_i, b_j \in R$. Set $z := a_0b_m$. Then $z \neq 0$. Further,

$$1/y = -a_0(b_0y^{m-1} + \cdots + b_{m-1})/z \in R_z[x].$$

Hence $R[x]_y \subset R_z[x] \subset R'_y$. So $R_z[x] = R'_y$. Therefore $R_z[x]$ is a field too. But $x^n + (a_1b_m/z)x^{n-1} + \cdots + (a_nb_m/z) = 0$, so is an equation of integral dependence of x on R_z. So $R_z[x]$ is integral over R_z **(10.28)** . Hence R_z is a field by **(14.1)**.

Further, if R is Jacobson, then $\langle 0\rangle$ is a maximal ideal by **(15.22)**, and so R is a field. Hence $R = R_z$. Thus R' is a field by **(14.1)**. □

Theorem **(15.26)** (Generalized Hilbert Nullstellensatz). — *Let R be a Jacobson ring, R' a finitely generated algebra, and $\mathfrak{m}'$ a maximal ideal of R'. Set $\mathfrak{m} := \mathfrak{m}' \cap R$. Then* (1) *$\mathfrak{m}$ is maximal, and $R'/\mathfrak{m}'$ is algebraic over $R/\mathfrak{m}$, and* (2) *R' is Jacobson.*

Proof: First, assume $R' = R[x]$ for some $x \in R'$. Given a prime $\mathfrak{q} \subset R'$ and a $y \in R' - \mathfrak{q}$, set $\mathfrak{p} := \mathfrak{q} \cap R$ and $R_1 := R/\mathfrak{p}$ and $R'_1 := R'/\mathfrak{q}$. Then R is Jacobson by **(15.20)**. Suppose $(R'_1)_y$ is a field. Then by **(15.25)**, $R_1 \subset R'_1$ is a finite extension of fields. Thus $\mathfrak{q}$ and $\mathfrak{p}$ are maximal. To obtain (1), simply take $\mathfrak{q} := \mathfrak{m}$ and $y := 1$. To obtain (2), take $\mathfrak{q}$ nonmaximal, so R'_1 is not a field; conclude $(R'_1)_y$ is not a field; whence, **(15.22)** yields (2).

Second, assume $R' = R[x_1, \ldots, x_n]$ with $n \geq 2$. Set $R'' := R[x_1, \ldots, x_{n-1}]$ and $\mathfrak{m}'' := \mathfrak{m}' \cap R''$. Then $R' = R''[x_n]$. By induction on n, we may assume (1) and (2) hold for R''/R. So the first case for R'/R'' yields (2) for R'; by the same token, $\mathfrak{m}''$ is maximal, and $R'/\mathfrak{m}'$ is algebraic over $R''/\mathfrak{m}''$. Hence, $\mathfrak{m}$ is maximal, and $R''/\mathfrak{m}''$ is algebraic over $R/\mathfrak{m}$ by (1) for R''/R. Finally, the Tower Law **(10.27)** implies that $R'/\mathfrak{m}'$ is algebraic over $R/\mathfrak{m}$, as desired. □

Example **(15.27)**. — Part (1) of **(15.26)** may fail if R is not Jacobson, even if $R' := R[Y]$ is the polynomial ring in one variable Y over R. For example, let k be a field, and $R := k[[X]]$ the formal power series ring. According to **(3.11)**, the ideal $\mathfrak{M} := \langle 1 - XY\rangle$ is maximal, but $\mathfrak{M} \cap R$ is $\langle 0\rangle$, not $\langle X\rangle$.

Exercise **(15.28)**. — Let $P := \mathbb{Z}[X_1, \ldots, X_n]$ be the polynomial ring. Assume $f \in P$ vanishes at every zero in K^n of $f_1, \ldots, f_r \in P$ for every finite field K; that is, if $(a) := (a_1, \ldots, a_n) \in K^n$ and $f_1(a) = 0, \ldots, f_r(a) = 0$ in K, then $f(a) = 0$ too. Prove there are $g_1, \ldots, g_r \in P$ and $N \geq 1$ such that $f^N = g_1f_1 + \cdots + g_rf_r$.

Exercise **(15.29)**. — Let R be a ring, R' an algebra. Prove that if R' is integral over R and R is Jacobson, then R' is Jacobson.

Exercise **(15.30)**. — Let R be a Jacobson ring, S a multiplicative subset, $f \in R$. True or false: prove or give a counterexample to each of the following statements.

(1) The localized ring R_f is Jacobson.
(2) The localized ring $S^{-1}R$ is Jacobson.
(3) The filtered direct limit $\varinjlim R_\lambda$ of Jacobson rings is Jacobson.
(4) In a filtered direct limit of rings R_λ, necessarily $\varinjlim \operatorname{rad}(R_\lambda) = \operatorname{rad}(\varinjlim R_\lambda)$.

Exercise **(15.31)**. — Let R be a reduced Jacobson ring with a finite set Σ of minimal primes, and P a finitely generated module. Show that P is locally free of rank r if and only if $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$ for any maximal ideal $\mathfrak{m}$.

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 nonempty set of ideals has a 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, it is equivalent for a module to be Noetherian, to be finitely generated, or to be finitely presented. Lastly, we study Artinian rings and modules; in them, by definition, every descending chain of ideals or of submodules, stabilizes.

(16.1) (*Noetherian rings*). — We call a ring **Noetherian** if every ideal is finitely generated. For example, a Principal Ideal Ring (PIR) is, trivially, Noetherian.

Here are two standard examples of non-Noetherian rings. A third is given below in **(16.6)**, and a fourth later in **(18.31)**.

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 $\mathfrak{a}$:

$$R := \big\{ f := a + Xg \mid a \in k \text{ and } g \in k[X,Y] \big\} \text{ and}$$
$$\mathfrak{a} := \langle X,\, XY,\, XY^2, \dots \rangle.$$

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 M be a finitely generated module over an arbitrary ring. Show every set that generates M contains a finite subset that generates.

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 $j \ge 0$ 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 $j \ge 0$, 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 $x_1, \dots, x_r$. For each i, there is a j_i with $x_i \in \mathfrak{a}_{j_i}$. 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, x_λ for $\lambda \in \Lambda$ generators, $\mathcal{S}$ the set of ideals generated by finitely many x_λ. Let $\mathfrak{b}$ be a maximal element of $\mathcal{S}$; say $\mathfrak{b}$ is generated by $x_{\lambda_1}, \dots, x_{\lambda_m}$. Then $\mathfrak{b} \subset \mathfrak{b} + \langle x_\lambda \rangle$ for any λ. So by maximality, $\mathfrak{b} = \mathfrak{b} + \langle x_\lambda \rangle$. Hence $x_\lambda \in \mathfrak{b}$. 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:

$$R := k[X,\, Y,\, X/Y,\, X/Y^2,\, X/Y^3, \dots].$$

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 subset, $\mathfrak{a}$ 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 **(1.9)** and by **(11.20)**(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 **(11.19)**(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.

Exercise **(16.9)**. — Let $R \subset R'$ be a ring extension with an R-linear retraction $\rho\colon R' \to R$. Assume R' is Noetherian, and prove R is too.

Theorem **(16.10)** (Cohen). — *A ring R is Noetherian if every prime is finitely generated.*

Proof: 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 $\mathfrak{a}_\lambda$ as $\mathfrak{a}_\lambda = \mathfrak{a}$, 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 $x_1 + w_1 a, \dots, x_n + w_n a$ with $x_i \in \mathfrak{p}$. Then $\{x_1, \dots, x_n, a\}$ generate $\mathfrak{p} + \langle a \rangle$.

Set $\mathfrak{b} = \operatorname{Ann}\big((\mathfrak{p} + \langle a \rangle)/\mathfrak{p}\big)$. Then $\mathfrak{b} \supset \mathfrak{p} + \langle b \rangle$ and $b \notin \mathfrak{p}$. So $\mathfrak{b}$ is finitely generated, say by $y_1, \dots, y_m$. 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 $\{x_1, \dots, x_n, ay_1, \dots, ay_m\}$, a contradiction. Thus there are no non-finitely-generated ideals; in other words, R is Noetherian. □

Lemma **(16.11)**. — *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 $\mathfrak{a}_i := \langle f_1, \dots, f_i \rangle$. 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, $\mathfrak{b} = \langle a_1, \dots, a_n \rangle$ 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 **(16.12)** (Hilbert Basis). — *Let R be a Noetherian ring, R' a finitely generated algebra. Then R' is Noetherian.*

Proof: Say $x_1, \dots, x_r$ generate R' over R, and let $P := R[X_1, \dots, X_r]$ be the polynomial ring in r variables. Then P is Noetherian by **(16.11)** 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)**. □

(16.13) (*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 **(16.14)**. — *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 **(16.15)**. — 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 **(16.16)**. — *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 **(5.2)**.

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 **(16.14)**. Thus M is Noetherian. □

Corollary **(16.17)**. — *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 **(16.16)**(2) by induction on r. $\square$

Exercise **(16.18)**. — 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 **(16.19)**. — *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 **(16.17)** and by **(16.13)**. Hence K is finitely generated, so (3) holds; further, (1) holds by **(16.16)**(2). Trivially, (1) or (3) implies (2). $\square$

Exercise **(16.20)**. — Let R be a Noetherian ring, M and N finitely generated modules. Show that $\operatorname{Hom}(M, N)$ is finitely generated.

Lemma **(16.21)** (Artin–Tate [**1**, Thm. 1]). — *Let $R \subset R' \subset R''$ be rings. Assume that R is Noetherian, that R''/R is algebra finite, and that R''/R' either is module finite or is integral. Then R'/R is algebra finite.*

Proof: Since R''/R is algebra finite, so is R''/R'. Hence, the two conditions on R''/R' are equivalent by **(10.28)**.

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

$$x_i = \textstyle\sum_j z_{ij} y_j \quad \text{and} \quad y_i y_j = \textstyle\sum_k z_{ijk} y_k. \qquad \textbf{(16.21.1)}$$

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, **(16.12)**.

Any $x \in R''$ is a polynomial in the x_i with coefficients in R. So **(16.21.1)** implies x is a linear combination of the y_j with coefficients in R'_0. Thus R''/R'_0 is module finite. But R'_0 is a Noetherian ring, and R' is an R'_0-submodule of R''. So R'/R'_0 is module finite by **(16.16)**. Since R'_0/R is algebra finite, R'/R is too. $\square$

Theorem **(16.22)** (Noether on Invariants). — *Let R be a Noetherian ring, R' an algebra-finite extension, and G a finite group of R-automorphisms of R'. Then the subring of invariants R'^G is also algebra finite; in other words, every invariant can be expressed as a polynomial in a certain finite number of "fundamental" invariants.*

Proof: By **(10.22)**, R' is integral over R'^G. So **(16.21)** yields the assertion. $\square$

(16.23) (*Artin–Tate proof* [**1**, Thm. 2] *of the Zariski Nullstellensatz* **(15.4)**). — In the setup of **(15.4)**, take a transcendence base $x_1, \ldots, x_r$ of R/k. Then R is integral over $k(x_1, \ldots, x_r)$ by definition of transcendence basis [**2**, (8.3), p. 526]. So $k(x_1, \ldots, x_r)$ is algebra finite over k by **(16.21)**, say $k(x_1, \ldots, x_r)k[y_1, \ldots, y_s]$.

Suppose $r \geq 1$. Write $y_i = F_i/G_i$ with $F_i, G_i \in k[x_1, \ldots, x_r]$. Let H be an irreducible factor of $G_1 \cdots G_s + 1$. Plainly $H \nmid G_i$ for all i.

Say $H^{-1} = P(y_1, \ldots, y_s)$ where P is a polynomial. Then $H^{-1} = Q/(G_1 \cdots G_s)^m$ for some $Q \in k[x_1, \ldots, x_r]$ and $m \geq 1$. But $H \nmid G_i$ for all i, a contradiction. Thus $r = 0$. So **(10.28)** implies R/k is module finite, as desired.

Exercise **(16.24)**. — Let R be a domain, R' an algebra, and set $K := \operatorname{Frac}(R)$. Assume R is Noetherian.

(1) [**1**, Thm. 3] Assume R' is a field containing R. Show R'/R is algebra finite if and only if K/R is algebra finite and R'/K is (module) finite.

(2) [**1**, bot. p. 77] Let $K' \supset R$ be a field that embeds in R'. Assume R'/R is algebra finite. Show K/R is algebra finite and K'/K is finite.

Example **(16.25)**. — Set $\delta := \sqrt{-5}$, set $R := \mathbb{Z}[\delta]$, and set $\mathfrak{p} := \langle 2, 1+\delta \rangle$. 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 **(13.51)** do not imply that P is free.

Since $\mathbb{Z}$ is Noetherian and since R is generated over $\mathbb{Z}$, the Hilbert Basis Theorem **(16.12)** yields that R is Noetherian. So since $\mathfrak{p}$ is generated by two elements, **(16.19)** yields that $\mathfrak{p}$ is finitely presented.

Recall from [**2**, 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 **(11.14)**(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 $S^{-1}\mathfrak{p} \xrightarrow{\sim} K$, 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 **(16.26)**. — We say a module is **Artinian** or the **descending chain condition** (dcc) is satisfied 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 a module if every nonempty set of submodules has a minimal member.

Proposition **(16.27)**. — *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 **(16.16)**(2), and the proof of **(16.17)**. $\square$

Exercise **(16.28)**. — 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 **(16.29)**. — 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 **(16.30)**. — 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 $\mathfrak{p} = \mathrm{Ann}(m)$. The set of associated primes is denoted by $\mathrm{Ass}(M)$ or $\mathrm{Ass}_R(M)$.

The primes that are minimal in $\mathrm{Ass}(M)$ 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 $\mathfrak{p} \in \mathrm{Ass}(M)$ if and only if there is an R-injection $R/\mathfrak{p} \hookrightarrow M$.*

Proof: Assume $\mathfrak{p} = \mathrm{Ann}(m)$ 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 $\mathfrak{p} = \mathrm{Ann}(m)$, so $\mathfrak{p} \in \mathrm{Ass}(M)$. □

Proposition **(17.3)**. — *Let M be a module. Then* $\mathrm{Ass}(M) \subset \mathrm{Supp}(M)$.

Proof: Let $\mathfrak{p} \in \mathrm{Ass}_R(M)$. Say $\mathfrak{p} = \mathrm{Ann}(m)$. Then $m/1 \in M_\mathfrak{p}$ is nonzero as no $x \in (R - \mathfrak{p})$ satisfies $xm = 0$. Thus $M_\mathfrak{p} \neq 0$ and so $\mathfrak{p} \in \mathrm{Supp}(M)$.

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 **(12.20)**. But $(R/\mathfrak{p})_\mathfrak{p} = \mathrm{Frac}(R/\mathfrak{p})$ by **(12.23)**. Thus $M_\mathfrak{p} \neq 0$. □

Lemma **(17.4)**. — *Let R be a ring, $\mathfrak{p}$ a prime ideal, $m \in R/\mathfrak{p}$ a nonzero element. Then* (1) $\mathrm{Ann}(m) = \mathfrak{p}$ *and* (2) $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

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*

$$\mathrm{Ass}(N) \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N).$$

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 $\mathrm{Ass}(N) \subset \mathrm{Ass}(M)$.

Let $\mathfrak{p} \in \mathrm{Ass}(M)$. 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, $\mathfrak{p} \in \mathrm{Ass}(M/N)$ by **(17.2)**. Else, take a nonzero $m \in E \cap N$. Then $\mathrm{Ann}(m) = \mathfrak{p}$ by **(17.4)**(1). Thus $\mathfrak{p} \in \mathrm{Ass}(N)$. □

Exercise **(17.6)**. — Given modules $M_1, \ldots, M_r$, set $M := M_1 \oplus \cdots \oplus M_r$. Prove

$$\mathrm{Ass}(M) = \mathrm{Ass}(M_1) \cup \cdots \cup \mathrm{Ass}(M_r).$$

Exercise **(17.7)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 2\rangle \oplus \mathbb{Z}$. Find $\mathrm{Ass}(M)$ and find two submodules $L, N \subset M$ with $L + N = M$ but $\mathrm{Ass}(L) \cup \mathrm{Ass}(N) \subsetneqq \mathrm{Ass}(M)$.

Exercise **(17.8)**. — If a prime $\mathfrak{p}$ is sandwiched between two primes in $\mathrm{Ass}(M)$, is $\mathfrak{p}$ necessarily in $\mathrm{Ass}(M)$ too?

Proposition **(17.9)**. — *Let M be a module, and Ψ a subset of $\mathrm{Ass}(M)$. Then there is a submodule N of M with $\mathrm{Ass}(M/N) = \Psi$ and $\mathrm{Ass}(N) = \mathrm{Ass}(M) - \Psi$.*

Proof: Given submodules N_λ of M totally ordered by inclusion, set $N := \bigcup N_\lambda$. Given $\mathfrak{p} \in \mathrm{Ass}(N)$, say $\mathfrak{p} = \mathrm{Ann}(m)$. Then $m \in N_\lambda$ for some λ; so $\mathfrak{p} \in \mathrm{Ass}(N_\lambda)$. Conversely, $\mathrm{Ass}(N_\lambda) \subset \mathrm{Ass}(N)$ for all λ by **(17.5)**. Thus $\mathrm{Ass}(N) = \bigcup \mathrm{Ass}(N_\lambda)$.

So we may apply Zorn's Lemma to obtain a submodule N of M that is maximal with $\mathrm{Ass}(N) \subset \mathrm{Ass}(M) - \Psi$. By **(17.5)**, it suffices to show that $\mathrm{Ass}(M/N) \subset \Psi$.

Take $\mathfrak{p} \in \mathrm{Ass}(M/N)$. Then M/N has a submodule N'/N isomorphic to $R/\mathfrak{p}$ by **(17.2)**. So $\mathrm{Ass}(N') \subset \mathrm{Ass}(N) \cup \{\mathfrak{p}\}$ by **(17.5)** and **(17.4)**(2). Now, $N' \supsetneqq N$ and N is maximal with $\mathrm{Ass}(N) \subset \mathrm{Ass}(M) - \Psi$. Hence $\mathfrak{p} \in \mathrm{Ass}(N') \subset \mathrm{Ass}(M)$, but $\mathfrak{p} \notin \mathrm{Ass}(M) - \Psi$. Thus $\mathfrak{p} \in \Psi$. □

Proposition **(17.10)**. — *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 $\mathfrak{p} \in \mathrm{Ass}(M)$, then $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$; the converse holds if $\mathfrak{p}$ is finitely generated.*

Proof: Assume $\mathfrak{p} \in \mathrm{Ass}(M)$. 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 **(12.20)**. But $S^{-1}(R/\mathfrak{p}) = S^{-1}R/S^{-1}\mathfrak{p}$ by **(12.22)**. Assume $\mathfrak{p} \cap S = \emptyset$ also. Then $\mathfrak{p}S^{-1}R$ is prime by **(11.19)**(3)(b). But $\mathfrak{p}S^{-1}R = S^{-1}\mathfrak{p}$ by **(12.2)**. Thus $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$.

Conversely, assume $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$. Then there are $m \in M$ and $t \in S$ with $S^{-1}\mathfrak{p} = \mathrm{Ann}(m/t)$. Say $\mathfrak{p} = \langle x_1, \ldots, x_n\rangle$. 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 $x_i \in \mathrm{Ann}(sm)$. Thus $\mathfrak{p} \subset \mathrm{Ann}(sm)$.

Take $b \in \mathrm{Ann}(sm)$. Then $bsm/st = 0$. So $b/1 \in S^{-1}\mathfrak{p}$. So $b \in \mathfrak{p}$ by **(11.19)**(1)(a) and **(11.19)**(3)(a). Thus $\mathfrak{p} \supset \mathrm{Ann}(sm)$. So $\mathfrak{p} = \mathrm{Ann}(sm)$. Thus $\mathfrak{p} \in \mathrm{Ass}(M)$.

Finally, $\mathfrak{p} \cap S = \emptyset$ by **(11.20)**(2), as $S^{-1}\mathfrak{p}$ is prime. □

Exercise **(17.11)**. — 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 **(17.12)**. — *Let R be a ring, M a module, and $\mathfrak{p}$ an ideal. Suppose $\mathfrak{p}$ is maximal in the set of annihilators of nonzero elements m of M. Then $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Proof: Say $\mathfrak{p} := \mathrm{Ann}(m)$ with $m \neq 0$. Then $1 \notin \mathfrak{p}$ as $m \neq 0$. Now, take $b, c \in R$ with $bc \in \mathfrak{p}$, but $c \notin \mathfrak{p}$. Then $bcm = 0$, but $cm \neq 0$. Plainly, $\mathfrak{p} \subset \mathrm{Ann}(cm)$. So $\mathfrak{p} = \mathrm{Ann}(cm)$ by maximality. But $b \in \mathrm{Ann}(cm)$, so $b \in \mathfrak{p}$. Thus $\mathfrak{p}$ is prime. □

Proposition **(17.13)**. — *Let R be a Noetherian ring, M a module. Then $M = 0$ if and only if $\mathrm{Ass}(M) = \emptyset$.*

Proof: Obviously, if $M = 0$, then $\mathrm{Ass}(M) = \emptyset$. 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 $\mathfrak{p}$ by **(16.5)**. By **(17.12)**, $\mathfrak{p} \in \mathrm{Ass}(M)$. Thus $\mathrm{Ass}(M) \neq \emptyset$. □

Definition **(17.14)**. — 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 $\mathrm{z.div}(M)$.

Proposition **(17.15)**. — *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 **(17.12)**. Thus $\mathrm{z.div}(M) \subset \bigcup \mathfrak{p}$. The opposite inclusion results from the definitions. □

Exercise **(17.16)**. — 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 **(17.17)**. — *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 **(17.13)**. 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 **(11.20)**(2) and **(17.10)**. 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 **(17.18)**. — *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 **(17.17)**, $\mathfrak{q}$ exists. Also, $\mathfrak{q} \in \mathrm{Supp}(M)$; so $\mathfrak{q} = \mathfrak{p}$ if $\mathfrak{p}$ is minimal. □

Theorem **(17.19)**. — *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 **(13.29)**. 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 **(17.17)**. The assertion follows. □

Lemma **(17.20)**. — *Let R be a Noetherian ring, M a finitely generated module. Then there exists a chain of submodules*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$$

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,

$$\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \mathrm{Supp}(M). \qquad \textbf{(17.20.1)}$$

Proof: Among all submodules of M having such a chain, there is a maximal submodule N by **(16.19)** and **(16.13)**. Suppose $M/N \neq 0$. Then by **(17.13)**, 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 **(17.20.1)** follows by induction from **(17.5)** and **(17.4)**(2). Now, $\mathfrak{p}_i \in \mathrm{Supp}(R/\mathfrak{p}_i)$ owing to **(12.23)**. Thus **(13.27)**(1) yields **(17.20.1)**. □

Theorem **(17.21)**. — *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 **(17.20)**. □

Exercise **(17.22)**. — 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 **(17.23)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}$ in **(17.20)**. Determine when a chain $0 \subset M_1 \subsetneqq M$ is acceptable, and show that then $\mathfrak{p}_2 \notin \mathrm{Ass}(M)$.

Exercise **(17.24)**. — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 12\rangle$ in **(17.20)**. Find all three acceptable chains, and show that, in each case, $\{\mathfrak{p}_i\} = \mathrm{Ass}(M)$.

Proposition **(17.25)**. — *Let R be a Noetherian ring, and M and N finitely generated modules. Then*

$$\mathrm{Ass}(\mathrm{Hom}(M,N)) = \mathrm{Supp}(M) \bigcap \mathrm{Ass}(N).$$

Proof: Take $\mathfrak{p} \in \mathrm{Ass}\big(\mathrm{Hom}(M,N)\big)$. Then **(17.2)** yields an injective R-map $R/\mathfrak{p} \hookrightarrow \mathrm{Hom}(M,N)$. Set $k(\mathfrak{p}) := \mathrm{Frac}(R/\mathfrak{p})$. Then $k(\mathfrak{p}) = (R/\mathfrak{p}R)_\mathfrak{p}$ by **(11.23)**. Now, M is finitely presented by **(16.19)** as R is Noetherian; hence,

$$\mathrm{Hom}(M,N)_\mathfrak{p} = \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \qquad \textbf{(17.25.1)}$$

by **(12.25)**(2). Therefore, by exactness, localizing yields an injection

$$\varphi\colon k(\mathfrak{p}) \hookrightarrow \mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}).$$

Thus $M_\mathfrak{p} \neq 0$; so $\mathfrak{p} \in \mathrm{Supp}(M)$.

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. But $k(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ by **(12.22)**. Hence by **(17.2)**, we have $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}(N_\mathfrak{p})$. Thus also $\mathfrak{p} \in \mathrm{Ass}(N)$ by **(17.10)**.

Conversely, take $\mathfrak{p} \in \mathrm{Supp}(M) \cap \mathrm{Ass}(N)$. 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 $k(\mathfrak{p}) \hookrightarrow N_\mathfrak{p}$; the latter exists by **(17.2)** and **(17.10)** since $\mathfrak{p} \in \mathrm{Ass}(N)$. We obtain a nonzero element of $\mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$, annihilated by $\mathfrak{p}R_\mathfrak{p}$. But $\mathfrak{p}R_\mathfrak{p}$ is maximal, so is the entire annihilator. So $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}\big(\mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})\big)$. Hence $\mathfrak{p} \in \mathrm{Ass}\big(\mathrm{Hom}(M,N)\big)$ by **(17.25.1)** and **(17.10)**. □

Exercise **(17.26)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Show that the following conditions are equivalent:

(1) $\mathbf{V}(\mathfrak{a}) \cap \mathrm{Ass}(M) = \emptyset$;
(2) $\mathrm{Hom}(N, M) = 0$ for all finitely generated modules N with $\mathrm{Supp}(N) \subset \mathbf{V}(\mathfrak{a})$;
(3) $\mathrm{Hom}(N, M) = 0$ for some finitely generated module N with $\mathrm{Supp}(N) = \mathbf{V}(\mathfrak{a})$;
(4) $\mathfrak{a} \not\subset \mathrm{z.div}(M)$; that is, there is a nonzerodivisor x on M in $\mathfrak{a}$;
(5) $\mathfrak{a} \not\subset \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Ass}(M)$.

Proposition **(17.27)**. — *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 $\mathfrak{p} \in \mathrm{Ass}(M/xM)$ if and only if $\mathfrak{p} \in \mathrm{Ass}(M/yM)$.*

Proof: Form the sequence $0 \to K \to M/xM \xrightarrow{\mu_y} M/xM$ with $K := \mathrm{Ker}(\mu_y)$. Apply the functor $\mathrm{Hom}(R/\mathfrak{p}, \bullet)$ to that sequence, and get the following one:

$$0 \to \mathrm{Hom}(R/\mathfrak{p},\, K) \to \mathrm{Hom}(R/\mathfrak{p},\, M/xM) \xrightarrow{\mu_y} \mathrm{Hom}(R/\mathfrak{p},\, M/xM).$$

It is exact by **(5.18)**. But $y \in \mathfrak{p}$; so the right-hand map vanishes. Thus

$$\mathrm{Hom}(R/\mathfrak{p}, K) \xrightarrow{\sim} \mathrm{Hom}(R/\mathfrak{p},\, M/xM).$$

Form the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\mu_x"] \arrow[d, "\mu_y"'] & M \arrow[r] \arrow[d, "\mu_y"'] & M/xM \arrow[r] \arrow[d, "\mu_y"'] & 0 \\
0 \arrow[r] & M \arrow[r, "\mu_x"] & M \arrow[r] & M/xM \arrow[r] & 0
\end{tikzcd}$$

The Snake Lemma **(5.13)** yields an exact sequence $0 \to K \to M/yM \xrightarrow{\mu_x} M/yM$ as $\mathrm{Ker}(\mu_y) = 0$. Hence, similarly, $\mathrm{Hom}(R/\mathfrak{p},\, K) \xrightarrow{\sim} \mathrm{Hom}(R/\mathfrak{p},\, M/yM)$. Therefore,

$$\mathrm{Hom}(R/\mathfrak{p},\, M/yM) = \mathrm{Hom}(R/\mathfrak{p},\, M/xM). \qquad \textbf{(17.27.1)}$$

Finally, $\mathfrak{p} \in \mathrm{Supp}(R/\mathfrak{p})$ by **(13.27)**(3). Thus **(17.25)** 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 it cannot be shortened. 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 $\mathrm{Ass}(M/Q)$ 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 $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ 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 $\mathfrak{p} = \mathrm{nil}(M/Q)$.*

Proof: The assertion holds as $\mathrm{nil}(M/Q) = \bigcap_{\mathfrak{q}\in\mathrm{Ass}(M/Q)} \mathfrak{q}$ by **(17.19)**. □

Theorem **(18.4)**. — *Let R be a Noetherian ring, M a nonzero finitely generated module, Q a submodule. Set $\mathfrak{p} := \mathrm{nil}(M/Q)$. Then these conditions are equivalent:*

(1) *$\mathfrak{p}$ is prime and Q is $\mathfrak{p}$-primary.* (2) $\mathfrak{p} = \mathrm{z.div}(M/Q)$.
(3) *Given $x \in R$ and $m \in M$ with $xm \in Q$ but $m \notin Q$, necessarily $x \in \mathfrak{p}$.*

Proof: Recall $\mathfrak{p} = \bigcap_{\mathfrak{q}\in\mathrm{Ass}(M/Q)} \mathfrak{q}$ by **(17.19)**, and $\mathrm{z.div}(M/Q) = \bigcup_{\mathfrak{q}\in\mathrm{Ass}(M/Q)} \mathfrak{q}$ by **(17.15)**. Thus $\mathfrak{p} \subset \mathrm{z.div}(M/Q)$.

Further, (2) holds if $\mathrm{Ass}(M/Q) = \{\mathfrak{p}\}$, that is, if (1) holds.

Conversely, if $x \in \mathfrak{q} \in \mathrm{Ass}(M/Q)$, but $x \notin \mathfrak{q}' \in \mathrm{Ass}(M/Q)$, then $x \notin \mathfrak{p}$, but $x \in \mathrm{z.div}(M/Q)$; hence, (2) implies (1). Thus (1) and (2) are equivalent.

Clearly, (3) means every zerodivisor on M/Q is nilpotent, or $\mathfrak{p} \supset \mathrm{z.div}(M/Q)$. 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 $\mathfrak{q} = \mathrm{Ann}(R/\mathfrak{q})$. So $\mathfrak{p} = \mathrm{nil}(R/\mathfrak{q})$. 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 $\mathfrak{p} := \mathrm{nil}(M/Q)$. If $\mathfrak{p}$ is maximal, then Q is $\mathfrak{p}$-primary.*

Proof: Since $\mathfrak{p} = \bigcap_{\mathfrak{q}\in \mathrm{Ass}(M/Q)} \mathfrak{q}$ by **(17.19)**, if $\mathfrak{p}$ is maximal, then $\mathfrak{p} = \mathfrak{q}$ for any $\mathfrak{q} \in \mathrm{Ass}(M/Q)$, or $\{\mathfrak{p}\} = \mathrm{Ass}(M/Q)$, 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 $\mathfrak{p} = \mathrm{nil}(R/\mathfrak{q})$, 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 **(3.33)**. 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 **(17.13)** and **(17.5)** yield

$$\emptyset \neq \mathrm{Ass}(M/Q) \subset \mathrm{Ass}(M/Q_1) \cup \mathrm{Ass}(M/Q_2).$$

Since the latter two sets are each equal to $\{\mathfrak{p}\}$, so is $\mathrm{Ass}(M/Q)$, 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 hold:

(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 so, then we call Q_i the **$\mathfrak{p}_i$-primary component** of the decomposition.

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. Set $\mathfrak{a} := \langle X^2, XY\rangle$. Below, it is proved that, for any $n \geq 1$,

$$\mathfrak{a} = \langle X\rangle \cap \langle X^2, XY, Y^n\rangle = \langle X\rangle \cap \langle X^2, Y\rangle. \qquad \textbf{(18.14.1)}$$

Here $\langle X^2, XY, Y^n\rangle$ and $\langle X^2, Y\rangle$ contain $\langle X, Y\rangle^n$; so they are $\langle X, Y\rangle$-primary by **(18.11)**. Thus **(18.14.1)** gives infinitely many primary decompositions of $\mathfrak{a}$. They are clearly irredundant. Note: *the $\langle X, Y\rangle$-primary component is not unique!*

Plainly, $\mathfrak{a} \subset \langle X\rangle$ and $\mathfrak{a} \subset \langle X^2, XY, Y^n\rangle \subset \langle X^2, Y\rangle$. 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, $R := k[X,Y]$ the polynomial ring, $a \in k$. Set $\mathfrak{a} := \langle X^2, XY\rangle$. Define an automorphism α of R by $X \mapsto X$ and $Y \mapsto aX + Y$. Then α preserves $\mathfrak{a}$ and $\langle X\rangle$, and carries $\langle X^2, Y\rangle$ onto $\langle X^2, aX + Y\rangle$. So **(18.14)** implies that $\mathfrak{a} = \langle X\rangle \cap \langle X^2, aX + Y\rangle$ is an irredundant primary decomposition. Moreover, if $a \neq b$, then $\langle X^2, aX+Y, bX+Y\rangle = \langle X, Y\rangle$. Thus *two $\langle X, Y\rangle$-primary components are not always contained in a third, although their intersection is one by* **(18.12)**.

Example **(18.16)**. — 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. Moreover, $\langle x\rangle$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^2$.

Exercise **(18.17)**. — 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 **(18.18)**. — Let $R := R' \times R''$ be a product of two domains. Find an irredundant primary decomposition of $\langle 0\rangle$.

Lemma **(18.19)**. — *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 $i = 1, \ldots, r$. Then*

$$\mathrm{Ass}(M/N) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}. \qquad \textbf{(18.19.1)}$$

If equality holds and if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ 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 $\mathrm{Ass}(M/N) \subseteq \bigcup \mathrm{Ass}(M/Q_i)$. Thus **(18.19.1)** holds.

If $N = Q_2 \cap \cdots \cap Q_r$, then $\mathrm{Ass}(M/N) \subseteq \{\mathfrak{p}_2, \ldots, \mathfrak{p}_r\}$ too. Thus if equality holds in **(18.19.1)** and if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ 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 $\mathrm{Ass}(P_i/N) \neq \emptyset$ by **(17.13)**. So the first injection yields $\mathrm{Ass}(P_i/N) = \{\mathfrak{p}_i\}$ by **(17.5)**; then the second yields $\mathfrak{p}_i \in \mathrm{Ass}(M/N)$. Thus $\mathrm{Ass}(M/N) \supseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, and **(18.19.1)** yields equality, as desired. □

Theorem **(18.20)** (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 **(18.19)**. □

Theorem **(18.21)** (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 **(17.21)**, M/N has finitely many distinct associated primes, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Owing to **(17.9)**, for each i, there is a $\mathfrak{p}_i$-primary submodule Q_i of M with $\mathrm{Ass}(Q_i/N) = \mathrm{Ass}(M/N) - \{\mathfrak{p}_i\}$. Set $P := \bigcap Q_i$. Fix i. Then $P/N \subset Q_i/N$. So $\mathrm{Ass}(P/N) \subset \mathrm{Ass}(Q_i/N)$ by **(17.5)**. But i is arbitrary. Hence $\mathrm{Ass}(P/N) = \emptyset$. Therefore, $P/N = 0$ by **(17.13)**. Finally, the decomposition $N = \bigcap Q_i$ is irredundant by **(18.19)**. □

Exercise **(18.22)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Consider the following submodule of M:

$$\Gamma_{\mathfrak{a}}(M) := \textstyle\bigcup_{n \geq 1} \{\, m \in M \mid \mathfrak{a}^n m = 0 \,\}.$$

(1) For any decomposition $0 = \bigcap Q_i$ with Q_i $\mathfrak{p}_i$-primary, show $\Gamma_{\mathfrak{a}}(M) = \bigcap_{\mathfrak{a} \not\subset \mathfrak{p}_i} Q_i$. (By convention, if $\mathfrak{a} \subset \mathfrak{p}_i$ for all i, then $\bigcap_{\mathfrak{a} \not\subset \mathfrak{p}_i} Q_i = M$.)
(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 **(18.23)**. — *Let R be a Noetherian ring, S a multiplicative subset, $\mathfrak{p}$ 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 **(11.20)**(2) and **(12.2)**. And $S^{-1}\mathfrak{q} \in \mathrm{Ass}(S^{-1}(M/Q))$ if and only if $\mathfrak{q} \in \mathrm{Ass}(M/Q)$, that is, $\mathfrak{q} = \mathfrak{p}$, by **(17.10)**.

However, $S^{-1}(M/Q) = S^{-1}M/S^{-1}Q$ by **(12.20)**. Therefore, if $S \cap \mathfrak{p} \neq \emptyset$, then $\mathrm{Ass}(S^{-1}M/S^{-1}Q) = \emptyset$; whence, **(17.13)** yields $S^{-1}M/S^{-1}Q = 0$. Otherwise, if $S \cap \mathfrak{p} = \emptyset$, then $\mathrm{Ass}(S^{-1}M/S^{-1}Q) = \{S^{-1}\mathfrak{p}\}$; whence, $S^{-1}Q$ is $S^{-1}\mathfrak{p}$-primary.

Finally, $Q^S = \varphi_S^{-1}(S^{-1}Q)$ by **(12.17)**(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, $\mathfrak{p} = \mathrm{z.div}(M/Q)$ owing to **(17.15)**. Therefore, $m \in Q$. Thus $Q^S \subset Q$. But $Q^S \supset Q$ as $1 \in S$. Thus $Q^S = Q$. □

Proposition **(18.24)**. — *Let R be a Noetherian ring, S a multiplicative subset, 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 **(12.17)**(4)(b), $S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_r$. Further, by **(18.23)**, $S^{-1}Q_i$ 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 **(18.19)**. Indeed, $\mathrm{Ass}(S^{-1}M/S^{-1}N)\{S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_h\}$ by an argument like that in the first part of **(18.23)**. Further, $S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_h$ are distinct by **(11.20)**(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 **(12.17)**(3), we get $N^S = Q_1^S \cap \cdots \cap Q_h^S$. But $Q_i^S = Q_i$ by **(18.23)**. 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 **(18.25)** (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 **(18.24)**, take $S := R - \mathfrak{p}$. Then $h = 1$ as $\mathfrak{p}$ is minimal. □

Exercise **(18.26)**. — Let R be a Noetherian ring, M a finitely generated module, N a submodule. Prove $N = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(M/N)} \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$.

Exercise **(18.27)**. — Let R be a Noetherian ring, $\mathfrak{p}$ a prime. Its n**th symbolic power** $\mathfrak{p}^{(n)}$ is defined as the saturation $(\mathfrak{p}^n)^S$ where $S := R - \mathfrak{p}$.

(1) Show $\mathfrak{p}^{(n)}$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^n$.
(2) Show $\mathfrak{p}^{(m+n)}$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^{(n)}\mathfrak{p}^{(m)}$.
(3) Show $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ if and only if $\mathfrak{p}^n$ is $\mathfrak{p}$-primary.
(4) Given a $\mathfrak{p}$-primary ideal $\mathfrak{q}$, show $\mathfrak{q} \supset \mathfrak{p}^{(n)}$ for all large n.

Exercise **(18.28)**. — Let R be a Noetherian ring, $\langle 0 \rangle = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ an irredundant primary decomposition. Set $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ for $i = 1, \ldots, n$.

(1) Suppose $\mathfrak{p}_i$ is minimal for some i. Show $\mathfrak{q}_i = \mathfrak{p}_i^{(r)}$ for all large r.

(2) Suppose $\mathfrak{p}_i$ is not minimal for some i. Show that replacing $\mathfrak{q}_i$ by $\mathfrak{p}_i^{(r)}$ for large r gives infinitely many distinct irredundant primary decompositions of $\langle 0 \rangle$.

Theorem **(18.29)** (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 **(16.19)**, 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 **(18.21)**: take a 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 **(3.32)**, and so again $N \subset Q_i$. Thus $N \subset \bigcap Q_i = \mathfrak{a}N$, as desired. □

Exercise **(18.30)**. — 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 **(18.31)** (*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 $n \ge 1$. Then, Taylor's Theorem yields

$$f(x) = f(0) + f'(0)x + \cdots + \tfrac{f^{(n-1)}(0)}{(n-1)!}x^{n-1} + x^n f_n(x)$$
$$\text{where}\quad f_n(x) := \int_0^1 \tfrac{(1-t)^{n-1}}{(n-1)!} f^{(n)}(xt)\,dt.$$

Here f_n is C^∞ too, since we can differentiate under the integral sign by [**9**, (7.1), p. 276]. So, if $f \in \mathfrak{m}$, then $f(x) = xf_1(x)$. 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 $\bigcap_{n\ge 0}\mathfrak{m}^n$ 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 [**9**, Ex. 7, p. 82]. Thus $\bigcap_{n\ge 0}\mathfrak{m}^n \neq 0$.

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 $1 + g(x) \ge 1/2$ 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 **(18.29)** 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 the Akizuki–Hopkins 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, $\ell(M) = 0$ if and only if $M = 0$.

For example, if R is a field, then M is a vector space and $\ell(M) = \dim_R(M)$. Also, the chains in **(17.24)** are composition series, but those in **(17.23)** 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 $\ell(M)$. Also,*

$$\operatorname{Supp}(M) = \{\, \mathfrak{m} \in \operatorname{Spec}(R) \mid \mathfrak{m} = \operatorname{Ann}(M_{i-1}/M_i) \text{ for some } i\,\};$$

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 whenever $M'_{i-1}/M'_i = 0$. 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 $n \le \ell(M)$ by induction on $\ell(M)$. If $\ell(M) = 0$, then $M = 0$; so also $n = 0$. Assume $\ell(M) \ge 1$. If $n = 0$, then we're done. If $n \ge 1$, then $\ell(N_1) < \ell(M)$ by **(19.3.1)**; so $n - 1 \le \ell(N_1)$ by induction. Thus $n \le \ell(M)$.

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 $\ell(M) \le n$ by **(19.1.2)**. But we proved $n \le \ell(M)$ above. Thus $n = \ell(M)$, and the first assertion is proved.

To proceed, fix a prime $\mathfrak{p}$. Exactness of Localization, **(12.20)**, 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)** and **(12.1)**. If $\mathfrak{p} \ne \mathfrak{m}$, 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
$$(M_{i-1})_{\mathfrak{p}}/(M_i)_{\mathfrak{p}} \begin{cases} 0, & \text{if } \mathfrak{p} \ne \mathfrak{m}_i; \\ M_{i-1}/M_i \simeq R/\mathfrak{m}_i, & \text{if } \mathfrak{p} = \mathfrak{m}_i. \end{cases}$$
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 **(13.43)**, to prove $\varphi_{\mathfrak{p}}$ is for each maximal ideal $\mathfrak{p}$. Now, localization commutes with finite product by **(12.11)**. Therefore,
$$\varphi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \longrightarrow \left(\prod_{\mathfrak{m}} M_{\mathfrak{m}}\right)_{\mathfrak{p}} = \prod_{\mathfrak{m}} (M_{\mathfrak{m}})_{\mathfrak{p}} = M_{\mathfrak{p}}$$
as $(M_{\mathfrak{m}})_{\mathfrak{p}} = 0$ if $\mathfrak{m} \ne \mathfrak{p}$ 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 the equivalence of the following three conditions:

(1) that M has finite length;
(2) that $\operatorname{Supp}(M)$ consists entirely of maximal ideals;
(3) that $\operatorname{Ass}(M)$ consists entirely of maximal ideals.

Prove that, if the conditions hold, then $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ are equal and finite.

Exercise **(19.5)**. — Let R be a Noetherian ring, $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal. Consider chains of primary ideals from $\mathfrak{q}$ to $\mathfrak{p}$. Show (1) all such chains have length at most $\ell(A) - 1$ where $A := (R/\mathfrak{q})_{\mathfrak{p}}$ and (2) all maximal chains have length exactly $\ell(A) - 1$.

Corollary **(19.6)**. — *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 $i \ge 1$, if $M_{i-1} \ne 0$, 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 **(19.7)**. — 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 **(16.29)**. Since M is infinite, $\ell(M) = \infty$.

Exercise **(19.8)**. — Let k be a field, R an algebra-finite extension. Prove that R is Artinian if and only if R is a finite-dimensional k-vector space.

Theorem **(19.9)** (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 **(19.10)**. — Let k be a field, A a local k-algebra. Assume the map from k to the residue field is bijective. Given an A-module M, prove $\ell(M) = \dim_k(M)$.

Theorem **(19.11)** (Akizuki–Hopkins). — *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 **(19.6)**.

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 $\mathfrak{a}\mathfrak{m} \ne 0$. If $\mathcal{S} \ne \emptyset$, take $\mathfrak{a} \in \mathcal{S}$ minimal. Then $\mathfrak{a}\mathfrak{m}^2 = \mathfrak{a}\mathfrak{m} \ne 0$; hence, $\mathfrak{a}\mathfrak{m} = \mathfrak{a}$ by minimality of $\mathfrak{a}$. For any $x \in \mathfrak{a}$, if $x\mathfrak{m} \ne 0$, 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 $1 \le i \le r$. 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 $R/\mathfrak{m}_i$.

Suppose $\dim(V_i) = \infty$. Take 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 strictly descending chain, a contradiction as R is Artinian. Thus $\dim(V_i) < \infty$. Hence $\ell(R) < \infty$ by **(19.9)**. So R is Noetherian by **(19.6)**. Now, $\operatorname{Ann}(R) = 0$; so 13.26 yields $\operatorname{Supp}(R) = \operatorname{Spec}(R)$. Thus, by **(19.4)**, every prime is maximal, and there are only finitely many primes. □

Exercise **(19.12)**. — Prove these conditions on a Noetherian ring R equivalent:

(1) that R is Artinian;
(2) that $\operatorname{Spec}(R)$ is discrete and finite;
(3) that $\operatorname{Spec}(R)$ is discrete.

EXERCISE **(19.13)**. — Let R be an Artinian ring. Show that $\operatorname{rad}(R)$ is nilpotent.

COROLLARY **(19.14)**. — *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 **(19.11)** every prime is maximal, so $\operatorname{Supp}(M)$ consists of maximal ideals. Also R is Noetherian by **(19.11)**. Hence **(19.4)** yields the assertions. □

COROLLARY **(19.15)**. — *A ring R is Artinian if and only if $\ell(R) < \infty$.*

PROOF: Simply take $M := R$ in **(19.14)** and **(19.6)**. □

EXERCISE **(19.16)**. — 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 **(19.17)**. — *A ring R is Artinian if and only if R is a finite product of Artinian local rings; if so, then $R = \prod_{\mathfrak{m}\in\operatorname{Spec}(R)} R_{\mathfrak{m}}$.*

PROOF: A finite product of rings is Artinian if and only if each factor is Artinian by **(16.27)**(3). If R is Artinian, then $\ell(R) < \infty$ by **(19.15)**; whence, $R = \prod R_{\mathfrak{m}}$ by the Jordan–Hölder Theorem. Thus the assertion holds. □

EXERCISE **(19.18)**. — Let R be a Noetherian ring, and M a finitely generated module. Prove the following four conditions are equivalent:

(1) that M has finite length;
(2) that M is annihilated by some finite product of maximal ideals $\prod \mathfrak{m}_i$;
(3) that every prime $\mathfrak{p}$ containing $\operatorname{Ann}(M)$ is maximal;
(4) that $R/\operatorname{Ann}(M)$ 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 $n \ge 0$ 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 $R = R_0[x_1, \ldots, x_r]$. 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 $m_1, \ldots, m_s$ 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 an R_0-linear combination of the products $x_1^{i_1} \cdots x_r^{i_r} m_i \in M_n$, as desired. □

(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 **(19.14)**. 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 $h(M, n)$, called 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, **(19.9)**. 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

$$N' := \{\, m \in M \mid \text{there is } k_0 \text{ such that } R_k m \subset N \text{ for all } k \geq k_0 \,\}.$$

(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 containing N.

(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.

As R_0 is Artinian, R_0 is Noetherian by the Akizuki–Hopkins Theorem, **(19.11)**. So, since R is a finitely generated R_0-algebra, R is Noetherian by **(16.12)**. Since M is a finitely generated R-module, obviously so is $M(-k_1)$. Hence, so are both K and L by **(16.16)**(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 $H(L, t)$ 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, **(19.9)**, 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)**, *say $R = R_0[x_1, \dots, x_r]$ with $x_i \in R_1$. Assume $M \neq 0$. Then $H(M, t)$ can be written uniquely in the form*

$$H(M, t) = e(t)/t^l(1-t)^d \qquad \textbf{(20.8.1)}$$

with $e(t) \in \mathbb{Z}[t]$ and $e(0)$, $e(1) \neq 0$ and $l \in \mathbb{Z}$ and $r \geq d \geq 0$; also, there is a polynomial $h(M, n) \in \mathbb{Q}[n]$ with degree $d-1$, leading coefficient $e(1)/(d-1)\,!$ and

$$\ell(M_n) = h(M, n) \quad \textit{for } n \geq \deg e(t) - l. \qquad \textbf{(20.8.2)}$$

Proof: We may take $k_i = 1$ for all i in the proof of **(20.7)**. Hence $H(M, t)$ has 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 $H(M, t)$ has 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 $\deg h(R, n) > \deg h(M, n)$; 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** $F^\bullet M$ of M is an infinite descending chain of submodules:

$$M \supset \cdots \supset F^n M \supset F^{n+1} M \supset \cdots.$$

Call it a **$\mathfrak{q}$-filtration** if $\mathfrak{q}F^nM \subset F^{n+1}M$ for all n, and a **stable $\mathfrak{q}$-filtration** if also $M = F^nM$ for $n \ll 0$ and $\mathfrak{q}F^nM = F^{n+1}M$ for $n \gg 0$. This condition means that there are μ and ν with $M = F^\mu$ and $\mathfrak{q}^nF^\nu M = F^{n+\nu}M$ for $n > 0$.

For example, setting $F^nM := M$ for $n \leq 0$ and $F^nM := \mathfrak{q}^nM$ for $n \geq 0$, we get a stable $\mathfrak{q}$-filtration. It is called the **$\mathfrak{q}$-adic filtration**.

The $\mathfrak{q}$-adic filtration of R yields a graded ring $G^\bullet R$, defined by

$$G^\bullet R := \textstyle\bigoplus_{n\geq 0} G^n R \quad \text{where} \quad G^n R := \mathfrak{q}^n/\mathfrak{q}^{n+1}.$$

We form 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 representatives, forming their product, and taking its residue in $\mathfrak{q}^{i+j}/\mathfrak{q}^{i+j+1}$. We call $G^\bullet R$ the **associated graded ring**.

As each F^nM is an R-module, so is the direct sum

$$G^\bullet M := \textstyle\bigoplus_{n\in\mathbb{Z}} G^n M \quad \text{where} \quad G^n M := F^nM/F^{n+1}M.$$

If $F^\bullet M$ is a $\mathfrak{q}$-filtration, then this R-structure amounts to an $R/\mathfrak{q}$-structure; further, $G^\bullet M$ is a graded $G^\bullet R$-module.

Given $m \in \mathbb{Z}$, let $M[m]$ denote M with the filtration $F^\bullet M$ reindexed by **shifting** it m places to the left; that is, $F^n(M[m]) := F^{n+m}M$ for all n. Then

$$G^n(M[m]) = F^{n+m}M/F^{n+m+1}M = (G^nM)(m).$$

If the quotients M/F^nM have finite length, call $n \mapsto \ell(M/F^nM)$ the **Hilbert–Samuel Function**, and call the generating function

$$P(F^\bullet M, t) := \textstyle\sum_{n\geq 0} \ell(M/F^nM)t^n$$

the **Hilbert–Samuel Series**. If the function $n \mapsto \ell(M/F^nM)$ is, for $n \gg 0$, a polynomial $p(F^\bullet M,\, n)$, then call it the **Hilbert–Samuel Polynomial**. If the filtration is the $\mathfrak{q}$-adic filtration, we also denote $P(F^\bullet M,\, t)$, and $p(F^\bullet M,\, n)$ 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 $G^\bullet R$ is generated as an $R/\mathfrak{q}$-algebra by finitely many elements of $\mathfrak{q}/\mathfrak{q}^2$, and $G^\bullet M$ is a finitely generated $G^\bullet R$-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 $G^\bullet R$ as an $R/\mathfrak{q}$-algebra.

By stability, there are μ and ν with $F^\mu M = M$ and $\mathfrak{q}^n F^\nu M = F^{n+\nu}M$ for $n \ge 0$. Hence $G^\bullet M$ is generated by $F^\mu M/F^{\mu+1}M, \dots, F^\nu M/F^{\nu+1}M$ over $G^\bullet R$. But R is Noetherian and M is finitely generated over R; hence, every F^nM is finitely generated over R. Therefore, every $F^nM/F^{n+1}M$ is finitely generated over $R/\mathfrak{q}$. Thus $G^\bullet M$ is a finitely generated $G^\bullet R$-module. □

Theorem **(20.13)** (Samuel). — *Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, and M a finitely generated module with a stable $\mathfrak{q}$-filtration $F^\bullet M$. Assume $\ell(M/\mathfrak{q}M) < \infty$. Then $\ell(F^nM/F^{n+1}M) < \infty$ and $\ell(M/F^nM) < \infty$ for every $n \ge 0$; further,*

$$P(F^\bullet M,\, t) = H(G^\bullet M,\, t)\, t/(1-t). \qquad \textbf{(20.13.1)}$$

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. Also, M can be viewed as a finitely generated R'-module, and $F^\bullet M$ as a stable $\mathfrak{q}'$-filtration. So $G^\bullet R'$ is generated as an $R'/\mathfrak{q}'$-algebra by finitely many elements of degree 1, and $G^\bullet M$ is a finitely generated $G^\bullet R'$-module by **(20.12)**. Therefore, each $F^nM/F^{n+1}M$ 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 **(13.27)**(3) and **(13.31)** 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 the Akizuki–Hopkins Theorem, **(19.11)**.

Hence $\ell(F^nM/F^{n+1}M) < \infty$ for every n by **(19.14)**. Form the exact sequence

$$0 \to F^nM/F^{n+1}M \to M/F^{n+1}M \to M/F^nM \to 0.$$

Then Additivity of Length, **(19.9)**, yields

$$\ell(F^nM/F^{n+1}M) = \ell(M/F^{n+1}M) - \ell(M/F^nM).$$

So induction on n yields $\ell(M/F^{n+1}M) < \infty$ for every n. Further, multiplying that equation by t^n and summing over n yields the desired expression in another form:

$$H(G^\bullet M,\, t) = (t^{-1}-1)P(F^\bullet M,\, t) = P(F^\bullet M,\, t)\,(1-t)/t. \qquad \square$$

Corollary **(20.14)**. — *Under the conditions of **(20.13)**, assume $\mathfrak{q}$ is generated by r elements and $M \neq 0$. Then $P(F^\bullet M,\, t)$ can be written uniquely in the form*

$$P(F^\bullet M,\, t) = e(t)/t^{l-1}(1-t)^{d+1} \qquad \textbf{(20.14.1)}$$

with $e(t) \in \mathbb{Z}[t]$ and $e(0),\ e(1) \neq 0$ and $l \in \mathbb{Z}$ and $r \ge d \ge 0$; also, there is a polynomial $p(F^\bullet M,\, n) \in \mathbb{Q}[n]$ with degree d and leading coefficient $e(1)/d\,!$ such that

$$\ell(M/F^nM) = p(F^\bullet M,\, n) \quad \text{for } n \ge \deg e(t) - l. \qquad \textbf{(20.14.2)}$$

Finally, $p_{\mathfrak{q}}(M,\, n) - p(F^\bullet M,\, n)$ is a polynomial with degree at most $d-1$ and positive leading coefficient; also, d and $e(1)$ are the same for every stable $\mathfrak{q}$-filtration.

Proof: The proof of **(20.13)** shows that $G^\bullet R'$ and $G^\bullet M$ satisfy the hypotheses of **(20.8)**. So **(20.8.1)** and **(20.13.1)** yield **(20.14.1)**. In turn, **(20.13.1)** yields **(20.14.2)** by the argument in the second paragraph of the proof of **(20.8)**.

Finally, as $F^\bullet M$ is a stable $\mathfrak{q}$-filtration, there is an m such that

$$F^nM \supset \mathfrak{q}^nM \supset \mathfrak{q}^nF^mM = F^{n+m}M$$

for all $n \ge 0$. Dividing into M and extracting lengths, we get

$$\ell(M/F^nM) \le \ell(M/\mathfrak{q}^nM) \le \ell(M/F^{n+m}M).$$

Therefore, **(20.14.2)** yields

$$p(F^\bullet M,\, n) \le p_{\mathfrak{q}}(M,\, n) \le p(F^\bullet M,\, n+m) \quad \text{for } n \gg 0.$$

The two extremes are polynomials in n with the same degree d and the same leading coefficient c where $c := e(1)/d\,!$. 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. Also $p_{\mathfrak{q}}(M,\, n) - p(F^\bullet M,\, n)$ 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

$$\mathcal{R}(\mathfrak{q}) := \bigoplus\nolimits_{n\in\mathbb{Z}} \mathcal{R}_n(\mathfrak{q}) \quad \text{with } \mathcal{R}_n(\mathfrak{q}) := \begin{cases} R & \text{if } n \le 0, \\ \mathfrak{q}^n & \text{if } n > 0 \end{cases}$$

is canonically an R-algebra, known as the **extended Rees Algebra** of $\mathfrak{q}$.

Let M be a module with a $\mathfrak{q}$-filtration $F^\bullet M$. Then the sum

$$\mathcal{R}(F^\bullet M) := \bigoplus\nolimits_{n\in\mathbb{Z}} F^nM$$

is canonically an $\mathcal{R}(\mathfrak{q})$-module, known as the **Rees Module** of $F^\bullet M$.

Lemma **(20.17)**. — *Let R be a Noetherian ring, $\mathfrak{q}$ an ideal, M a finitely generated module with a $\mathfrak{q}$-filtration $F^\bullet M$. Then $\mathcal{R}(\mathfrak{q})$ is algebra finite over R. Also, $F^\bullet M$ is stable if and only if $\mathcal{R}(F^\bullet M)$ is module finite over $\mathcal{R}(\mathfrak{q})$ and $\bigcup F^nM = M$.*

Proof: As R is Noetherian, $\mathfrak{q}$ is finitely generated, say by $x_1, \dots, x_r$. View the x_i as in $\mathcal{R}_1(\mathfrak{q})$ and $1 \in R$ as in $\mathcal{R}_{-1}(\mathfrak{q})$. These $r+1$ elements generate $\mathcal{R}(\mathfrak{q})$ over R.

Suppose that $F^\bullet M$ is stable: say $F^\mu M = M$ and $\mathfrak{q}^nF^\nu MF^{n+\nu}M$ for $n > 0$. Then $\bigcup F^nM = M$. Further, $\mathcal{R}(F^\bullet M)$ is generated by $F^\mu M, \dots, F^\nu M$ over $\mathcal{R}(\mathfrak{q})$. But R is Noetherian and M is finitely generated over R; hence, every F^nM is finitely generated over R. Thus $\mathcal{R}(F^\bullet M)$ is a finitely generated $\mathcal{R}(\mathfrak{q})$-module.

Conversely, suppose that $\mathcal{R}(F^\bullet M)$ is generated over $\mathcal{R}(\mathfrak{q})$ by $m_1, \dots, m_s$. Say $m_i = \sum_{j=\mu}^{\nu} m_{ij}$ with $m_{ij} \in F^jM$ for some uniform $\mu \le \nu$. Then given n, any $m \in F^nM$ can be written as $m = \sum f_{ij}m_{ij}$ with $f_{ij} \in \mathcal{R}_{n-j}(\mathfrak{q})$. Hence if $n \le \mu$, then $F^nM \subset F^\mu M$. Suppose $\bigcup F^nM = M$. Then $F^\mu M = M$. But if $j \le \nu \le n$, then $f_{ij} \in \mathfrak{q}^{n-j} = \mathfrak{q}^{n-\nu}\mathfrak{q}^{\nu-j}$. Thus $\mathfrak{q}^{n-\nu}F^\nu M = F^nM$. Thus $F^\bullet M$ is stable. □

Lemma **(20.18)** (Artin–Rees). — *Let R be a Noetherian ring, M a finitely generated module, N a submodule, $\mathfrak{q}$ an ideal, $F^\bullet M$ a stable $\mathfrak{q}$-filtration. Set*

$$F^nN := N \cap F^nM \quad \text{for } n \in \mathbb{Z}.$$

Then the F^nN form a stable $\mathfrak{q}$-filtration $F^\bullet N$.

Proof: By **(20.17)**, the extended Rees Algebra $\mathcal{R}(\mathfrak{q})$ is finitely generated over R, so Noetherian by the Hilbert Basis Theorem **(16.12)**. By **(20.17)**, the module $\mathcal{R}(F^\bullet M)$ is finitely generated over $\mathcal{R}(\mathfrak{q})$, so Noetherian by **(16.19)**. Clearly, $F^\bullet N$ is a $\mathfrak{q}$-filtration; hence, $\mathcal{R}(F^\bullet N)$ is a submodule of $\mathcal{R}(F^\bullet M)$, so finitely generated. But $\bigcup F^nM = M$, so $\bigcup F^nN = N$. Thus $F^\bullet N$ is stable by **(20.17)**. □

Exercise **(20.19)**. — Derive the Krull Intersection Theorem, **(18.29)**, 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 $\deg p_{\mathfrak{q}}(M',n) - 1$ 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, **(13.31)** and **(13.27)**(1) and **(13.31)** again yield

$$\begin{aligned}\operatorname{Supp}(M/\mathfrak{q}M) &= \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q}) = \big(\operatorname{Supp}(M') \bigcup \operatorname{Supp}(M'')\big) \bigcap \mathbf{V}(\mathfrak{q}) \\ &= \big(\operatorname{Supp}(M') \bigcap \mathbf{V}(\mathfrak{q})\big) \bigcup \big(\operatorname{Supp}(M'') \bigcap \mathbf{V}(\mathfrak{q})\big) \\ &= \operatorname{Supp}(M'/\mathfrak{q}M') \bigcup \operatorname{Supp}(M''/\mathfrak{q}M'').\end{aligned}$$

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 $n \in \mathbb{Z}$, set $F^nM' := M' \bigcap \mathfrak{q}^nM$. Then the F^nM' form a stable $\mathfrak{q}$-filtration $F^\bullet M'$ by the Artin–Rees Lemma. Form this canonical commutative diagram:

$$\begin{tikzcd} 0 \arrow[r] & F^nM' \arrow[r] \arrow[d] & \mathfrak{q}^nM \arrow[r] \arrow[d] & \mathfrak{q}^nM'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0 \end{tikzcd}$$

Its rows are exact. So the Nine Lemma yields this exact sequence:

$$0 \to M'/F^nM' \to M/\mathfrak{q}^nM \to M''/\mathfrak{q}^nM'' \to 0.$$

Assume $M/\mathfrak{q}M$ has finite length. Then Additivity of Length and **(20.14)** yield

$$p(F^\bullet M',\, n) - p_{\mathfrak{q}}(M,\, n) + p_{\mathfrak{q}}(M'',\, n) = 0. \tag{20.20.1}$$

Hence $p_{\mathfrak{q}}(M',\, n) - p_{\mathfrak{q}}(M,\, n) + p_{\mathfrak{q}}(M'',\, n)$ is equal to $p_{\mathfrak{q}}(M',\, n) - p(F^\bullet M',\, n)$. But by **(20.14)** again, the latter is a polynomial with degree at most $\deg p_{\mathfrak{q}}(M',\, n) - 1$ 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 $\operatorname{Ker}(\alpha)$ is a homogeneous submodule of M. Further, $\operatorname{Coker}(\alpha)$ is canonically graded, and the quotient map $M \to \operatorname{Coker}(\alpha)$ is homogeneous of degree 0.

Exercise **(20.22)**. — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus_{n \ge n_0} M_n$ a graded module, $\mathfrak{a} \subset \bigoplus_{n>0} R_n$ a homogeneous ideal. Assume $M = \mathfrak{a}M$. Show $M = 0$.

Exercise **(20.23)**. — Let $R = \bigoplus R_n$ be a Noetherian graded ring, $M = \bigoplus M_n$ a finitely generated graded R-module, $N = \bigoplus N_n$ a homogeneous submodule. Set

$$N' := \{\, m \in M \mid R_n m \in N \text{ for all } n \gg 0 \,\}.$$

Show that N' is the largest homogeneous submodule of M containing N and having, for all $n \gg 0$, its degree-n homogeneous component N'_n equal to N_n.

Proposition **(20.24)**. — *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 $x \in \mathfrak{p} := \operatorname{nil}(M/Q)$. 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: $x = \sum_{i \ge r} x_i$ and $m = \sum_{j \ge s} m_j$. 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 $x'^k \in \operatorname{Ann}(M/Q)$ for some $k \ge 1$. 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 $x'' \ne 0$. 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 **(20.25)**. — 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.

Exercise **(20.26)**. — 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 **(20.27)**. — *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 **(18.21)**. 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 **(20.26)**. Thus $N = \bigcap Q_j^*$ is a primary decomposition into homogeneous primary submodules. And, owing to **(18.19)**, 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 **(18.20)** and **(20.25)**. □

(20.28) (*Graded Domains*). — Let $R = \bigoplus_{n\geq 0} R_n$ be a graded domain, and set $K := \operatorname{Frac}(R)$. 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 **(20.29)**. — *Let R be a Noetherian graded domain, $K := \operatorname{Frac}(R)$, and $\overline{R}$ the integral closure of R in K. Then $\overline{R}$ is a graded subring of K.*

Proof: Use the setup of **(20.28)**. Since $K_0[x]$ is a polynomial ring over a field, it is normal by **(10.34)**. 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 **(10.23)**. So **(20.28)** 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 **(20.30)**. — 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.

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 **(17.20)**. They are also the minimal primes $\mathfrak{p}_0 \in \operatorname{Supp}(M)$ by **(17.17)**. Thus **(1.9)** yields

$$\dim(M) = \max\{\, \dim(R/\mathfrak{p}_0) \mid \mathfrak{p}_0 \in \operatorname{Supp}(M) \text{ is minimal}\,\}. \qquad \mathbf{(21.1.1)}$$

(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 **(13.27)**(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 **(16.19)**. Fix an ideal $\mathfrak{q}$. Then by **(19.6)**, $M/\mathfrak{q}M$ 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 **(17.21)**. Also, by **(13.31)**, **(13.27)**(3), and **(13.1)**,

$$\operatorname{Supp}(M/\mathfrak{q}M) = \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q}) = \mathbf{V}(\operatorname{Ann}(M)) \bigcap \mathbf{V}(\mathfrak{q}) = \mathbf{V}(\operatorname{Ann}(M) + \mathfrak{q}).$$

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 **(19.11)**, if and only if $R/\mathfrak{q}'$ is Artinian. But **(19.18)** implies that $R/\mathfrak{q}'$ is Artinian if and only if $\mathfrak{q}'$ contains a product of maximal ideals each containing $\mathfrak{q}'$. 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*

$$\mathfrak{m} \supset \mathfrak{q}' \supset \mathfrak{m}^n \quad \textit{for some } n, \qquad \mathbf{(21.2.1)}$$

or by **(3.33)** *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 $H(G^{\bullet}M, t)$. 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 $x_1, \ldots, x_s \in \mathfrak{m}$ with

$$\ell(M/\langle x_1, \ldots, x_s\rangle M) < \infty. \tag{21.2.2}$$

By convention, if $\ell(M) < \infty$, then $s(M) = 0$. We say that $x_1, \ldots, x_s \in \mathfrak{m}$ 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 $x \in \mathrm{rad}(M)$. Set $K := \mathrm{Ker}(M \xrightarrow{\mu_x} M)$.*

(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 $\mathfrak{p} \in \mathrm{Supp}(M)$ 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 $x_1, \ldots, x_s \in \mathrm{rad}(M/xM)$ with

$$\ell(M/\langle x, x_1, \ldots, x_s\rangle M) < \infty.$$

Now, $\mathrm{Supp}(M/xM) = \mathrm{Supp}(M) \cap \mathbf{V}(\langle x\rangle)$ by **(13.31)**. However, $x \in \mathrm{rad}(M)$. Hence, $\mathrm{Supp}(M/xM)$ and $\mathrm{Supp}(M)$ have the same maximal ideals. Therefore, $\mathrm{rad}(M/xM) = \mathrm{rad}(M)$. 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 $\mathrm{Supp}(M/xM)$. Again, $\mathrm{Supp}(M/xM) = \mathrm{Supp}(M) \cap \mathbf{V}(\langle x\rangle)$ by **(13.31)**. So $x \in \mathfrak{p}_0 \in \mathrm{Supp}(M)$. So, by hypothesis, $\dim(R/\mathfrak{p}_0) < \dim(M)$. Hence $r \le \dim(M) - 1$. Thus (2) holds.

To prove (3), note that $xM := \mathrm{Im}(\mu_x)$, 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 $\mathfrak{m} := \mathrm{rad}(M)$. 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 **(10.11)** applied over the semilocal ring $R/\mathrm{Ann}(M)$. Hence $\ell(M) < \infty$. So $\dim(M) = 0$ by **(19.4)**.

Suppose $d(M) \ge 1$. By **(21.1.1)**, $\dim(R/\mathfrak{p}_0) = \dim(M)$ for some $\mathfrak{p}_0 \in \mathrm{Supp}(M)$. Then $\mathfrak{p}_0$ is minimal. So $\mathfrak{p}_0 \in \mathrm{Ass}(M)$ by **(17.18)**. Hence M has a submodule N isomorphic to $R/\mathfrak{p}_0$ by **(17.2)**. Further, by **(20.20)**, $d(N) \le d(M)$.

Take a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in $\mathrm{Supp}(N)$. If $r = 0$, then $r \le d(M)$. Suppose $r \ge 1$. 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 $\mathrm{Supp}(M)$, 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 $\mathrm{Supp}(N) \bigcap \mathbf{V}(\langle x\rangle)$. But the latter is equal to $\mathrm{Supp}(N/xN)$ by **(13.31)**. So $r - 1 \le \dim(N/xN)$.

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 $d(N/xN) \le d(N) - 1$. But $d(N) \le d(M)$. So $\dim(N/xN) \le d(N/xN)$ by the induction hypothesis. Therefore, $r \le d(M)$. Thus $\dim(M) \le d(M)$.

Second, let's prove $d(M) \le s(M)$. Let $\mathfrak{q}$ be a parameter ideal of M with $s(M)$ generators. Then $d(M) := \deg p_{\mathfrak{q}}(M, n)$. But $\deg p_{\mathfrak{q}}(M, n) \le s(M)$ owing to **(20.14)**. Thus $d(M) \le s(M)$.

Finally, let's prove $s(M) \le \dim(M)$. Set $r := \dim(M)$, which is finite since $r \le d(M)$ by the first step. The proof proceeds by induction on r. If $r = 0$, then M has finite length by **(19.4)**; so by convention $s(M) = 0$.

Suppose $r \ge 1$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the primes of $\mathrm{Supp}(M)$ with $\dim(R/\mathfrak{p}_i) = r$. No $\mathfrak{p}_i$ is maximal as $r \ge 1$. So $\mathfrak{m}$ lies in no $\mathfrak{p}_i$. Hence, by Prime Avoidance **(3.19)**, there is an $x \in \mathfrak{m}$ such that $x \notin \mathfrak{p}_i$ for all i. So **(21.3)**(1), (2) yield $s(M) \le s(M/xM) + 1$ and $\dim(M/xM) + 1 \le r$. By the induction hypothesis, $s(M/xM) \le \dim(M/xM)$. Hence $s(M) \le r$, as desired. □

Corollary **(21.5)**. — *Let R be a Noetherian ring, M a nonzero Noetherian semilocal module, $x \in \mathrm{rad}(M)$. Then $\dim(M/xM) \ge \dim(M) - 1$, with equality if $x \notin \mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$; equality holds if $x \notin \mathrm{z.div}(M)$.*

Proof: By **(21.3)**(1), we have $s(M/xM) \ge s(M) - 1$. So the asserted inequality holds by **(21.4)**. If $x \notin \mathfrak{p} \in \mathrm{Supp}(M)$ when $\dim(R/\mathfrak{p}) = \dim(M)$, then **(21.3)**(2) yields the opposite inequality, so equality. Finally, if $x \notin \mathrm{z.div}(M)$, then $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$ owing to **(17.18)** and **(17.15)**. □

Exercise **(21.6)**. — Let A be a Noetherian local ring, N a finitely generated module, $y_1, \ldots, y_r$ a sop for N. Set $N_i := N/\langle y_1, \ldots, y_i\rangle N$. Show $\dim(N_i) = r - i$.

(21.7) (*Height*). — Let R be a ring, and $\mathfrak{p}$ a prime. The **height** of $\mathfrak{p}$, denoted $\mathrm{ht}(\mathfrak{p})$, is defined by this formula:

$$\mathrm{ht}(\mathfrak{p}) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{p} \,\}.$$

The bijective correspondence $\mathfrak{p} \mapsto \mathfrak{p}R_{\mathfrak{p}}$ of **(11.20)**(2) yields this formula:

$$\mathrm{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}}). \tag{21.7.1}$$

If $\mathrm{ht}(\mathfrak{p}) = h$, then we say that $\mathfrak{p}$ is a *height-h prime*.

Corollary **(21.8)**. — *Let R be a Noetherian ring, $\mathfrak{p}$ a prime. Then $\mathrm{ht}(\mathfrak{p}) \le r$ if and only if $\mathfrak{p}$ is a minimal prime of some 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 **(11.20)**. So $\mathfrak{q} = \mathfrak{p}$. Hence $\mathfrak{p}R_{\mathfrak{p}} = \sqrt{\mathfrak{a}R_{\mathfrak{p}}}$ by the Scheinnullstellensatz. Hence $r \ge s(R_{\mathfrak{p}})$ by **(21.2)**. But $s(R_{\mathfrak{p}}) = \dim(R_{\mathfrak{p}})$ by **(21.4)**, and $\dim(R_{\mathfrak{p}}) = \mathrm{ht}(\mathfrak{p})$ by **(21.7.1)**. Thus $\mathrm{ht}(\mathfrak{p}) \le r$.

Conversely, assume $\mathrm{ht}(\mathfrak{p}) \le r$. Then $R_{\mathfrak{p}}$ has a parameter ideal $\mathfrak{b}$ generated by r elements, say $y_1, \ldots, y_r$ by **(21.7.1)** 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 **(11.20)**(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

(11.20)(2). Thus $\mathfrak{p}$ is minimal containing $\mathfrak{a}$, which is generated by r elements. □

Exercise **(21.9)**. — 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 $\mathrm{ht}(\mathfrak{p}) = r$. Prove $\mathrm{ht}(\mathfrak{p}') = r - r'$.

Theorem **(21.10)** (Krull Principal Ideal). — *Let R be a Noetherian ring, $x \in R$, and $\mathfrak{p}$ a minimal prime of $\langle x\rangle$. If $x \notin \mathrm{z.div}(R)$, then $\mathrm{ht}(\mathfrak{p}) = 1$.*

Proof: By **(21.8)**, $\mathrm{ht}(\mathfrak{p}) \le 1$. But by **(14.10)**, $x \in \mathrm{z.div}(R)$ if $\mathrm{ht}(\mathfrak{p}) = 0$. □

Exercise **(21.11)**. — Let R be a Noetherian ring, $\mathfrak{p}$ a prime of height at least 2. Prove that $\mathfrak{p}$ is the union of height-1 primes, but not of finitely many.

Exercise **(21.12)**. — Let R be a Noetherian ring. Prove the following equivalent:

(1) R has only finitely many primes.
(2) R has only finitely many height-1 primes.
(3) R is semilocal of dimension 1.

Exercise **(21.13)** (*Artin–Tate* [**1**, Thm. 4]). — Let R be a Noetherian domain, and set $K := \mathrm{Frac}(R)$. Prove the following statements are equivalent:

(1) $K = R_f$ for some nonzero $f \in R$.
(2) K is algebra finite over R.
(3) Some nonzero $f \in R$ lies in every nonzero prime.
(4) R has only finitely many height-1 primes.
(5) R is semilocal of dimension 1.

Exercise **(21.14)**. — 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 **(21.15)**. — (1) Let A be a Noetherian local ring with a principal prime $\mathfrak{p}$ of height at least 1. Prove A is a domain by showing any prime $\mathfrak{q} \subsetneqq \mathfrak{p}$ is $\langle 0\rangle$.

(2) Let k be a field, $P := k[[X]]$ the formal power series ring in one variable. Set $R := P \times P$. Prove that R is Noetherian and semilocal, and that R contains a principal prime $\mathfrak{p}$ of height 1, but that R is not a domain.

Exercise **(21.16)**. — 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 **(21.17)**. — *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. 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 $\dim(B) \ge \dim(B/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p})$ 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 $\mathrm{ht}(\mathfrak{p})$ is a chain of primes of B of length $\mathrm{ht}(\mathfrak{p}) + \dim(B/\mathfrak{p})$. Hence it suffices to show that $\mathrm{ht}(\mathfrak{p}) \ge \dim(A)$.

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 $\mathrm{ht}(\mathfrak{p}) \ge \dim(A)$, as desired. □

Exercise **(21.18)**. — Let R be a Noetherian ring. Prove that

$$\dim(R[X]) = \dim(R) + 1.$$

Exercise **(21.19)**. — 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.

(21.20) (*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 **(21.19)**, 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 conversely. An example of a regular local ring of given dimension n is the localization $P_\mathfrak{m}$ of a polynomial ring P in n variables over a field at any maximal ideal $\mathfrak{m}$, as $\dim(P_\mathfrak{m}) = n$ by **(15.13)** and **(15.14)** and as $\mathfrak{m}$ is generated by n elements by **(15.6)**.

Lemma **(21.21)**. — *Let A be a Noetherian semilocal ring of dimension r, and $\mathfrak{q}$ a parameter ideal. Then $\deg h(G^\bullet A,\, n) = r - 1$.*

Proof: By **(20.8)**, $\deg h(G^\bullet A,\, n)$ is equal to 1 less than the order of pole at 1 of the Hilbert series $H(G^\bullet A,\, t)$. But that order is equal to $d(A)$ by **(21.2)**. Also, $d(A) = r$ by the Dimension Theorem, **(21.4)**. Thus the assertion holds. □

Proposition **(21.22)**. — *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 $G^\bullet A$ is a polynomial ring; if so, then the number of variables is r.*

Proof: Say $G^\bullet A$ is a polynomial ring in s variables. Then $\dim(\mathfrak{m}/\mathfrak{m}^2) = s$. By **(20.4)**, $\deg h(G^\bullet A,\, n) = s - 1$. So $s = r$ by **(21.21)**. So A is regular by **(21.20)**.

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 $\varphi\colon P \to G^\bullet A$ with $\varphi(X_i) = x_i'$.

Then φ is surjective as the x_i' generate $G^\bullet A$. Set $\mathfrak{a} := \mathrm{Ker}\,\varphi$. Let $P = \bigoplus P_n$ be the grading by total degree. Then φ preserves the gradings of P and $G^\bullet A$. So $\mathfrak{a}$ inherits a grading: $\mathfrak{a} = \bigoplus \mathfrak{a}_n$. So for $n \ge 0$, there's this canonical exact sequence:

$$0 \to \mathfrak{a}_n \to P_n \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to 0. \qquad \textbf{(21.22.1)}$$

Suppose $\mathfrak{a} \ne 0$. Then there's a nonzero $f \in \mathfrak{a}_m$ for some m. Take $n \ge m$. Then $P_{n-m}f \subset \mathfrak{a}_n$. Since P is a domain, $P_{n-m} \xrightarrow{\sim} P_{n-m}f$. Therefore, **(21.22.1)** yields

$$\begin{aligned}\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) &= \dim_k(P_n) - \dim_k(\mathfrak{a}_n)\\ &\le \dim_k(P_n) - \dim_k(P_{n-m}) = \tbinom{r-1+n}{r-1} - \tbinom{r-1+n-m}{r-1}.\end{aligned}$$

The expression on the right is a polynomial in n of degree $r-2$.

On the other hand, $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = h(G^\bullet A,\, n)$ for $n \gg 0$ by **(20.8)**. Further, $\deg h(G^\bullet A,\, n) = r - 1$ by **(21.21)**. However, it follows from the conclusion of the preceding paragraph that $\deg h(G^\bullet A, n) \le r-2$. We have a contradiction! Hence $\mathfrak{a}=0$. Thus φ is injective, so bijective, as desired. □

Exercise **(21.23)**. — Let A be a Noetherian local ring of dimension r, and let $x_1, \dots, x_s \in A$ with $s \le r$. 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 **(21.24)**. — *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 $r \ge 1$. Let x be a member of a regular sop. Then $A/\langle x \rangle$ is regular of dimension $r-1$ by **(21.23)**. By induction, $A/\langle x \rangle$ is a domain. So $\langle x \rangle$ is prime. Thus A is a domain by **(21.15)**. □

Lemma **(21.25)**. — *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 **(21.26)**. — *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, **(21.25)** 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 **(21.23)**. By **(21.24)**, both $A/\mathfrak{b}$ and B are domains of dimension $r-s$; whence, **(15.11)** 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 $F^\bullet M$. Then M has a *topology*: the open sets are the arbitrary unions of sets of the form $m + F^n M$ for various m and n. Indeed, the intersection of two open sets is open, as the intersection of two unions is the union of the pairwise intersections; further, if the intersection U of $m + F^n M$ and $m' + F^{n'} M$ is nonempty and if $n \ge n'$, then $U = m + F^n M$, because, if say $m'' \in U$, then

$$m + F^n M = m'' + F^n M \subset m'' + F^{n'} M = m' + F^{n'} M. \qquad \textbf{(22.1.1)}$$

The addition map $M \times M \to M$, given by $(m, m') \mapsto m + m'$, is continuous, as

$$(m + F^n M) + (m' + F^n M) \subset (m + m') + F^n M.$$

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

$$(x + \mathfrak{a}^n)(m + F^n M) \subset xm + F^n M.$$

Further, if the filtration is $\mathfrak{a}$-stable, then it yields the same topology as the $\mathfrak{a}$-adic filtration, because for some n' and any n,

$$F^n M \supset \mathfrak{a}^n M \supset \mathfrak{a}^n F^{n'} M = F^{n+n'} M.$$

Thus *any two stable $\mathfrak{a}$-filtrations give the same topology*: 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 $N \subset M$ be a submodule. *Its closure $\overline{N}$ is equal to $\bigcap_n (N + F^n M)$*, as $m \notin \overline{N}$ means there's n with $(m + F^n M) \cap N = \emptyset$, or equivalently $m \notin (N + F^n M)$. In particular, each $F^n M$ is closed, and $\{0\}$ is closed if and only if $\bigcap F^n M = \{0\}$.

Also, M *is* **separated**—that is, **Hausdorff**—*if and only if $\{0\}$ is closed.* For, if $\{0\}$ is closed, so is each $\{m\}$. So given $m' \ne m$, there's n' with $m \notin (m' + F^{n'} M)$. Take $n \ge n'$. Then $(m + F^n M) \cap (m' + F^{n'} M) = \emptyset$ owing to **(22.1.1)**.

Finally, M is **discrete**—that is, every $\{m\}$ is both open and closed—*if and only if $\{0\}$ is just open.*

A sequence $(m_n)_{n \ge 0}$ in M is called **Cauchy** if, given n_0, there's n_1 with

$$m_n - m_{n'} \in F^{n_0} M, \quad \text{or simply } m_n - m_{n+1} \in F^{n_0} M, \quad \text{for all } n, n' \ge n_1;$$

the two conditions are equivalent because $F^{n_0} M$ 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 $m - m_n \in F^{n_0}M$ 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 scalar multiplication. The sequences with 0 as a limit form a submodule. The quotient module is denoted $\widehat{M}$ and called the (separated) **completion**. There is a canonical homomorphism, which carries $m \in M$ to the class of the constant sequence (m):

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

If M is complete, but not separated, then κ is surjective, but not bijective.

It is easy to check that the notions of Cauchy sequence and limit depend only on the topology. Further, $\widehat{M}$ is separated and complete with respect to the filtration $F^k\widehat{M} := (F^kM)\widehat{\ }$ where $(F^kM)\widehat{\ }$ is the completion of F^kM arising from the intersections $F^kM \cap F^nM$ for all n. In addition, *κ is the universal continuous R-linear map from M into a separated and complete, filtered $\widehat{R}$-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 R' be a ring, and $R := R'[X_1, \ldots, X_r]$ 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 $R'[[X_1, \ldots, X_r]]$.

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 that the following three conditions are equivalent:

$$(1)\ \ \kappa\colon M \to \widehat{M} \text{ is injective;} \quad (2)\ \ \bigcap \mathfrak{a}^n M = \langle 0\rangle; \quad (3)\ \ M \text{ is separated.}$$

Assume R is Noetherian and M finitely generated. Assume either (a) $\mathfrak{a} \subset \operatorname{rad}(R)$ or (b) R is a domain, $\mathfrak{a}$ is proper, and M is torsionfree. Conclude $M \subset \widehat{M}$.

(22.5) (*Inverse limits*). — Let R be a ring. Given R-modules Q_n equipped with linear maps $\alpha_n^{n+1}\colon Q_{n+1} \to Q_n$ for n, 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.

Given Q_n and α_n^{n+1} for all $n \in \mathbb{Z}$, use only those for n in the present context.

Define $\theta\colon \prod Q_n \to \prod Q_n$ by $\theta(q_n) := (q_n - \alpha_n^{n+1} q_{n+1})$. Then

$$\varprojlim Q_n = \operatorname{Ker}\theta. \quad \text{Set } \varprojlim{}^1 Q_n := \operatorname{Coker}\theta. \tag{22.5.1}$$

Plainly, $\varprojlim Q_n$ *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 the following natural R-linear isomorphism:

$$\varprojlim \operatorname{Hom}(P, Q_n) = \operatorname{Hom}(P, \varprojlim Q_n).$$

(The notion of inverse limit is formally dual to that of direct limit.)

For example, let R' be a ring, and $R := R'[X_1, \ldots, X_r]$ the polynomial ring in r variables. Set $\mathfrak{m} := \langle X_1, \ldots, X_r\rangle$ 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 $R'[[X_1, \ldots, X_r]]$.

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 $0 \leq z_i < p$, 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.

Exercise **(22.6)**. — Let R be a ring. Given R-modules Q_n equipped with linear maps $\alpha_n^{n+1}\colon Q_{n+1} \to Q_n$ for $n \geq 0$, set $\alpha_n^m := \alpha_n^{n+1} \cdots \alpha_{m-1}^m$ for $m > n$. We say the Q_n satisfy the **Mittag-Leffler Condition** if the descending chain

$$Q_n \supset \alpha_n^{n+1} Q_{n+1} \supset \alpha_n^{n+2} Q_{n+2} \supset \cdots \supset \alpha_n^m Q_m \supset \cdots$$

stabilizes; that is, $\alpha_n^m Q_m = \alpha_n^{m+k} Q_{m+k}$ for all $k > 0$.

(1) Assume for each n, there is $m > n$ with $\alpha_n^m = 0$. Show $\varprojlim^1 Q_n = 0$.

(2) Assume α_n^{n+1} is surjective for all n. Show $\varprojlim^1 Q_n = 0$.

(3) Assume the Q_n satisfy the Mittag-Leffler Condition. Set $P_n := \bigcap_{m\geq n} \alpha_n^m Q_m$, which is the stable submodule. Show $\alpha_n^{n+1} P_{n+1} = P_n$.

(4) Assume the Q_n satisfy the Mittag-Leffler Condition. Show $\varprojlim^1 Q_n = 0$.

Lemma **(22.7)**. — *For $n \geq 0$, consider commutative diagrams with exact rows*

$$\begin{tikzcd}
0 \arrow[r] & Q'_{n+1} \arrow[r, "\gamma'_{n+1}"] \arrow[d, "\alpha'^{n+1}_n"'] & Q_{n+1} \arrow[r, "\gamma_{n+1}"] \arrow[d, "\alpha^{n+1}_n"'] & Q''_{n+1} \arrow[r] \arrow[d, "\alpha''^{n+1}_n"'] & 0 \\
0 \arrow[r] & Q'_n \arrow[r, "\gamma'_n"] & Q_n \arrow[r, "\gamma_n"] & Q''_n \arrow[r] & 0
\end{tikzcd}$$

Then the induced sequence

$$0 \to \varprojlim Q'_n \xrightarrow{\widehat{\gamma}'} \varprojlim Q_n \xrightarrow{\widehat{\gamma}} \varprojlim Q''_n \tag{22.7.1}$$

is exact; further, $\widehat{\gamma}$ is surjective if the Q'_n satisfy the Mittag-Leffler Condition.

Proof: The given commutative diagrams yield the following one:

$$\begin{tikzcd}
0 \arrow[r] & \prod Q'_n \arrow[r, "\prod\gamma'_n"] \arrow[d, "\theta'"'] & \prod Q_n \arrow[r, "\prod\gamma_n"] \arrow[d, "\theta"'] & \prod Q''_n \arrow[r] \arrow[d, "\theta''"'] & 0 \\
0 \arrow[r] & \prod Q'_n \arrow[r, "\prod\gamma'_n"] & \prod Q_n \arrow[r, "\prod\gamma_n"] & \prod Q''_n \arrow[r] & 0
\end{tikzcd}$$

Owing to **(22.5.1)**, the Snake Lemma **(5.13)** yields the exact sequence **(22.7.1)** and an injection $\operatorname{Coker}\widehat{\gamma} \hookrightarrow \varprojlim^1 Q'_n$. Assume the Q'_n satisfy the Mittag-Leffler Condition. Then $\varprojlim^1 Q'_n = 0$ by **(22.6)**. So $\operatorname{Coker}\widehat{\gamma} = 0$. Thus $\widehat{\gamma}$ is surjective. □

Proposition **(22.8)**. — *Let R be a ring, M a module, $F^\bullet M$ a filtration. Then*

$$\widehat{M} \xrightarrow{\sim} \varprojlim (M/F^nM).$$

Proof: First, let us define a map $\alpha\colon \widehat{M} \to \varprojlim(M/F^nM)$. Given a Cauchy sequence (m_ν), let q_n be the residue of m_ν in M/F^nM 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/F^nM. Also, (m_ν) has 0 as a limit if and only if $q_n = 0$ for all n. Define α by $\alpha m_\nu := (q_n)$. It is easy to check that α is well defined, linear, and injective.

As to surjectivity, given $(q_n) \in \varprojlim(M/F^nM)$, for each ν lift $q_\nu \in M/F^\nu M$ up to $m_\nu \in M$. Then $m_\mu - m_\nu \in F^\nu M$ for $\mu \geq \nu$, as $q_\mu \in M/F^\mu M$ maps to $q_\nu \in M/F^\nu M$. Hence (m_ν) is Cauchy. Thus α is surjective, so an isomorphism. □

Example **(22.9)**. — Let R be a ring, M a module, $F^\bullet M$ a filtration. For $n \geq 0$, consider the following natural commutative diagrams with exact rows:

$$\begin{array}{ccccccccc}
0 & \to & F^{n+1}M & \to & M & \to & M/F^{n+1}M & \to & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F^nM & \longrightarrow & M & \longrightarrow & M/F^nM & \longrightarrow & 0
\end{array}$$

with vertical maps, respectively, the inclusion, the identity, and the quotient map. By **(22.8)**, the left-exact sequence of inverse limits is

$$0 \to \varprojlim F^nM \to M \xrightarrow{\kappa} \widehat{M}.$$

But κ is not surjective when M is not complete; for examples of such M, see the end of **(22.1)**. Thus $\varprojlim$ is not always exact, nor $\varprojlim^1$ always 0.

Exercise **(22.10)**. — Let A be a ring, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ be maximal ideals. Set $\mathfrak{m} := \bigcap \mathfrak{m}_i$, and give A the $\mathfrak{m}$-adic topology. Prove that $\widehat{A} = \prod \widehat{A}_{\mathfrak{m}_i}$.

Exercise **(22.11)**. — Let R be a ring, M a module, $F^\bullet M$ a filtration, and $N \subset M$ a submodule. Give N and M/N the induced filtrations:

$$F^nN := N \cap F^nM \quad \text{and} \quad F^n(M/N) := F^nM/F^nN.$$

(1) Prove $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = (M/N)\widehat{\ }$.

(2) Also assume $N \supset F^nM$ for $n \gg 0$. Prove $\widehat{M}/\widehat{N} = M/N$ and $G^\bullet\widehat{M} = G^\bullet M$.

Exercise **(22.12)**. — (1) Let R be a ring, $\mathfrak{a}$ an ideal. If $G^\bullet R$ is a domain, show $\widehat{R}$ is a 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 **(22.13)**. — *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 **(22.11)**; 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 **(22.14)**. — Let A be a Noetherian local ring, $\mathfrak{m}$ the maximal ideal, M a finitely generated module. Prove (1) that $\widehat{A}$ is a Noetherian local ring with $\widehat{\mathfrak{m}}$ as maximal ideal, (2) that $\dim(M) = \dim(\widehat{M})$, and (3) that A is regular if and only if $\widehat{A}$ is regular.

Exercise **(22.15)**. — Let A be a ring, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ maximal ideals. Set $\mathfrak{m} := \bigcap \mathfrak{m}_i$ and give A the $\mathfrak{m}$-adic topology. Prove that $\widehat{A}$ is a semilocal ring, that $\widehat{\mathfrak{m}}_1, \ldots, \widehat{\mathfrak{m}}_m$ are all its maximal ideals, and that $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{A})$.

(22.16) (*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 **(22.8)**, 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 $u_nt \equiv 1 \pmod{\mathfrak{a}^n}$. 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 **(2.31)** and **(1.9)** yield

$$T = \{\, t \in R \mid t \text{ lies in no maximal ideal containing } \mathfrak{a} \,\}. \qquad \textbf{(22.16.1)}$$

Set $S := 1 + \mathfrak{a}$. Then $S \subset T$ owing to **(22.16.1)** as no maximal ideal can contain both x and $1 + x$. Hence the UMP of localization **(11.5)** yields this diagram:

$$\begin{array}{ccccc}
 & & R & & \\
 & \swarrow{\scriptstyle\varphi_S} & \downarrow{\scriptstyle\varphi_T} & \searrow{\scriptstyle\kappa} & \\
S^{-1}R & \xrightarrow{\sigma} & T^{-1}R & \xrightarrow{\tau} & \widehat{R}
\end{array}$$

Further, S and T map into $(R/\mathfrak{a}^n)^\times$; hence, **(11.6)**, **(11.23)**, and **(12.22)** yield:

$$R/\mathfrak{a}^n = S^{-1}R/\mathfrak{a}^nS^{-1}R = T^{-1}R/\mathfrak{a}^nT^{-1}R.$$

Therefore, $\widehat{R}$ is, by **(22.8)**, 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 **(22.16.1)**. 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, **(18.29)** 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 **(22.17)** (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 finitely generated modules. Set $F^nM' := M' \cap \mathfrak{a}^nM$. By the Artin–Rees Lemma **(20.18)**, the F^nM' form an $\mathfrak{a}$-stable filtration. Hence, it yields the same topology, so the same completion, as the $\mathfrak{a}$-adic filtration by **(22.1)**. Thus $0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$ is exact by **(22.7)** and **(22.8)**, as desired. □

Exercise **(22.18)**. — Let A be a Noetherian semilocal ring. Prove that an element $x \in A$ is a nonzerodivisor on A if and only if its image $\widehat{x} \in \widehat{A}$ is one on $\widehat{A}$.

Exercise **(22.19)**. — Let $p \in \mathbb{Z}$ be prime. For $n > 0$, define a $\mathbb{Z}$-linear map

$$\alpha_n\colon \mathbb{Z}/\langle p\rangle \to \mathbb{Z}/\langle p^n\rangle \quad \text{by} \quad \alpha_n(1) = p^{n-1}.$$

Set $A := \bigoplus_{n\geq 1} \mathbb{Z}/\langle p\rangle$ and $B := \bigoplus_{n\geq 1} \mathbb{Z}/\langle p^n\rangle$. Set $\alpha := \bigoplus \alpha_n$; so $\alpha\colon A \to B$.

(1) Show that the p-adic completion $\widehat{A}$ is just A.

(2) Show that, in the topology on A induced by the p-adic topology on B, the completion $\overline{A}$ is equal to $\prod_{n=1}^\infty \mathbb{Z}/\langle p\rangle$.

(3) Show that the natural sequence of p-adic completions
$$\widehat{A} \xrightarrow{\widehat{\alpha}} \widehat{B} \xrightarrow{\widehat{\kappa}} (B/A)\widehat{\ }$$
is not exact at $\widehat{B}$. (Thus p-adic completion is *neither* left exact *nor* right exact.)

Corollary **(22.20)**. — *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 **(22.17)**, the functor $M \mapsto \widehat{M}$ is exact on the category of finitely generated modules, and so **(8.19)** yields the conclusion. □

Exercise **(22.21)**. — 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 **(22.22)**. — *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 **(22.20)**, and the bottom map is injective by **(22.17)**. 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 $\mathfrak{b}^nR' = (\mathfrak{b}R')^n$ for any R-algebra R'. Thus (2) holds. □

Corollary **(22.23)**. — *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 **(22.20)**, and $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$ by **(22.22)**(2). Thus $\widehat{R}$ is flat by the Ideal Criterion **(9.26)**. □

Exercise **(22.24)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Prove that $\widehat{R}$ is faithfully flat if and only if $\mathfrak{a} \subset \operatorname{rad}(R)$.

Exercise **(22.25)**. — 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 **(22.26)**. — *Let R be a ring, $\alpha\colon M \to N$ a map of modules, $F^\bullet M$ and $F^\bullet N$ filtrations. Assume $\alpha F^nM \subset F^nN$ for all n. Assume $F^nM = M$ and $F^nN = N$ for $n \ll 0$. If the induced map $G^\bullet\alpha$ is injective or surjective, then so is $\widehat{\alpha}$.*

Proof: For each $n \in \mathbb{Z}$, form the following commutative diagram of R-modules:
$$\begin{array}{ccccccccc} 0 & \to & F^nM/F^{n+1}M & \to & M/F^{n+1}M & \to & M/F^nM & \to & 0 \\ & & \downarrow{\scriptstyle G^n\alpha} & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} & & \\ 0 & \longrightarrow & F^nN/F^{n+1}N & \longrightarrow & N/F^{n+1}N & \longrightarrow & N/F^nN & \longrightarrow & 0 \end{array}$$

Its rows are exact. So the Snake Lemma **(5.13)** yields this exact sequence:
$$\operatorname{Ker} G^n\alpha \to \operatorname{Ker}\alpha_{n+1} \to \operatorname{Ker}\alpha_n \to \operatorname{Coker} G^n\alpha \to \operatorname{Coker}\alpha_{n+1} \to \operatorname{Coker}\alpha_n.$$

Assume $G^\bullet\alpha$ is injective. Then $\operatorname{Ker} G^n\alpha = 0$. But $M/F^nM = 0$ for $n \ll 0$. So by induction $\operatorname{Ker}\alpha_n = 0$ for all n. Thus $\widehat{\alpha}$ is injective by **(22.7)** and **(22.8)**.

Assume $G^\bullet\alpha$ is surjective, or $\operatorname{Coker} G^n\alpha = 0$. So $\operatorname{Ker}\alpha_{n+1} \to \operatorname{Ker}\alpha_n$ is surjective. But $N/F^nN = 0$ for $n \ll 0$. So by induction, $\operatorname{Coker}\alpha_n = 0$ for all n. So
$$0 \to \operatorname{Ker}\alpha_n \to M/F^nM \xrightarrow{\alpha_n} N/F^nN \to 0$$
is exact. Thus $\widehat{\alpha}$ is surjective by **(22.7)** and **(22.8)**. □

Lemma **(22.27)**. — *Let R be a ring, $\mathfrak{a}$ an ideal, M a module, $F^\bullet M$ an $\mathfrak{a}$-filtration. Assume R is complete, M is separated, and $F^nM = M$ for $n \ll 0$. Assume $G^\bullet M$ is module finite over $G^\bullet R$. Then M is complete, and is module finite over R.*

Proof: Take finitely many generators μ_i of $G^\bullet M$, and replace them by their homogeneous components. Set $n_i := \deg(\mu_i)$. Lift μ_i to $m_i \in F^{n_i}M$.

Filter R $\mathfrak{a}$-adically. Set $E := \bigoplus_i R[-n_i]$. Filter E with $F^nE := \bigoplus_i F^n(R[-n_i])$. Then $F^nE = E$ for $n \ll 0$. Define $\alpha\colon E \to M$ by sending $1 \in R[-n_i]$ to $m_i \in M$. Then $\alpha F^nE \subset F^nM$ for all n. Also, $G^\bullet\alpha\colon G^\bullet E \to G^\bullet M$ is surjective as the μ_i generate. So $\widehat{\alpha}$ is surjective by **(22.26)**.

Form the following canonical commutative diagram:
$$\begin{array}{ccc} E & \xrightarrow{\kappa_E} & \widehat{E} \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \widehat{\alpha}} \\ M & \xrightarrow{\kappa_M} & \widehat{M} \end{array}$$
As R is complete, $\kappa_R\colon R \to \widehat{R}$ is surjective by **(22.1)**; hence, κ_E is surjective. Thus κ_M is surjective; that is, M is complete. As M is separated, κ_M is injective by **(22.4)**. So κ_M is bijective. So α is surjective. Thus M is module finite. □

Exercise **(22.28)** (*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 $m_1, \ldots, m_n \in M$ generate assuming their images $m'_1, \ldots, m'_n$ in $M/\mathfrak{a}M$ generate.

Proposition **(22.29)**. — *Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Assume R is complete, and M separated. Assume $G^\bullet M$ is a Noetherian $G^\bullet R$-module. Then M is a Noetherian R-module, and every submodule N is complete.*

Proof: Let $F^\bullet M$ denote the $\mathfrak{a}$-adic filtration, and $F^\bullet N$ the induced filtration: $F^nN := N \cap F^nM$. Then N is separated, and $F^nN = N$ for $n \ll 0$. Further, $G^\bullet N \subset G^\bullet M$. However, $G^\bullet M$ is Noetherian. So $G^\bullet N$ is module finite. Thus N is complete and is module finite over R by **(22.27)**. Thus M is Noetherian. □

Theorem **(22.30)**. — *Let R be a ring, $\mathfrak{a}$ an ideal. If R is Noetherian, so is $\widehat{R}$.*

Proof: Assume R is Noetherian. Then $G^\bullet R$ is algebra finite over $R/\mathfrak{a}$ by **(20.12)**, so Noetherian by the Hilbert Basis Theorem, **(16.12)**. But $G^\bullet R = G^\bullet\widehat{R}$ by **(22.11)**. Thus $\widehat{R}$ is Noetherian by **(22.29)** with $\widehat{R}$ for R and $\widehat{R}$ for M. □

Example **(22.31)**. — 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 **(22.30)**.

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 **(3.10)**. 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 $\dim A \ge r$.

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 **(22.13)** or again by **(3.10)**. Therefore, $\dim A \le r$ by **(21.19)**. Thus A *is regular of dimension r.*

Theorem **(22.32)** (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 in the $\mathfrak{b}$-adic topology, then there is a unique R-algebra map $\widehat{\pi}\colon P \to R'$ with $\widehat{\pi}(X_i) = x_i$ for $1 \le i \le n$.*

Proof: Form the map $\pi\colon R[X_1, \dots, X_n] \to R'$ with $\pi(X_i) = x_i$. By the UMP of completion π induces the desired map $\widehat{\pi}\colon P \to R'$.

Alternatively, for each m, the map π 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 $\widehat{\pi}$ owing to **(22.5)** and **(22.8)**. □

Theorem **(22.33)** (Cohen Structure). — *Let A be a complete Noetherian local ring with maximal ideal $\mathfrak{m}$. Assume that A contains a* **coefficient field** *k; that is, $k \xrightarrow{\sim} A/\mathfrak{m}$. 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 **(22.32)**. Then $G^\bullet\pi$ is surjective. Hence, π is surjective by **(22.26)**. Set $\mathfrak{a} := \mathrm{Ker}(\pi)$. Then $k[[X_1, \dots, X_n]]/\mathfrak{a} \xrightarrow{\sim} A$.

Assume A is regular of dimension r. Take $n := r$. Then $G^\bullet A$ is a polynomial ring in r variables over k by **(21.22)**. And $G^\bullet\big(k[[X_1, \dots, X_r]]\big)$ is too by **(22.5)**. Since $G^\bullet\pi$ is surjective, it is bijective by **(10.4)** with $G^\bullet A$ for both R and M. So π is bijective by **(22.26)**. 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. Along the way, we study the notions of regular sequence, depth, and Cohen–Macaulayness; these notions are so important that we study them further in an appendix.

(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 $x, y \in K^\times$,

$$(1)\ v(x \cdot y) = v(x) + v(y), \quad (2)\ v(x + y) \ge \min\{v(x),\, v(y)\} \text{ if } x \ne -y. \quad \textbf{(23.1.1)}$$

Condition (1) just means v is a group homomorphism. Hence, for any $x \in K^\times$,

$$(1)\ v(1) = 0 \quad \text{and} \quad (2)\ v(x^{-1}) = -v(x). \quad \textbf{(23.1.2)}$$

As a convention, we define $v(0) := \infty$. Consider the sets

$$A := \{x \in K \mid v(x) \ge 0\} \quad \text{and} \quad \mathfrak{m} := \{x \in K \mid v(x) > 0\}.$$

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, $\mathrm{Frac}(A) = K$. Further,

$$A^\times = \{x \in K \mid v(x) = 0\} = A - \mathfrak{m}.$$

Indeed, if $x \in A^\times$, then $v(x) \ge 0$ and $-v(x) = v(x^{-1}) \ge 0$; 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 $v(a) \ge 0$ and $v(b) \ge 0$ 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 $u \in A^\times$; also, A is a UFD.

Moreover, A *is a* PID; *in fact, any nonzero ideal $\mathfrak{a}$ of A has the form*

$$\mathfrak{a} = \langle t^m\rangle \quad \text{where} \quad m := \min\{\, v(x) \mid x \in \mathfrak{a}\,\}. \quad \textbf{(23.1.3)}$$

Indeed, given a nonzero $x \in \mathfrak{a}$, say $x = ut^n$ where $u \in A^\times$. Then $t^n \in \mathfrak{a}$. So $n \ge m$. 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.

Example **(23.2)**. — The prototype is this example. Let k be a field, t a variable, and $K := k((t))$ the field of formal Laurent series $x := \sum_{i \ge n} a_i t^i$ with $n \in \mathbb{Z}$ and with $a_i \in k$ and $a_n \ne 0$. 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 **(22.4)**, and $\widehat{A} = k[[t]]$ by the proof of the Cohen Structure Theorem **(22.33)**. 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 **(23.3)**. — *Let A be a local domain, $\mathfrak{m}$ its maximal ideal. Assume that $\mathfrak{m}$ is nonzero and principal and that $\bigcap_{n\ge 0}\mathfrak{m}^n = 0$. Then A is a DVR.*

Proof: Given a nonzero $x \in A$, there is an $n \ge 0$ 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 $K := \mathrm{Frac}(A)$. 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 $n \ge h$, 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 $n \ge h$. Then $x + y = t^h(ut^{n-h} + w)$. Hence

$$v(x+y) \ge h = \min\{n, h\} = \min\{v(x),\, v(y)\}.$$

Thus (2) holds. So $v\colon K^\times \to \mathbb{Z}$ is a valuation. Clearly, A is the DVR of v. □

(23.4) (*Depth*). — Let R be a ring, M a nonzero module, and $x_1, \dots, x_n \in R$. Set $M_i := M/\langle x_1, \dots, x_i\rangle M$. We say the sequence $x_1, \dots, x_n$ is M-**regular**, or is an M-**sequence**, and we call n its **length** if $M_n \ne 0$ and $x_i \notin \mathrm{z.div}(M_{i-1})$ for all i.

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 $\mathrm{depth}(\mathfrak{a}, M)$. By convention, $\mathrm{depth}(\mathfrak{a}, M) = 0$ means $\mathfrak{a}$ contains no nonzerodivisor on M.

If M is semilocal, call the depth of $\mathrm{rad}(M)$ on M simply the **depth** of M and denote it by $\mathrm{depth}(M)$. Notice that, in this case, the condition $M_n \ne 0$ is automatic owing to Nakayama's Lemma **(10.11)**.

If M is semilocal and $\mathrm{depth}(M) = \dim(M)$, call M **Cohen–Macaulay**. When R is semilocal, call R **Cohen–Macaulay** if R is a Cohen–Macaulay R-module.

Lemma **(23.5)**. — *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, and M a nonzero finitely generated module.*

(1) *Then* $\mathrm{depth}(M) = 0$ *if and only if* $\mathfrak{m} \in \mathrm{Ass}(M)$.

(2) *Then* $\mathrm{depth}(M) = 1$ *if and only if there is an* $x \in \mathfrak{m}$ *with* $x \notin \mathrm{z.div}(M)$ *and* $\mathfrak{m} \in \mathrm{Ass}(M/xM)$.

(3) *Then* $\mathrm{depth}(M) \le \dim(M)$.

Proof: Consider (1). If $\mathfrak{m} \in \mathrm{Ass}(M)$, then it is immediate from the definitions that $\mathfrak{m} \subset \mathrm{z.div}(M)$ and so $\mathrm{depth}(M) = 0$.

Conversely, assume $\mathrm{depth}(M) = 0$. Then $\mathfrak{m} \subset \mathrm{z.div}(M)$. Since A is Noetherian, $\mathrm{z.div}(M) = \bigcup_{\mathfrak{p}\in\mathrm{Ass}(M)} \mathfrak{p}$ by **(17.15)**. Since M is also finitely generated, $\mathrm{Ass}(M)$ is finite by **(17.21)**. Hence $\mathfrak{m} = \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M)$ by Prime Avoidance, **(3.19)**.

Consider (2). Assume $\mathrm{depth}(M) = 1$. Then there is an M-sequence of length 1, but none longer. So there is an $x \in \mathfrak{m}$ with $x \notin \mathrm{z.div}(M)$ and $\mathrm{depth}(M/xM) = 0$. Then $\mathfrak{m} \in \mathrm{Ass}(M/xM)$ by (1).

Conversely, assume there is $x \in \mathfrak{m}$ with $x \notin \mathrm{z.div}(M)$. Then $\mathrm{depth}(M) \ge 1$ by definition. Assume $\mathfrak{m} \in \mathrm{Ass}(M/xM)$. Then given any $y \in \mathfrak{m}$ with $y \notin \mathrm{z.div}(M)$, also $\mathfrak{m} \in \mathrm{Ass}(M/yM)$ by **(17.27)**. So $\mathrm{depth}(M/yM) = 0$ by (1). So there is no $z \in \mathfrak{m}$ such that y, z is an M-sequence. Thus $\mathrm{depth}(M) \le 1$. Thus $\mathrm{depth}(M) = 1$.

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 $\dim(M) - n = \dim(M_n) \ge 0$. But $\mathrm{depth}(M) := \sup\{n\}$. Thus (3) holds. □

Exercise **(23.6)**. — Let R be a ring, M a module, and $x, y \in R$.

(1) Assume that x, y form an M-sequence. Prove that, given any $m, n \in M$ with $xm = yn$, there exists $p \in M$ with $m = yp$ and $n = xp$.

(2) Assume that x, y form an M-sequence and that $y \notin \mathrm{z.div}(M)$. Prove that y, x form an M-sequence too.

(3) Assume that R is local, that x, y lie in its maximal ideal $\mathfrak{m}$, and that M is nonzero and Noetherian. Assume that, given any $m, n \in M$ with $xm = yn$, there exists $p \in M$ with $m = yp$ and $n = xp$. Prove that x, y form an M-sequence.

Exercise **(23.7)**. — Let A be a Noetherian local ring, M and N nonzero finitely generated modules, $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ a left-exact functor that preserves the finitely generated modules (such as $F(\bullet) := \mathrm{Hom}(M, \bullet)$ by **(16.20)**). Show that, for $d = 1, 2$, if N has depth at least d, then so does $F(N)$.

Exercise **(23.8)**. — 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 **(23.9)**. — Prove that a Noetherian local ring A of dimension $r \ge 1$ is regular if and only if its maximal ideal $\mathfrak{m}$ is generated by an A-sequence. Prove that, if A is regular, then A is Cohen–Macaulay.

Theorem **(23.10)** (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 **(10.33)**. 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 $A/\langle x\rangle \ne 0$, so $\mathrm{Ass}\big(A/\langle x\rangle\big) \ne \emptyset$ by **(17.13)**. Now, A is a local domain of dimension 1. So A has just two primes: $\langle 0\rangle$ and $\mathfrak{m}$. But $\langle 0\rangle \notin \mathrm{Ass}(A/\langle x\rangle)$. So $\mathfrak{m} \in \mathrm{Ass}(A/\langle x\rangle)$. Thus **(23.5)**(2) yields (3).

Assume (3). By **(23.5)**(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 $\mathfrak{m} = \mathrm{Ann}(\overline{y})$. So $y\mathfrak{m} \subset \langle x\rangle$. Set $z := y/x \in \mathrm{Frac}(A)$. Then $z\mathfrak{m} = (y\mathfrak{m})/x \subset A$. Suppose $z\mathfrak{m} \subset \mathfrak{m}$. Then z is integral over A by **(10.23)**. 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, $\mathrm{ht}(\mathfrak{m}) \ge 1$ because $x \in \mathfrak{m}$ and $x \ne 0$. Thus (5) holds.

Assume (5). Set $N := \bigcap \mathfrak{m}^n$. The Krull Intersection Theorem **(18.29)** yields an $x \in \mathfrak{m}$ with $(1+x)N = 0$. Then $1 + x \in A^\times$. So $N = 0$. Further, A is a domain by

(21.15)(1). Thus (1) holds by **(23.3)**. □

Exercise **(23.11)**. — 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 **(23.12)**. — 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 $(0,0)$; see **(23.21)**.)

Exercise **(23.13)**. — 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 **(23.14)**. — 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 $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q})$.
(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 $q \in Q$.

(23.15) (*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 $m \le n$, the localization $R_\mathfrak{p}$ is regular of dimension m.

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.

We say **Serre's Condition** (S_n) holds for an R-module M if, for any prime $\mathfrak{p}$,

$$\mathrm{depth}(M_\mathfrak{p}) \ge \min\{\dim(M_\mathfrak{p}),\, n\}.$$

Note $\mathrm{depth}(M_\mathfrak{p}) \le \dim(M_\mathfrak{p})$ by **(23.5)**(3). Hence (S_n) holds if and only if $M_\mathfrak{p}$ is Cohen–Macaulay when $\mathrm{depth}(M_\mathfrak{p}) < n$. In particular, ($\mathrm{S}_1$) holds if and only if $\mathfrak{p}$ is minimal when $\mathfrak{p} \in \mathrm{Ass}(M)$ by **(17.15)**; that is, M has no embedded primes.

Exercise **(23.16)**. — Let R be a Noetherian domain, M a finitely generated module. Show that M is torsionfree if and only if it satisfies (S_1).

Exercise **(23.17)**. — Let R be a Noetherian ring. Show that R is reduced if and only if (R_0) and (S_1) hold.

Lemma **(23.18)**. — *Let R be a Noetherian domain. Set*

$$\Phi := \{\,\mathfrak{p} \text{ prime} \mid \mathrm{ht}(\mathfrak{p}) = 1\,\} \quad \text{and} \quad \Sigma := \{\,\mathfrak{p} \text{ prime} \mid \mathrm{depth}(R_\mathfrak{p}) = 1\,\}.$$

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 $\mathfrak{q} \in \mathrm{Ass}(R_\mathfrak{p}/\langle x\rangle)$ by **(17.18)**. Hence $\mathrm{depth}(R_\mathfrak{p}) = 1$ by **(23.5)**(2). Thus $\Phi \subset \Sigma$.

However, (S_1) holds by **(23.17)**. Hence (S_2) holds if and only if $\Phi \supset \Sigma$. Thus $\Phi = \Sigma$ if and only if (S_2) holds.

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 $\mathfrak{p}R_\mathfrak{p} \in \mathrm{Ass}(R_\mathfrak{p}/bR_\mathfrak{p})$ by **(23.5)**(2), so if $\mathfrak{p} \in \mathrm{Ass}(R/bR)$ by **(17.10)**. Hence $a \in bR$ by **(18.26)**. Thus $x \in R$, as desired. □

Theorem **(23.19)**. — *Let R be a normal Noetherian domain. Then*

$$R = \textstyle\bigcap_{\mathfrak{p}\in\Phi} R_\mathfrak{p} \quad \text{where} \quad \Phi := \{\,\mathfrak{p} \text{ prime} \mid \mathrm{ht}(\mathfrak{p}) = 1\,\}.$$

Proof: As R is normal, so is $R_\mathfrak{p}$ for any prime $\mathfrak{p}$ by **(11.32)**. So $\mathrm{depth}(R_\mathfrak{p}) = 1$ if and only if $\dim(R_\mathfrak{p}) = 1$ by **(23.10)**. Thus **(23.18)** yields the assertion. □

Theorem **(23.20)** (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 **(23.17)**. If R is normal, then so is $R_\mathfrak{p}$ for any prime $\mathfrak{p}$ by **(11.32)**; whence, (R_1) and (S_2) hold by **(23.10)**.

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 **(23.18)**. Thus R is normal. □

Example **(23.21)**. — 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 **(15.13)** or by **(21.18)**. 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 **(23.12)** 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 **(23.22)**. — 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 **(23.23)**. — Let R be a Noetherian ring, K its total quotient ring,

$$\Phi := \{\,\mathfrak{p} \text{ prime} \mid \mathrm{ht}(\mathfrak{p}) = 1\,\} \quad \text{and} \quad \Sigma := \{\,\mathfrak{p} \text{ prime} \mid \mathrm{depth}(R_\mathfrak{p}) = 1\,\}.$$

Assuming (S_1) holds for 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:

$$R \to K \to \textstyle\prod_{\mathfrak{p}\in\Sigma} K_\mathfrak{p}/R_\mathfrak{p}.$$

Exercise **(23.24)**. — Let R be a Noetherian ring, and K its total quotient ring. Set $\Phi := \{\,\mathfrak{p} \text{ prime} \mid \mathrm{ht}(\mathfrak{p}) = 1\,\}$. 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.

23. Appendix: Cohen–Macaulayness

Exercise **(23.25)**. — Let $R \to R'$ be a flat map of Noetherian rings, $\mathfrak{a} \subset R$ an ideal, M a finitely generated R-module, and $x_1, \dots, x_r$ an M-sequence in $\mathfrak{a}$. Set $M' := M \otimes_R R'$. Assume $M'/\mathfrak{a}M' \neq 0$. Show $x_1, \dots, x_r$ is an M'-sequence in $\mathfrak{a}R'$.

Exercise **(23.26)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module with $M/\mathfrak{a}M \neq 0$. Let $x_1, \dots, x_r$ be an M-sequence in $\mathfrak{a}$ and $\mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)$. Prove the following statements:
(1) $x_1/1, \dots, x_r/1$ is an $M_\mathfrak{p}$-sequence in $\mathfrak{a}_\mathfrak{p}$, and
(2) $\mathrm{depth}(\mathfrak{a}, M) \le \mathrm{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p})$.

(23.27) (*Finished Sequences*). — Let R be a ring, $\mathfrak{a}$ an ideal, M a nonzero module. We say an M-sequence in $\mathfrak{a}$ is **finished in** $\mathfrak{a}$, if it can not be lengthened in $\mathfrak{a}$.

In particular, a sequence of length 0 is finished in $\mathfrak{a}$ if there are no nonzerodivisors on M in $\mathfrak{a}$; that is, $\mathfrak{a} \subset \mathrm{z.div}(M)$.

An M-sequence in $\mathfrak{a}$ can, plainly, be lengthened until finished in $\mathfrak{a}$ provided $\mathrm{depth}(\mathfrak{a}, M)$ is finite. It is finite if R is Noetherian, M is finitely generated, and $M/\mathfrak{a}M \neq 0$, as then $\mathrm{depth}(\mathfrak{a}, M) \le \mathrm{depth}(M_\mathfrak{p})$ for any $\mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)$ by **(23.26)**(2) and $\mathrm{depth}(M_\mathfrak{p}) \le \dim(M_\mathfrak{p})$ by **(23.5)**(3) and $\dim(M_\mathfrak{p}) < \infty$ by **(21.4)**.

Proposition **(23.28)**. — *Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Assume $M/\mathfrak{a}M \neq 0$. Let $x_1, \dots, x_m$ be a finished M-sequence in $\mathfrak{a}$. Then $m = \mathrm{depth}(\mathfrak{a}, M)$.*

Proof: Let $y_1, \dots, y_n$ be a second finished M-sequence in $\mathfrak{a}$. Say $m \le n$. Induct on m. Suppose $m = 0$. Then $\mathfrak{a} \subset \mathrm{z.div}(M)$. Hence $n = 0$ too. Now, suppose $m \ge 1$.

Set $M_i := M/\langle x_1, \dots, x_i\rangle M$ and $N_j := M/\langle y_1, \dots, y_j\rangle M$ for all i, j. Set

$$U := \bigcup_{i=0}^{m-1} \mathrm{z.div}(M_i) \cup \bigcup_{j=0}^{n-1} \mathrm{z.div}(N_j).$$

Then U is equal to the union of all associated primes of M_i for $i < m$ and of N_j for $j < n$ by **(17.15)**. And these primes are finite in number by **(17.21)**. Suppose $\mathfrak{a} \subset U$. Then $\mathfrak{a}$ lies in one of the primes, say $\mathfrak{p} \in \mathrm{Ass}(M_i)$, by **(3.19)**. But $x_{i+1} \in \mathfrak{a} - \mathrm{z.div}(M_i)$ and $\mathfrak{a} \subset \mathfrak{p} \subset \mathrm{z.div}(M_i)$, a contradiction. Thus $\mathfrak{a} \not\subset U$.

Take $z \in \mathfrak{a} - U$. Then $z \notin \mathrm{z.div}(M_i)$ for $i < m$ and $z \notin \mathrm{z.div}(N_j)$ for $j < n$. Now, $\mathfrak{a} \subset \mathrm{z.div}(M_m)$ by finishedness. So $\mathfrak{a} \subset \mathfrak{q}$ for some $\mathfrak{q} \in \mathrm{Ass}(M_m)$ by **(17.26)**. But $M_m = M_{m-1}/x_m M_{m-1}$. Moreover, x_m and z are nonzerodivisors on M_{m-1}. Also $x_m, z \in \mathfrak{a} \subset \mathfrak{q}$. So $\mathfrak{q} \in \mathrm{Ass}(M_{m-1}/zM_{m-1})$ by **(17.27)**. Hence

$$\mathfrak{a} \subset \mathrm{z.div}(M/\langle x_1, \dots, x_{m-1}, z\rangle M).$$

Hence $x_1, \dots, x_{m-1}, z$ is finished in $\mathfrak{a}$. Similarly, $y_1, \dots, y_{n-1}, z$ is finished in $\mathfrak{a}$. Thus we may replace both x_m and y_n by z.

By **(23.6)**(2), we may move z to the front of both sequences. Thus we may assume $x_1 = y_1 = z$. Then $M_1 = N_1$. Further, $x_2, \dots, x_m$ and $y_2, \dots, y_n$ are finished M_1-sequences in $\mathfrak{a}$. So by induction, $m - 1 = n - 1$. Thus $m = n$. □

Exercise **(23.29)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module with $M/\mathfrak{a}M \neq 0$. Let $x \in \mathfrak{a}$ be a nonzerodivisor on M. Show

$$\mathrm{depth}(\mathfrak{a}, M/xM) = \mathrm{depth}(\mathfrak{a}, M) - 1.$$

Exercise **(23.30)**. — Let A be a Noetherian local ring, M a finitely generated module, $x \notin \mathrm{z.div}(M)$. Show M is Cohen–Macaulay if and only if M/xM is so.

Proposition **(23.31)**. — *Let $R \to R'$ be a map of Noetherian rings, $\mathfrak{a} \subset R$ an ideal, and M a finitely generated R-module with $M/\mathfrak{a}M \neq 0$. Set $M' := M \otimes_R R'$. Assume R'/R is faithfully flat. Then* $\mathrm{depth}(\mathfrak{a}R', M') = \mathrm{depth}(\mathfrak{a}, M)$.

Proof: By **(23.27)**, there is a finished M-sequence $x_1, \dots, x_r$ in $\mathfrak{a}$. For all i, set $M_i := M/\langle x_1, \dots, x_i\rangle M$ and $M'_i := M'/\langle x_1, \dots, x_i\rangle M'$. By **(8.13)**, we have

$$M'/\mathfrak{a}M' = M/\mathfrak{a}M \otimes_R R' \quad \text{and} \quad M'_i = M_i \otimes_R R'.$$

So $M'/\mathfrak{a}M' \neq 0$ by faithful flatness. Hence $x_1, \dots, x_r$ is an M'-sequence by **(23.25)**.

As $x_1, \dots, x_r$ is finished, $\mathfrak{a} \subset \mathrm{z.div}(M_r)$. So $\mathrm{Hom}_R(R/\mathfrak{a}, M_r) \neq 0$ by **(17.26)**. However, **(9.20)** and **(8.11)** yield

$$\mathrm{Hom}_R(R/\mathfrak{a}, M_r) \otimes_R R' = \mathrm{Hom}_R(R/\mathfrak{a}, M'_r) = \mathrm{Hom}_{R'}(R'/\mathfrak{a}R', M'_r).$$

So $\mathrm{Hom}_{R'}(R'/\mathfrak{a}R', M'_r) \neq 0$ by faithful flatness. So $\mathfrak{a}R' \subset \mathrm{z.div}(M'_r)$ by **(17.26)**. So $x_1, \dots, x_r$ is a finished M'-sequence in $\mathfrak{a}R'$. Thus **(23.28)** yields the assertion. □

Exercise **(23.32)**. — Let A be a Noetherian local ring, and M a nonzero finitely generated module. Prove the following statements:
(1) $\mathrm{depth}(M) = \mathrm{depth}(\widehat{M})$.
(2) M is Cohen–Macaulay if and only if $\widehat{M}$ is Cohen–Macaulay.

Exercise **(23.33)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module with $M/\mathfrak{a}M \neq 0$. Show that there is $\mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)$ with

$$\mathrm{depth}(\mathfrak{a}, M) = \mathrm{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p}).$$

Lemma **(23.34)**. — *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{a}$ another ideal, M a nonzero finitely generated module, and $x \in \mathfrak{m} - \mathrm{z.div}(M)$. Assume $\mathfrak{a} \subset \mathrm{z.div}(M)$. Set $M' := M/xM$. Then there is $\mathfrak{p} \in \mathrm{Ass}(M')$ with $\mathfrak{p} \supset \mathfrak{a}$.*

Proof: By hypothesis, the sequence $0 \to M \xrightarrow{\mu_x} M \to M' \to 0$ is exact. Set $H := \mathrm{Hom}(A/\mathfrak{a}, M)$. Then $H \neq 0$ by **(17.26)** as $\mathfrak{a} \subset \mathrm{z.div}(M)$. Further, H is finitely generated by **(16.20)**. So $H/xH \neq 0$ by Nakayama's Lemma **(10.11)**. Also, $0 \to H \xrightarrow{\mu_x} H \to \mathrm{Hom}(A/\mathfrak{a}, M')$ is exact by **(5.18)**; so $H/xH \subset \mathrm{Hom}(A/\mathfrak{a}, M')$. So $\mathrm{Hom}(A/\mathfrak{a}, M') \neq 0$. But $\mathrm{Supp}(A/\mathfrak{a}) = \mathbf{V}(\mathfrak{a})$ by **(13.31)**. Thus **(17.26)** yields the desired $\mathfrak{p}$. □

Lemma **(23.35)**. — *Let R be a Noetherian ring, M a nonzero finitely generated module, $\mathfrak{p}_0 \in \mathrm{Ass}(M)$, and $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ a chain of primes. Assume that there is no prime $\mathfrak{p}$ with $\mathfrak{p}_{i-1} \subsetneqq \mathfrak{p} \subsetneqq \mathfrak{p}_i$ for any i. Then* $\mathrm{depth}(\mathfrak{p}_r, M) \le r$.

Proof: If $r = 0$, then $\mathfrak{p}_0 \subset \mathrm{z.div}(M)$. So $\mathrm{depth}(\mathfrak{p}_0, M) = 0$, as desired. Induct on r. Assume $r \ge 1$. As $\mathfrak{p}_0 \in \mathrm{Ass}(M)$, we have $\mathfrak{p}_r \in \mathrm{Supp}(M)$ by **(17.17)**; so $M_{\mathfrak{p}_r} \neq 0$. So Nakayama's Lemma **(10.11)** yields $M_{\mathfrak{p}_r}/\mathfrak{p}_r M_{\mathfrak{p}_r} \neq 0$. Further, $\mathrm{depth}(\mathfrak{p}_r, M) \le \mathrm{depth}(M_{\mathfrak{p}_r})$ by **(23.26)**(2). So localizing at $\mathfrak{p}_r$, we may assume R is local and $\mathfrak{p}_r$ is the maximal ideal.

Let $x_1, \dots, x_s$ be a finished M-sequence in $\mathfrak{p}_{r-1}$. Then as $\mathfrak{p}_{r-1} \subset \mathfrak{p}_r$, clearly $M/\mathfrak{p}_{r-1}M \neq 0$. So $s = \mathrm{depth}(\mathfrak{p}_{r-1}, M)$ by **(23.28)**. So by induction $s \le r - 1$. Set $M_s := M/\langle x_1, \dots, x_s\rangle M$. Then $\mathfrak{p}_{r-1} \subset \mathrm{z.div}(M_s)$ by finishedness.

Suppose $\mathfrak{p}_r \subset \mathrm{z.div}(M_s)$. Then $x_1, \dots, x_s$ is finished in $\mathfrak{p}_r$. So $s = \mathrm{depth}(\mathfrak{p}_r, M)$

by **(23.28)**, as desired.

Suppose instead $\mathfrak{p}_r \not\subset \mathrm{z.div}(M_s)$. Then there's $x \in \mathfrak{p}_r - \mathrm{z.div}(M_s)$. So $x_1, \ldots, x_s, x$ is an M-sequence in $\mathfrak{p}_r$. By **(23.34)**, there is $\mathfrak{p} \in \mathrm{Ass}(M_s/xM_s)$ with $\mathfrak{p} \supset \mathfrak{p}_{r-1}$. But $\mathfrak{p} = \mathrm{Ann}(m)$ for some $m \in M_s/xM_s$, so $x \in \mathfrak{p}$. Hence $\mathfrak{p}_{r-1} \subsetneqq \mathfrak{p} \subset \mathfrak{p}_r$. Hence, by hypothesis, $\mathfrak{p} = \mathfrak{p}_r$. Hence $x_1, \ldots, x_s, x$ is finished in $\mathfrak{p}_r$. So **(23.28)** yields $s + 1 = \mathrm{depth}(\mathfrak{p}_r, M)$. Thus $\mathrm{depth}(\mathfrak{p}_r, M) \le r$, as desired. □

Theorem **(23.36)** (Unmixedness). — *Let A be a Noetherian local ring, and M a finitely generated module. Assume M is Cohen–Macaulay. Then M has no embedded primes, and all maximal chains of primes in* $\mathrm{Supp}(M)$ *are of the same length, namely,* $\dim(M)$.

Proof: Given $\mathfrak{p}_0 \in \mathrm{Ass}(M)$, take any maximal chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$. Then $\mathfrak{p}_r$ is the maximal ideal. So $\mathrm{depth}(M) = \mathrm{depth}(\mathfrak{p}_r, M)$. So $\mathrm{depth}(M) \le r$ by **(23.35)**. But $\mathrm{depth}(M) = \dim(M)$ as M is Cohen–Macaulay. And $r \le \dim(M)$ by **(21.1)**. So $r = \dim(M)$. Hence $\mathfrak{p}_0$ is minimal. Thus M has no embedded primes.

Given any maximal chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in $\mathrm{Supp}(M)$, necessarily $\mathfrak{p}_0$ is minimal. So $\mathfrak{p}_0 \in \mathrm{Ass}(M)$ by **(17.18)**. Thus, as above, $r = \dim(M)$, as desired. □

Exercise **(23.37)**. — Prove that a Cohen–Macaulay local ring A is catenary.

Proposition **(23.38)**. — *Let A be a Noetherian local ring, M a finitely generated module. Let $x_1, \ldots, x_n$ be nonunits of A, and set $M_i := M/\langle x_1, \ldots, x_i\rangle M$ for all i. Assume M is Cohen–Macaulay. Then $x_1, \ldots, x_n$ is an M-sequence if and only if it is part of a sop; if so, then M_n is Cohen–Macaulay.*

Proof: First, assume $x_1, \ldots, x_n$ is part of a sop. Induct on n. For $n = 0$, the assertion is trivial. Say $n \ge 1$. By induction $x_1, \ldots, x_{n-1}$ is an M-sequence, and M_{n-1} is Cohen–Macaulay. Now, all maximal chains of primes in $\mathrm{Supp}(M_{n-1})$ have the same length by **(23.36)**, and $\dim(M_n) = \dim(M_{n-1}) - 1$ by **(21.6)**. Hence x_n is in no minimal prime of M_{n-1}. But M_{n-1} has no embedded primes by **(23.36)**. So $x_n \notin \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Ass}(M_{n-1})$. So $x_n \notin \mathrm{z.div}(M_{n-1})$ by **(17.26)**. Thus $x_1, \ldots, x_n$ is an M-sequence. Finally, as M_{n-1} is Cohen–Macaulay, so is M_n by **(23.30)**.

Conversely, assume $x_1, \ldots, x_n$ is an M-sequence. By **(23.27)**, extend it to a finished M-sequence $x_1, \ldots, x_r$. Then $\mathrm{depth}(M_r) = 0$, and M_r is Cohen–Macaulay by **(23.30)** applied recursively. So $\dim(M_r) = 0$. Thus $x_1, \ldots, x_r$ is a sop. □

Proposition **(23.39)**. — *Let A be a Noetherian local ring, M a finitely generated module,* $\mathfrak{p} \in \mathrm{Supp}(M)$. *Set* $s := \mathrm{depth}(\mathfrak{p}, M)$. *Assume M is Cohen–Macaulay. Then $M_\mathfrak{p}$ is a Cohen–Macaulay $A_\mathfrak{p}$-module of dimension s.*

Proof: Induct on s. Assume $s = 0$. Then $\mathfrak{p} \subset \mathrm{z.div}(M)$. So $\mathfrak{p}$ lies in some $\mathfrak{q} \in \mathrm{Ass}(M)$ by **(17.26)**. But $\mathfrak{q}$ is minimal in $\mathrm{Supp}(M)$ by **(23.36)**. So $\mathfrak{q} = \mathfrak{p}$. Hence $\dim(M_\mathfrak{p}) = 0$. Thus $M_\mathfrak{p}$ is a Cohen–Macaulay $A_\mathfrak{p}$-module of dimension 0.

Assume $s \ge 1$. Then there is $x \in \mathfrak{p} - \mathrm{z.div}(M)$. Set $M' := M/xM$, and set $s' := \mathrm{depth}(\mathfrak{p}, M')$. Then $M/\mathfrak{p}M \neq 0$ by **(13.31)**. So $s' = s - 1$ by **(23.29)**, and M' is Cohen–Macaulay by **(23.30)**. Further, $M'_\mathfrak{p} = M_\mathfrak{p}/xM_\mathfrak{p}$ by **(12.22)**. But $x \in \mathfrak{p}$. So $M'_\mathfrak{p} \neq 0$ by Nakayama's Lemma **(10.11)**. So $\mathfrak{p} \in \mathrm{Supp}(M')$. Hence by induction, $M'_\mathfrak{p}$ is a Cohen–Macaulay $A_\mathfrak{p}$-module of dimension $s - 1$.

As $x \notin \mathrm{z.div}(M)$, also $x \notin \mathrm{z.div}(M_\mathfrak{p})$ by **(23.26)**(1). Hence $M_\mathfrak{p}$ is a Cohen–Macaulay $A_\mathfrak{p}$-module by **(23.30)**. Finally, $\dim(M_\mathfrak{p}) = s$ by **(21.5)**. □

Definition **(23.40)**. — Let R be a Noetherian ring, and M a finitely generated module. We call M **Cohen–Macaulay** if $M_\mathfrak{m}$ is a Cohen–Macaulay $R_\mathfrak{m}$-module for every maximal ideal $\mathfrak{m} \in \mathrm{Supp}(M)$. It is equivalent that $M_\mathfrak{p}$ be a Cohen–Macaulay $R_\mathfrak{p}$-module for every $\mathfrak{p} \in \mathrm{Supp}(M)$, because if $\mathfrak{p}$ lies in the maximal ideal $\mathfrak{m}$, then $R_\mathfrak{p}$ is the localization of $R_\mathfrak{m}$ at the prime ideal $\mathfrak{p}R_\mathfrak{m}$ by **(11.28)**, and hence $R_\mathfrak{p}$ is Cohen–Macaulay if $R_\mathfrak{m}$ is by **(23.39)**.

We say R is **Cohen–Macaulay** if R is a Cohen–Macaulay R-module.

Proposition **(23.41)**. — *Let R be a Noetherian ring. Then R is Cohen–Macaulay if and only if the polynomial ring $R[X]$ is Cohen–Macaulay.*

Proof: First, assume $R[X]$ is Cohen–Macaulay. Given a prime $\mathfrak{p}$ of R, set $\mathfrak{P} := \mathfrak{p}R[X] + \langle X\rangle$. Then $\mathfrak{P}$ is prime in $R[X]$ by **(2.18)**. Now, $R[X]/\langle X\rangle = R$ and $\mathfrak{P}/\langle X\rangle = \mathfrak{p}$ owing to **(1.8)**; hence, $R_\mathfrak{P} = R_\mathfrak{p}$ by **(11.29)**(1). Further, **(12.22)** yields $(R[X]/\langle X\rangle)_\mathfrak{P} = R[X]_\mathfrak{P}/\langle X\rangle R[X]_\mathfrak{P}$. Hence $R[X]_\mathfrak{P}/\langle X\rangle R[X]_\mathfrak{P} = R_\mathfrak{p}$. But $R[X]_\mathfrak{P}$ is Cohen–Macaulay by **(23.40)**, and X is plainly a nonzerodivisor; so $R_\mathfrak{p}$ is Cohen–Macaulay by **(23.30)**. Thus R is Cohen–Macaulay.

Conversely, assume R is Cohen–Macaulay. Given a maximal ideal $\mathfrak{M}$ of $R[X]$, set $\mathfrak{m} := \mathfrak{M} \cap R$. Then $R[X]_\mathfrak{M} = (R[X]_\mathfrak{m})_\mathfrak{M}$ by **(11.29)**(1), and $R[X]_\mathfrak{m} = R_\mathfrak{m}[X]$ by **(11.30)**. But $R_\mathfrak{m}$ is Cohen–Macaulay. Thus, to show $R[X]_\mathfrak{M}$ is Cohen–Macaulay, replace R by $R_\mathfrak{m}$, and so assume R is local with maximal ideal $\mathfrak{m}$.

As $\mathfrak{M}(R/\mathfrak{m})[X]$ is maximal, it contains a nonzero polynomial $\overline{f}$. As $R/\mathfrak{m}$ is a field, we may take $\overline{f}$ monic. Lift $\overline{f}$ to a monic polynomial $f \in \mathfrak{M}$. Set $B := R[X]/\langle f\rangle$. Then B is a free, module-finite extension of R by **(10.25)**. So $\dim(R) = \dim(B)$ by **(15.12)**. Plainly $\dim(B) \ge \dim(B_\mathfrak{M})$. So $\dim(R) \ge \dim(B_\mathfrak{M})$.

Further, B is flat over R by **(9.7)**. And $B_\mathfrak{M}$ is flat over B by **(12.21)**. So $B_\mathfrak{M}$ is flat over R by **(9.12)**. So any R-sequence in $\mathfrak{m}$ is a $B_\mathfrak{M}$-sequence by **(23.25)** as $B_\mathfrak{M}/\mathfrak{m}B_\mathfrak{M} \neq 0$. Hence $\mathrm{depth}(B_\mathfrak{M}) \ge \mathrm{depth}(R)$.

But $\mathrm{depth}(R) = \dim(R)$ and $\dim(R) \ge \dim(B_\mathfrak{M})$. So $\mathrm{depth}(B_\mathfrak{M}) \ge \dim(B_\mathfrak{M})$. But the opposite inequality holds by **(23.5)**. Thus $B_\mathfrak{M}$ is Cohen–Macaulay. But $B_\mathfrak{M} = R[X]_\mathfrak{M}/\langle f\rangle R[X]_\mathfrak{M}$ by **(12.22)**. And f is monic, so a nonzerodivisor. So $R[X]_\mathfrak{M}$ is Cohen–Macaulay by **(23.30)**. Thus $R[X]$ is Cohen–Macaulay. □

Definition **(23.42)**. — A ring R is called **universally catenary** if every finitely generated R-algebra is catenary.

Theorem **(23.43)**. — *A Cohen–Macaulay ring R is universally catenary.*

Proof: Clearly any quotient of a catenary ring is catenary, as chains of primes can be lifted by **(1.9)**. So it suffices to prove that, for any n, the polynomial ring P in n variables over R is catenary.

Notice P is Cohen–Macaulay by induction on n, as $P = R$ if $n = 0$, and the induction step holds by **(23.41)**. Now, given nested primes $\mathfrak{q} \subset \mathfrak{p}$ in P, put $\mathfrak{p}$ in a maximal ideal $\mathfrak{m}$. Then any chain of primes from $\mathfrak{q}$ to $\mathfrak{p}$ corresponds to a chain from $\mathfrak{q}P_\mathfrak{m}$ to $\mathfrak{p}P_\mathfrak{m}$ by **(11.20)**. But $P_\mathfrak{m}$ is Cohen–Macaulay, so catenary by **(23.37)**. Thus the assertion holds. □

Example **(23.44)**. — Trivially, a field is Cohen–Macaulay. Plainly, a domain of dimension 1 is Cohen–Macaulay. By **(23.20)**, a normal domain of dimension 2 is Cohen–Macaulay. Thus these rings are all universally catenary by **(23.43)**. In particular, we recover **(15.16)**.

Proposition **(23.45)**. — *Let A be a regular local ring of dimension n, and M a finitely generated module. Assume M is Cohen–Macaulay of dimension n. Then M is free.*

Proof: Induct on n. If $n=0$, then A is a field by **(21.20)**, and so M is free.

Assume $n \ge 1$. Let $t \in A$ be an element of a regular system of parameters. Then $A/\langle t\rangle$ is regular of dimension $n-1$ by **(21.23)**. As M is Cohen–Macaulay of dimension n, any associated prime $\mathfrak{q}$ is minimal in A by **(23.36)**; so $\mathfrak{q} = \langle 0\rangle$ as A is a domain by **(21.24)**. Hence t is a nonzerodivisor on M by **(17.15)**. So M/tM is Cohen–Macaulay of dimension $n-1$ by **(23.30)** and **(21.5)**. Hence by induction, M/tM is free, say of rank r.

Let k be the residue field of A. Then $M \otimes_A k = (M/tM) \otimes_{A/\langle t\rangle} k$ by **(8.16)**(1). So $r = \operatorname{rank}(M \otimes_A k)$.

Set $\mathfrak{p} := \langle t\rangle$. Then $A_{\mathfrak{p}}$ is a DVR by **(23.10)**. Moreover, $M_{\mathfrak{p}}$ is Cohen–Macaulay of dimension 1 by **(23.39)** as $\operatorname{depth}(\langle t\rangle, M) = 1$. So $M_{\mathfrak{p}}$ is torsionfree by **(23.16)**. Therefore $M_{\mathfrak{p}}$ is flat by **(9.28)**, so free by **(10.20)**. Set $s := \operatorname{rank}(M_{\mathfrak{p}})$.

Let $k(\mathfrak{p})$ be the residue field of $A_{\mathfrak{p}}$. Then $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} k(\mathfrak{p}) = M_{\mathfrak{p}}/tM_{\mathfrak{p}}$ by **(8.16)**(1). Moreover, $M_{\mathfrak{p}}/tM_{\mathfrak{p}} = (M/tM)_{\mathfrak{p}}$ by **(12.22)**. So $r = s$.

Set $K := \operatorname{Frac}(A)$. Then $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K = M \otimes_A K$ by **(11.29)**(1). Hence $M \otimes_A K$ has rank r. Thus M is free by **(14.14)**. □

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 the trace pairing of the extension. We conclude that a ring of algebraic integers is a Dedekind domain and that, if a domain is algebra finite over a field of characteristic 0, then in the fraction field or in any algebraic extension of it, the integral closure is module finite over the domain and is algebra finite 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, **(10.33)**; and R is of dimension 1 since every nonzero prime is maximal by **(2.25)**.

On the other hand, any local Dedekind domain is a DVR by **(23.10)**.

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 [**2**, Prp. (6.14), p. 412]; so R is normal by **(10.26)**. Also, $\dim(R) = \dim(\mathbb{Z})$ by **(15.12)**; so $\dim(R) = 1$. Finally, R is Noetherian by **(16.12)** 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 **(23.21)**, 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 subset.

(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 $\dim(R) \ge 1$. 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 subset. 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 **(23.10)**.

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, $\dim(R) \ge 1$; 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 $\mathfrak a \ne 0$ 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, $\{\mathfrak p_1, \dots, \mathfrak p_r\} = \mathrm{Ass}(R/\mathfrak a)$ and $\mathfrak q_i = \mathfrak a R_{\mathfrak p_i} \cap R$ for each i.*

Proof: The Lasker–Noether Theorem, **(18.21)**, yields an irredundant primary decomposition $\mathfrak a = \bigcap \mathfrak q_i$. Say $\mathfrak q_i$ is $\mathfrak p_i$-primary. Then by **(18.19)** the $\mathfrak p_i$ are distinct and $\{\mathfrak p_i\} = \mathrm{Ass}(R/\mathfrak a)$.

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 **(3.32)**. Hence $\mathfrak p_i^{n_i} \subset \mathfrak m$. So $\mathfrak p_i \subset \mathfrak m$ by **(2.2)**. But $0 \ne \mathfrak a \subset \mathfrak p_i$; 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, **(1.14)**, 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 $\mathfrak p_i$ lie in $\mathrm{Ass}(R/\mathfrak a)$ by **(17.18)**. 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 **(18.19)**. So the $\mathfrak p_i$ are unique by the First Uniqueness Theorem, **(18.20)**, and $\mathfrak q_i = \mathfrak a R_{\mathfrak p_i} \cap R$ by the Second Uniqueness Theorem, **(18.25)**, and by **(12.17)**(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 $m_i := v_{\mathfrak p_i}(\mathfrak a)$. 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 **(18.23)**. 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 $\mathfrak m \ne 0$. So $\mathfrak m \ne \mathfrak m^2$ 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 **(11.19)**(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 **(23.10)**. 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)** (Artin Character). — *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 $m \ge 1$ minimal. Now, $\sigma_i \ne 0$ as $\sigma_i \colon G \to L^\times$; so $m \ge 2$. Since $\sigma_1 \ne \sigma_2$, there's an $x \in G$ with $\sigma_1(x) \ne \sigma_2(x)$. 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 $b_i := a_i\bigl(1 - \sigma_i(x)/\sigma_1(x)\bigr)$. Then

$$\sum_{i=1}^m b_i\sigma_i = \sum_{i=1}^m a_i\sigma_i - \frac{1}{\sigma_1(x)}\sum_{i=1}^m a_i\sigma_i(x)\sigma_i = 0.$$

But $b_1 = 0$ and $b_2 \ne 0$, 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**:

$$L \times L \to K \quad \text{by} \quad (x, y) \mapsto \mathrm{tr}(xy). \qquad \textbf{(24.15.1)}$$

It is nondegenerate for this reason. As tr is nonzero, there is $z \in L$ with $\mathrm{tr}(z) \ne 0$. Now, given $x \in L^\times$, set $y := z/x$. Then $\mathrm{tr}(xy) \ne 0$, 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, and is Noetherian.*

Proof: Let L_1 be the Galois closure of L/K, and R'_1 the integral closure of R in L_1. Let $z_1, \dots, z_n \in L_1$ form a K-basis. Using **(11.25)**, write $z_i = y_i/a_i$ with $y_i \in R'_1$ and $a_i \in R$. Clearly, $y_1, \dots, y_n$ form a basis of L_1/K contained in R'_1.

Let $x_1, \dots, x_n$ form the dual basis with respect to the Trace Pairing, **(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

$$\mathrm{tr}(by_j) = \mathrm{tr}\Bigl(\sum_i c_ix_iy_j\Bigr) = \sum_i c_i\,\mathrm{tr}(x_iy_j) = c_j \quad \text{for each } j.$$

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 module finite over R-module and Noetherian owing to **(16.19)**. □

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 **(16.19)**. Second, R' is normal by **(10.32)**. Finally, $\dim(R') = \dim(R)$ by **(15.12)**, 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 on Finiteness of Integral Closure). — *Let k be a field of characteristic 0, and R an algebra-finite domain over k. Set $K := \mathrm{Frac}(R)$. Let L/K be a finite field extension (possibly $L = K$), and R' the integral closure of R in L. Then R' is module finite over R and is algebra finite over k.*

Proof: By the Noether Normalization Lemma, **(15.1)**, R is module finite over a polynomial subring P. Then P is normal by Gauss's Theorem, **(10.33)**, and Noetherian by the Hilbert Basis Theorem, **(16.12)**; also, $L/\mathrm{Frac}(P)$ is a finite field extension, which is separable as k is of characteristic 0. Thus R' is module finite over P by **(24.17)**, and so R' is plainly algebra finite over k. □

(24.21) (*Other cases*). — In **(24.18)**, even if L/K is inseparable, the integral closure R' of R in L is still Dedekind; see **(26.18)**.

However, Akizuki constructed an example of a DVR R and a finite inseparable extension $L/\mathrm{Frac}(R)$ such that the integral closure of R is a DVR, but is not module finite over R. The construction is nicely explained in [**11**, 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 [**4**, (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 ordinary ideals have an invertible fractional ideal as their quotient. We characterize Dedekind domains as those domains whose ordinary 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 torsionfree 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 $K := \mathrm{Frac}(R)$. We call an R-submodule M of K a **fractional ideal**. 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:

$$MN := \{ \textstyle\sum x_i y_i \mid x_i \in M \text{ and } y_i \in N \} \quad \text{and} \quad (M : N) := \{ z \in K \mid zN \subset M \}.$$

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:

$$\pi\colon M \otimes N \twoheadrightarrow MN \quad \text{and} \quad \varphi\colon (M : N) \xrightarrow{\sim} \mathrm{Hom}(N, M).$$

Proposition **(25.3)**. — *Let R be a domain, and $K := \mathrm{Frac}(R)$. Consider these finiteness conditions on a fractional ideal M:*

(1) *There exist ordinary 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 ordinary, and $M = (xM : xR)$; thus (1) holds.

Assume (4) holds. Say $y_1/x_1, \ldots, y_n/x_n \in K^\times$ 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 $y_1, \ldots, y_n$. Then $y_1/x, \ldots, y_n/x$ generate M. Thus (4) holds.

Finally, assume all four conditions are equivalent for every M. If M is ordinary, 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 subset. 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. □

Exercise **(25.9)**. — Let R be a domain, M and N fractional ideals.

(1) Assume N is invertible, and show that $(M:N) = M \cdot N^{-1}$.

(2) Show that both M and N are invertible if and only if their product MN is, and that if so, then $(MN)^{-1} = N^{-1}M^{-1}$.

Lemma **(25.10)**. — *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 **(25.11)**. — *Let A be a local domain, M a fractional ideal. Then 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 invertible by **(25.7)**. □

Exercise **(25.12)**. — Let R be a UFD. Show that a fractional ideal M is invertible if and only if M is principal and nonzero.

Theorem **(25.13)**. — *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 **(25.10)**. Let S be a multiplicative subset. 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 **(25.11)**, 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 **(13.35)** yields $\mathfrak{a} = R$, as desired. □

Theorem **(25.14)**. — *Let R be a Dedekind domain, $\mathfrak{a}$, $\mathfrak{b}$ nonzero ordinary ideals, $M := (\mathfrak{a} : \mathfrak{b})$. Then M is invertible, and has a unique factorization into powers of primes $\mathfrak{p}$: if $v_\mathfrak{p}$ denotes the valuation of $R_\mathfrak{p}$ and if $\mathfrak{p}^v := (\mathfrak{p}^{-1})^{-v}$ when $v < 0$, then*

$$M = \prod \mathfrak{p}^{v_\mathfrak{p}(M)} \quad \textit{where} \quad v_\mathfrak{p}(M) := \min\{\, v_\mathfrak{p}(x) \mid x \in M \,\}.$$

Further, $v_\mathfrak{p}(M) = \min\{v_\mathfrak{p}(x_i)\}$ 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 $xM \subset R$. Also, each $R_\mathfrak{p}$ is a DVR by **(24.7)**. So $xM_\mathfrak{p}$ is principal by **(23.1.3)**. Thus M is invertible by **(25.13)**.

The Main Theorem of Classical Ideal Theory, **(24.10)**, yields $xM = \prod \mathfrak{p}^{v_\mathfrak{p}(xM)}$ and $xR = \prod \mathfrak{p}^{v_\mathfrak{p}(x)}$. But $v_\mathfrak{p}(xM) = v_\mathfrak{p}(x) + v_\mathfrak{p}(M)$. Thus **(25.9)** yields

$$M = (xM : xR) = \prod \mathfrak{p}^{v_\mathfrak{p}(x) + v_\mathfrak{p}(M)} \cdot \prod \mathfrak{p}^{-v_\mathfrak{p}(x)} = \prod \mathfrak{p}^{v_\mathfrak{p}(M)}.$$

Further, given $x \in M$, say $x = \sum_{i=1}^n a_i x_i$ with $a_i \in R$. Then **(23.1.1)** yields

$$v_\mathfrak{p}(x) \ge \min\{v_\mathfrak{p}(a_i x_i)\} \ge \min\{v_\mathfrak{p}(x_i)\}$$

by induction on n. Thus $v_\mathfrak{p}(M) = \min\{v_\mathfrak{p}(x_i)\}$. □

Exercise **(25.15)**. — Show that a ring is a PID if and only if it's a Dedekind domain and a UFD.

(25.16) (*Invertible modules*). — Let R be an arbitrary ring. We call a module M **invertible** if there is another module N with $M \otimes N \simeq R$.

Up to (noncanonical) isomorphism, N is unique if it exists: if $N' \otimes M \simeq R$, then

$$N = R \otimes N \simeq (N' \otimes M) \otimes N = N' \otimes (M \otimes N) \simeq N' \otimes R = N'.$$

Exercise **(25.17)**. — 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 **(25.18)**. — 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 $M \otimes \operatorname{Hom}(M, R) = R$.

Proposition **(25.19)**. — *Let R be a domain, M a fractional ideal. Then the following conditions are equivalent:*

(1) *M is an invertible fractional ideal.*
(2) *M is an invertible abstract module.*
(3) *M is a projective abstract module.*

Proof: Assume (1). Then M is locally principal by **(25.13)**. So **(25.6)** yields $M \otimes M^{-1} = MM^{-1}$ by (1). But $MM^{-1} = 1$. Thus (2) holds.

If (2) holds, then M is locally free of rank 1 by **(25.18)**; so **(13.51)** yields (3).

Finally, assume (3). By **(5.23)**, there's an M' with $M \oplus M' \simeq R^{\oplus\Lambda}$. Let $\rho\colon R^{\oplus\Lambda} \to M$ be the projection, and set $x_\lambda := \rho(e_\lambda)$ where e_λ is the standard basis vector. Define $\varphi_\lambda\colon M \hookrightarrow R^{\oplus\Lambda} \to R$ to be the composition of the injection with the projection φ_λ on the λth factor. Then given $x \in M$, we have $\varphi_\lambda(x) = 0$ for almost all λ and $x = \sum_{\lambda\in\Lambda} \varphi_\lambda(x)x_\lambda$.

Fix a nonzero $y \in M$. For $\lambda \in \Lambda$, set $q_\lambda := \frac{1}{y}\varphi_\lambda(y) \in \operatorname{Frac}(R)$. Set $N := \sum Rq_\lambda$. Given any nonzero $x \in M$, say $x = a/b$ and $y = c/d$ with $a, b, c, d \in R$. Then $a, c \in M$; whence, $ad\varphi_\lambda(y)\varphi_\lambda(ac) = bc\varphi_\lambda(x)$. 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 $M \cdot N = R$. Thus (1) holds. □

Theorem **(25.20)**. — *Let R be a domain. Then the following are equivalent:*

(1) *R is a Dedekind domain or a field.*
(2) *Every nonzero ordinary ideal $\mathfrak{a}$ is invertible.*
(3) *Every nonzero ordinary ideal $\mathfrak{a}$ is projective.*
(4) *Every nonzero ordinary ideal $\mathfrak{a}$ is finitely generated and flat.*

Proof: Assume R is not a field; otherwise, (1)–(4) hold trivially.

If R is Dedekind, then **(25.14)** yields (2) since $\mathfrak{a} = (\mathfrak{a} : R)$.

Assume (2). Then $\mathfrak{a}$ is finitely generated by **(25.10)**. Thus R is Noetherian. Let $\mathfrak{p}$ be any nonzero prime of R. Then by hypothesis, $\mathfrak{p}$ is invertible. So by **(25.13)**, $\mathfrak{p}$ is locally principal. So $R_\mathfrak{p}$ is a DVR by **(23.10)**. Hence R is Dedekind by **(24.7)**. Thus (1) holds. Thus (1) and (2) are equivalent.

By **(25.19)**, (2) and (3) are equivalent. But (2) implies that R is Noetherian by **(25.10)**. Thus (3) and (4) are equivalent by **(16.19)** and **(13.51)**. □

Theorem **(25.21)**. — *Let R be a Noetherian domain, but not a field. Then R is Dedekind if and only if every torsionfree module is flat.*

Proof: (Of course, as R is a domain, every flat module is torsionfree by **(9.28)**.)

Assume R is Dedekind. Let M be a torsionfree module, $\mathfrak{m}$ a maximal ideal. Let's see that $M_\mathfrak{m}$ is torsionfree 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 torsionfree. 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 torsionfree.

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 **(9.28)**. But $\mathfrak{m}$ is arbitrary. Thus by **(13.46)**, M is flat over R.

Conversely, assume every torsionfree module is flat. In particular, every nonzero ordinary ideal is flat. But R is Noetherian. Thus R is Dedekind by **(25.20)**. □

(25.22) (*The Picard Group*). — Let R be a ring. We denote the collection of isomorphism classes of invertible modules by $\operatorname{Pic}(R)$. By **(25.17)**, every invertible module is finitely generated, so isomorphic to a quotient of R^n for some integer n. Hence, $\operatorname{Pic}(R)$ is a set. Further, $\operatorname{Pic}(R)$ is, clearly, a group under tensor product

with the class of R as identity. We call $\operatorname{Pic}(R)$ the **Picard Group** of R.

Assume R is a domain, not a field. Set $K := \operatorname{Frac}(R)$. Given an invertible abstract 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 **(12.17)** 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 **(25.17)**. Hence $\mu_x\colon M_\mathfrak{m} \to M_\mathfrak{m}$ is injective. Therefore, $\mu_x\colon M \to M$ is injective by **(13.43)**. 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.

Hence, **(25.19)** implies M is also invertible as a fractional ideal.

The invertible fractional ideals N, clearly, form a group $\mathcal{F}(R)$. Sending an N to its isomorphism class yields a map $\kappa\colon \mathcal{F}(R) \to \operatorname{Pic}(R)$ by **(25.16)**. 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 **(25.13)**, finitely generated and nonzero, so of the form $(\mathfrak{a} : \mathfrak{b})$ where $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ordinary ideals by **(25.3)**. Conversely, by **(25.14)** and **(25.20)**, 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 **(25.15)**, a PID. See [**2**, 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 a subring of a field such that the reciprocal of any element outside the subring lies in it. Valuation rings are normal local domains. They are maximal under *domination of local rings*; that is, one contains the other, and the inclusion map is a local homomorphism. Given any domain, its normalization is equal to the intersection of all the valuation rings containing it. Given a 1-dimensional Noetherian domain and a finite extension of its fraction field with a proper subring containing the domain, that subring too is 1-dimensional and Noetherian, this is the Krull–Akizuki Theorem. So normalizing a Dedekind domain in any finite extension of its fraction field yields 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 **(3.6)**. 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 of K, and $V \subset W \subset K$ a subring. Prove that W is also a valuation ring of K, that its maximal ideal $\mathfrak{p}$ lies in V, that $V/\mathfrak{p}$ is a valuation ring of the field $W/\mathfrak{p}$, and that $W = V_{\mathfrak{p}}$.

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 $m \le n$. 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. □

(26.7) (*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 $\mathfrak{n} \cap A = \mathfrak{m}$; in other words, the inclusion map $\varphi\colon A \hookrightarrow B$ is a local homomorphism.

Proposition **(26.8)**. — *Let K be a field, A any local subring. Then A is dominated by a valuation ring V of K with algebraic residue field extension.*

Proof: Let $\mathfrak{m}$ be the maximal ideal of A. Let $\mathcal{S}$ be the set of pairs $(R, \mathfrak{n})$ where $R \subset K$ is a subring containing A and where $\mathfrak{n} \subset R$ is a maximal ideal with $\mathfrak{n} \cap A = \mathfrak{m}$ and with $R/\mathfrak{n}$ an algebraic extension of $A/\mathfrak{m}$. Then $(A, \mathfrak{m}) \in \mathcal{S}$. Order $\mathcal{S}$ as follows: $(R, \mathfrak{n}) \le (R', \mathfrak{n}')$ if $R \subset R'$ and $\mathfrak{n} = \mathfrak{n}' \cap R$. Let $(R_\lambda, \mathfrak{n}_\lambda)$ form a totally ordered subset. Set $B := \bigcup R_\lambda$ and $\mathfrak{N} = \bigcap \mathfrak{n}_\lambda$. Plainly $\mathfrak{N} \cap R_\lambda = \mathfrak{n}_\lambda$ and $B/\mathfrak{N} = \bigcap R_\lambda/\mathfrak{n}_\lambda$ for all λ. So any $y \in B/\mathfrak{N}$ is in $R_\lambda/\mathfrak{n}_\lambda$ for some λ. Hence $B/\mathfrak{N}$ is a field and is algebraic over $A/\mathfrak{m}$. Thus by Zorn's Lemma, $\mathcal{S}$ has a maximal element, say $(V, \mathfrak{M})$.

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 $1 \notin \mathfrak{M}V''$. Say $1 \notin \mathfrak{M}V'$. Then $\mathfrak{M}V'$ is proper, so it is contained in a maximal ideal $\mathfrak{M}'$ of V'. Since $\mathfrak{M}' \cap V \supset \mathfrak{M}$ and $V \cap \mathfrak{M}'$ is proper, $\mathfrak{M}' \cap V = \mathfrak{M}$. Further $V'/\mathfrak{M}'$ is generated as a ring over $V/\mathfrak{M}$ by the residue x' of x. Hence x' is algebraic over $V/\mathfrak{M}$; otherwise, $V'/\mathfrak{M}'$ would be a polynomial ring, so not a field. Hence $(V', \mathfrak{M}') \in \mathcal{S}$, and $(V', \mathfrak{M}') \ge (V, \mathfrak{M})$. By maximality, $V = V'$; so $x \in V$. Thus V is a valuation ring of K. So V is local, and $\mathfrak{M}$ is its unique maximal ideal. Finally, $(V, \mathfrak{M}) \in \mathcal{S}$; so V dominates A with algebraic residue field extension. □

Exercise **(26.9)**. — Let K be a field, $\mathcal{S}$ the set of local subrings ordered by domination. Show that the valuation rings of K are the maximal elements of $\mathcal{S}$.

Theorem **(26.10)**. — *Let R be any subring of a field K. Then the integral closure $\overline{R}$ 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 with algebraic residue field extension suffice.*

Proof: Every valuation ring V is normal by **(26.5)**. So if $V \supset R$, then $V \supset \overline{R}$. Thus $\left(\bigcap_{V \supset R} V\right) \supset \overline{R}$.

To prove the opposite inclusion, take any $x \in K - \overline{R}$. 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,

$$1/y = a_0 y^n + a_1 y^{n-1} + \cdots + a_n \quad \text{with} \quad a_\lambda \in R.$$

Multiplying by x^n yields $x^{n+1} - a_n x^n - \cdots - a_0 = 0$. So $x \in \overline{R}$, 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 $y \in \mathfrak{m}$. Its kernel is $\mathfrak{m} \cap R$, so $\mathfrak{m} \cap R$ is a maximal ideal of R. By **(26.8)**, there is a valuation ring V that dominates $R[y]_{\mathfrak{m}}$ with algebraic residue field extension; whence, if R is local, then V also dominates R, and the residue field of $R[y]_{\mathfrak{m}}$ is equal to that of R. But $y \in \mathfrak{m}$; so $x = 1/y \notin V$, as desired. □

(26.11) (*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 $K := \mathrm{Frac}(V)$ 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:

$$v(xy) = v(x) + v(y). \qquad \textbf{(26.11.1)}$$

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 $x, y \in K^\times$,

$$v(x+y) \ge \min\{v(x),\, v(y)\} \quad \text{if} \quad x \ne -y. \tag{26.11.2}$$

Indeed, say $v(x) \ge v(y)$. Then $z := x/y \in V$. So $v(z+1) \ge 0$. Hence

$$v(x+y) = v(z+1) + v(y) \ge v(y) = \min\{v(x), v(y)\},$$

Note that **(26.11.1)** and **(26.11.2)** 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 **(26.11.2)**. Set

$$V := \{x \in K^\times \mid v(x) \ge 0\} \cup \{0\}.$$

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 **(26.12)**. — Fix totally ordered additive abelian group Γ, and a field k. Form the k-vector space R with basis the symbols X^a for $a \in \Gamma$. Define $X^aX^b := X^{a+b}$, 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

$$v\big(\textstyle\sum r_a X^a\big) := \min\{a \mid r_a \ne 0\}.$$

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 $v(x) \le a$ or $v(y) \le a$. Thus $v(x+y) \ge \min\{v(x),\, v(y)\}$.

Set $K := \operatorname{Frac}(R)$, and extend v to a map $v\colon K^\times \to \Gamma$ by $v(x/y) := v(x) - v(y)$ if $y \ne 0$. Clearly v is well defined, surjective, and a homomorphism. Further, for $x, y \in K^\times$, clearly $v(x+y) \ge \min\{v(x),\, v(y)\}$. Thus v is a valuation with group Γ.

Set $R' := \{x \in R \mid v(x) \ge 0\}$ 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 **(26.13)**. — *Let v be a valuation of a field K, and $x_1, \dots, x_n \in K^\times$ with $n \ge 2$. Set $m := \min\{v(x_i)\}$.*

(1) *If $n = 2$ and if $v(x_1) \ne v(x_2)$, 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 $i \ne j$.*

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,

$$0 = v(1) = v(z+1-z) \ge \min\{v(z+1),\ v(-z)\} \ge 0.$$

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 $i \le k$ and $v(x_i) > m$ for $i > k$. By induction, **(26.11.2)** yields $v(x_{k+1} + \cdots + x_n) \ge \min_{i>k}\{v(x_i)\}$. 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 **(26.14)**. — 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 **(26.15)**. — 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 **(26.16)**. — *Let R be a 1-dimensional Noetherian domain, K its fraction field, M a torsionfree module, and $x \in R$ nonzero. Then $\ell(R/xR) < \infty$. Further,*

$$\ell(M/xM) \le \dim_K(M \otimes_R K)\, \ell(R/xR), \tag{26.16.1}$$

with equality if M is finitely generated.

Proof: Set $r := \dim_K(M \otimes_R K)$. If $r = \infty$, then **(26.16.1)** 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 torsionfree. 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, **(19.9)**; it yields $\ell\big(N'\big) = \ell(N/xN)$.

Since M is torsionfree, $\mu_x\colon M \to M$ is injective. Consider this commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & R^r \arrow[r, "\alpha"] \arrow[d, "\mu_x"'] & M \arrow[r] \arrow[d, "\mu_x"'] & N \arrow[r] \arrow[d, "\mu_x"'] & 0 \\
0 \arrow[r] & R^r \arrow[r, "\alpha"] & M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

Apply the snake lemma **(5.13)**. 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 **(26.16.1)** when M is finitely generated.

Second, assume M is arbitrary, but **(26.16.1)** 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 $r \ge \dim_K(M'_K)$. Therefore,

$$\ell(M'/xM') \ge \ell(H) > r\,\ell(R/xR) \ge \dim_K(M'_K)\,\ell\big(R/xR\big).$$

However, together these inequalities contradict the first case with M' for M. □

Theorem **(26.17)** (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, **(26.16)** yields $\ell(R/a_0R) < \infty$.

Clearly, R' is a domain, so a torsionfree R-module. Further, $R' \otimes_R K \subset K'$; hence, $\dim_K(R' \otimes_R K) < \infty$. Therefore, **(26.16)** 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, $\ell_{R''}R'' \le \ell_R R''$. 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 **(26.18)**. — *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 **(26.17)**. Thus R' is Dedekind by **(24.1)**. □

Corollary **(26.19)**. — *Let K'/K be a field extension, V' a valuation ring of K' not containing K. Set $V := V' \cap K$. Then V is a DVR if V' is, and the converse holds if K'/K is finite.*

Proof: It follows easily from **(26.1)** that V is a valuation ring, and from **(26.11)** 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, $V' \not\supset K$, so $V' \subsetneq K'$. Hence, V' is Noetherian by **(26.17)**, so a DVR by **(26.15)**(2). □

Exercise **(26.20)**. — Let R be a Noetherian domain, $K := \operatorname{Frac}(R)$, and L a finite extension field (possibly $L = K$). Prove the integral closure $\overline{R}$ of R in L is the intersection of all DVRs V of L containing R by modifying the proof of **(26.10)**: show y is contained in a height-1 prime $\mathfrak{p}$ of $R[y]$ and apply **(26.18)** to $R[y]_{\mathfrak{p}}$.

Solutions

1. Rings and Ideals

Exercise **(1.5)**. — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Set $\mathfrak{a}^e := \varphi(\mathfrak{a})R'$ and $\mathfrak{b}^c := \varphi^{-1}(\mathfrak{b})$. Prove these statements:

(1) Then $\mathfrak{a}^{ec} \supset \mathfrak{a}$ and $\mathfrak{b}^{ce} \subset \mathfrak{b}$. (2) Then $\mathfrak{a}^{ece} = \mathfrak{a}^e$ and $\mathfrak{b}^{cec} = \mathfrak{b}^c$.

(3) If $\mathfrak{b}$ is an extension, then $\mathfrak{b}^c$ is the largest ideal of R with extension $\mathfrak{b}$.

(4) If two extensions have the same contraction, then they are equal.

Solution: For (1), given $x \in \mathfrak{a}$, note $\varphi(x) = x \cdot 1 \in \mathfrak{a}R'$. So $x \in \varphi^{-1}(\mathfrak{a}R')$, or $x \in \mathfrak{a}^{ec}$. Thus $\mathfrak{a} \subset \mathfrak{a}^{ec}$. Next, $\varphi(\varphi^{-1}\mathfrak{b}) \subset \mathfrak{b}$. But $\mathfrak{b}$ is an ideal of R'. So $\varphi(\varphi^{-1}\mathfrak{b})R' \subset \mathfrak{b}$, or $\mathfrak{b}^{ce} \subset \mathfrak{b}$. Thus (1) holds.

For (2), note $\mathfrak{a}^{ece} \subset \mathfrak{a}^e$ by (1) applied with $\mathfrak{b} := \mathfrak{a}^e$. But $\mathfrak{a} \subset \mathfrak{a}^{ec}$ by (1); so $\mathfrak{a}^e \subset \mathfrak{a}^{ece}$. Thus $\mathfrak{a}^e = \mathfrak{a}^{ece}$. Similarly, $\mathfrak{b}^{cec} \supset \mathfrak{b}^c$ by (1) applied with $\mathfrak{a} := \mathfrak{b}^c$. But $\mathfrak{b}^{ce} \subset \mathfrak{b}$ by (1); so $\mathfrak{b}^{cec} \subset \mathfrak{b}^c$. Thus $\mathfrak{b}^{cec} = \mathfrak{b}^c$. Thus (2) holds.

For (3), say $\mathfrak{b} = \mathfrak{a}^e$. Then $\mathfrak{b}^{ce} = \mathfrak{a}^{ece}$. But $\mathfrak{a}^{ece} = \mathfrak{a}^e$ by (2). Hence $\mathfrak{b}^c$ has extension $\mathfrak{b}$. Further, it's the largest such ideal, as $\mathfrak{a}^{ec} \supset \mathfrak{a}$ by (1). Thus (3) holds.

For (4), say $\mathfrak{b}_1^c = \mathfrak{b}_2^c$ for extensions $\mathfrak{b}_i$. Then $\mathfrak{b}_i^{ce} = \mathfrak{b}_i$ by (3). Thus (4) holds. □

Exercise **(1.7)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and $P := R[X_1, \ldots, X_n]$ the polynomial ring. Prove $P/\mathfrak{a}P = (R/\mathfrak{a})[X_1, \ldots, X_n]$.

Solution: The two R-algebras are equal, as they have the same UMP: each is universal among R-algebras R' with distinguished elements $x_1, \ldots, x_n$ and with $\mathfrak{a}R' = 0$. Namely, the structure map $\varphi\colon R \to R'$ factors through a unique map $\pi\colon P \to R'$ such that $\pi(X_i) = x_i$ for all i by **(1.3)**; then π factors through a unique map $P/\mathfrak{a}P \to R'$ as $\mathfrak{a}R' = 0$ by **(1.6)**. On the other hand, φ factors through a unique map $\psi\colon R/\mathfrak{a} \to R'$ as $\mathfrak{a}R' = 0$ by **(1.6)**; then ψ factors through a unique map $(R/\mathfrak{a})[X_1, \ldots, X_n] \to R'$ such that $\pi(X_i) = x_i$ for all i by **(1.3)**. □

Exercise **(1.10)**. — Let R be ring, and $P := R[X_1, \ldots, X_n]$ the polynomial ring. Let $m \le n$ and $a_1, \ldots, a_m \in R$. Set $\mathfrak{p} := \langle X_1 - a_1, \ldots, X_m - a_m \rangle$. Prove that $P/\mathfrak{p} = R[X_{m+1}, \ldots, X_n]$.

Solution: First, assume $m = n$. Set $P' := R[X_1, \ldots, X_{n-1}]$ and

$$\mathfrak{p}' := \langle X_1 - a_1, \ldots, X_{n-1} - a_{n-1} \rangle \subset P'.$$

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 **(1.7)**. Thus $P/\mathfrak{p}'P = R[X_n]$.

We have $P/\mathfrak{p} = (P/\mathfrak{p}'P)\big/\mathfrak{p}(P/\mathfrak{p}'P)$ by **(1.9)**. 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 **(1.8)**.

In general, $P = (R[X_1, \ldots, X_m])[X_{m+1}, \ldots, X_n]$. Thus $P/\mathfrak{p} = R[X_{m+1}, \ldots, X_n]$ by **(1.7)**. □

Exercise **(1.14)** (*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 $m, n \geq 1$. 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) $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\sim} \prod (R/\mathfrak{a}_i)$.

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 **(1.15)**. — 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 **(1.14)** 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:

$$\begin{aligned}
m &\equiv 0 \pmod 3 \quad\text{and}\quad m \equiv 0 \pmod 4;\\
m &\equiv 1 \pmod 3 \quad\text{and}\quad m \equiv 1 \pmod 4;\\
m &\equiv 1 \pmod 3 \quad\text{and}\quad m \equiv 0 \pmod 4;\\
m &\equiv 0 \pmod 3 \quad\text{and}\quad m \equiv 1 \pmod 4.
\end{aligned}$$

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 **(1.16)**. — 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. $\square$

Exercise **(1.17)**. — Let R be a ring, and e, e' idempotents. (See **(10.7)** also.)

(1) Set $\mathfrak{a} := \langle e \rangle$. Show $\mathfrak{a}$ is **idempotent**; that is, $\mathfrak{a}^2 = \mathfrak{a}$.
(2) Let $\mathfrak{a}$ be a principal idempotent ideal. Show $\mathfrak{a}\langle f \rangle$ with f idempotent.
(3) Set $e'' := e + e' - ee'$. Show $\langle e, e' \rangle = \langle e'' \rangle$ and e'' is idempotent.
(4) Let $e_1, \ldots, e_r$ be idempotents. Show $\langle e_1, \ldots, e_r \rangle = \langle f \rangle$ with f idempotent.
(5) Assume R is Boolean. Show every finitely generated ideal is principal.

Solution: For (1), note $\mathfrak{a}^2 = \langle e^2 \rangle$ since $\mathfrak{a} = \langle e \rangle$. But $e^2 = e$. Thus (1) holds.

For (2), say $\mathfrak{a} = \langle g \rangle$. Then $\mathfrak{a}^2 = \langle g^2 \rangle$. But $\mathfrak{a}^2 = \mathfrak{a}$. So $g = xg^2$ for some x. Set $f := xg$. Then $f \in \mathfrak{a}$; so $\langle f \rangle \subset \mathfrak{a}$. And $g = fg$. So $\mathfrak{a} \subset \langle f \rangle$. Thus (2) holds.

For (3), note $\langle e'' \rangle \subset \langle e, e' \rangle$. Conversely, $ee'' = e^2 + ee' - e^2e' = e + ee' - ee' = e$. By symmetry, $e'e'' = e'$. So $\langle e, e' \rangle \subset \langle e'' \rangle$ and $e''^2 = ee'' + e'e'' - ee'e'' = e''$. Thus (4) holds.

For (4), induct on r. Thus (3) yields (4).

For (5), recall that every element of R is idempotent. Thus (4) yields (5). $\square$

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) $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$.

Solution: Trivially, (1) implies (2). If (2) holds, then (3) follows as $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. 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, $xy \in \mathfrak{a}\mathfrak{b}$. Thus (3) implies (1). $\square$

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 as a subring.

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. $\square$

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 **(2.18)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal, $R[X]$ the polynomial ring. Show that $\mathfrak{p}R[X]$ and $\mathfrak{p}R[X]+\langle X\rangle$ are prime ideals of $R[X]$, and that if $\mathfrak{p}$ is maximal, then so is $\mathfrak{p}R[X] + \langle X\rangle$.

Solution: Note $R[X]/\mathfrak{p}R[X] = (R/\mathfrak{p})[X]$ by **(1.7)**. But $R/\mathfrak{p}$ is a domain by **(2.9)**. So $R[X]/\mathfrak{p}R[X]$ is a domain by **(2.3)**. Thus $\mathfrak{p}R[X]$ is prime by **(2.9)**.

Note $(\mathfrak{p}R[X] + \langle X\rangle)/\mathfrak{p}R[X]$ is equal to $\langle X\rangle \subset (R/\mathfrak{p})[X]$. But $(R/\mathfrak{p})[X]/\langle X\rangle$ is equal to $R/\mathfrak{p}$ by **(1.8)**. So $R[X]/(\mathfrak{p}R[X]+\langle X\rangle)$ is equal to $R/\mathfrak{p}$ by **(1.9)**. But $R/\mathfrak{p}$ is a domain by **(2.9)**. Thus $\mathfrak{p}R[X] + \langle X\rangle$ is prime again by **(2.9)**.

Assume $\mathfrak{p}$ is maximal. Then $R/\mathfrak{p}$ is a field by **(2.17)**. But, as just noted, $R/\mathfrak{p}$ is equal to $R[X]/(\mathfrak{p}R[X]+\langle X\rangle)$. Thus $\mathfrak{p}R[X]+\langle X\rangle$ is maximal again by **(2.17)**. □

Exercise **(2.11)**. — Let $R := R' \times R''$ be a **product** of rings, $\mathfrak{p} \subset R$ an ideal. Show $\mathfrak{p}$ is prime if and only if either $\mathfrak{p} = \mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $\mathfrak{p} = R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime.

Solution: Simply combine **(1.16)**, **(2.9)**, and **(2.5)**. □

Exercise **(2.16)**. — 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 **(2.15)**. Thus φ is injective. □

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.

Solution: Simply combine **(2.9)**, **(2.3)**, and **(1.10)**. □

Exercise **(2.12)**. — Let R be a domain, and $x, y \in R$. Assume $\langle x\rangle = \langle y\rangle$. Show $x = uy$ for some unit u.

Solution: By hypothesis, $x = uy$ and $y = vx$ for some $u, v \in R$. So $x = 0$ if and only if $y = 0$; if so, take $u := 1$. Assume $x \neq 0$. Now, $x = uvx$, or $x(1 - uv) = 0$. But R is a domain. So $1 - uv = 0$. Thus u is a unit. □

Exercise **(2.19)**. — Let B be a Boolean ring. Show that every prime $\mathfrak{p}$ is maximal, and $B/\mathfrak{p} = \mathbb{F}_2$.

Solution: Given $x \in B/\mathfrak{p}$, plainly $x(x-1) = 0$. But $B/\mathfrak{p}$ is a domain by **(2.9)**. So $z = 0, 1$. Thus $B/\mathfrak{p} = \mathbb{F}_2$. Plainly, $\mathbb{F}_2$ is a field. So $\mathfrak{p}$ is maximal by **(2.17)**. □

Exercise **(2.20)**. — Let R be a ring. Assume that, given $x \in R$, there is $n \ge 2$ with $x^n = x$. Show that every prime $\mathfrak{p}$ is maximal.

Solution: Given $y \in R/\mathfrak{p}$, say $y(y^{n-1} - 1) = 0$ with $n \ge 2$. But $R/\mathfrak{p}$ is a domain by **(2.9)**. So $y = 0$ or $yy^{n-2} = 1$. So $R/\mathfrak{p}$ is a field. Thus $\mathfrak{p}$ is maximal by **(2.17)**. □

Exercise **(2.22)**. — Prove the following statements, or give a counterexample.

(1) The complement of a multiplicative subset 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 **(1.9)**, an ideal $n' \subset R/\mathfrak{a}$ is maximal if and only if $\kappa^{-1}\mathfrak{n}' \subset R$ is maximal.

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. By **(1.9)**, the operation $\mathfrak{b}' \mapsto \kappa^{-1}\mathfrak{b}'$ sets up an inclusion-preserving bijective correspondence between the ideals $\mathfrak{b}' \supset \mathfrak{n}'$ and the ideals $\mathfrak{b} \supset \kappa^{-1}\mathfrak{n}'$. □

Exercise **(2.23)**. — Let k be a field, $P := k[X_1,\dots,X_n]$ the polynomial ring, $f \in P$ nonzero. Let d be the highest power of any variable appearing in f.

(1) Let $S \subset k$ have at least $d+1$ elements. Proceeding by induction on n, find $a_1,\dots,a_n \in S$ with $f(a_1,\dots,a_n) \neq 0$.

(2) Using the algebraic closure K of k, find a maximal ideal $\mathfrak{m}$ of P with $f \notin \mathfrak{m}$.

Solution: Consider (1). Assume $n = 1$. Then f has at most d roots by [**2**, (1.8), p. 392]. So $f(a_1) \neq 0$ for some $a_1 \in S$.

Assume $n > 1$. Say $f = \sum_j g_j X_1^j$ with $g_j \in k[X_2,\dots,X_n]$. But $f \neq 0$. So $g_i \neq 0$ for some i. By induction, $g_i(a_2,\dots,a_n) \neq 0$ for some $a_2,\dots,a_n \in S$. By $n = 1$, find $a_1 \in S$ such that $f(a_1,\dots,a_n) = \sum_j g_j(a_2,\dots,a_n)a_1^j \neq 0$. Thus (1) holds.

Consider (2). As K is infinite, (1) yields $a_1,\dots,a_n \in K$ with $f_i(a_1,\dots,a_n) \neq 0$. Define $\varphi\colon P \to K$ by $\varphi(X_i) = a_i$. Then $\operatorname{Im}(\varphi) \subset K$ is the k-subalgebra generated by the a_i. It is a field by [**2**, (2.6), p. 495]. Set $\mathfrak{m} := \operatorname{Ker}(\varphi)$. Then $\mathfrak{m}$ is maximal by **(1.6.1)** and **(2.17)**, and $f_i \notin \mathfrak{m}$ as $\varphi(f_i) = f_i(a_1,\dots,a_n) \neq 0$. Thus (2) holds. □

Exercise **(2.26)**. — 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 **(2.29)**. — Preserve the setup of **(2.28)**. 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, $\deg(f') = n \ge 1$. 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 **(1.7)** and **(1.9)**. So $\mathfrak{a}$ is proper. Thus $\langle f\rangle$ is not maximal. □

3. Radicals

Exercise **(3.3)**. — Let R be a ring, $\mathfrak{a} \subset \operatorname{rad}(R)$ an ideal, $w \in R$, and $w' \in R/\mathfrak{a}$ its residue. Prove that $w \in R^\times$ if and only if $w' \in (R/\mathfrak{a})^\times$. What if $\mathfrak{a} \not\subset \operatorname{rad}(R)$?

Solution: Plainly, $w \in R^\times$ implies $w' \in (R/\mathfrak{a})^\times$, whether $\mathfrak{a} \subset \mathrm{rad}(R)$ or not.

Assume $\mathfrak{a} \subset \mathrm{rad}(R)$. As every maximal ideal of R contains $\mathrm{rad}(R)$, the operation $\mathfrak{m} \mapsto \mathfrak{m}/\mathfrak{a}$ establishes a bijective correspondence between the maximal ideals of R and those of $R/\mathfrak{a}$ owing to **(1.9)**. So w belongs to a maximal ideal of R if and only if w' belongs to one of $R/\mathfrak{a}$. Thus $w \in R^\times$ if and only if $w' \in (R/\mathfrak{a})^\times$ by **(2.31)**.

Assume $\mathfrak{a} \not\subset \mathrm{rad}(R)$. Then there is a maximal ideal $\mathfrak{m} \subset R$ with $\mathfrak{a} \not\subset \mathfrak{m}$. So $\mathfrak{a} + \mathfrak{m} = R$. So there are $a \in \mathfrak{a}$ and $v \in \mathfrak{m}$ with $a + v = w$. Then $v \notin R^\times$, but the residue of v is w', even if $w' \in (R/\mathfrak{a})^\times$. For example, take $R := \mathbb{Z}$ and $\mathfrak{a} := \langle 2 \rangle$ and $w := 3$. Then $w \notin R^\times$, but the residue of w is $1 \in (R/\mathfrak{a})^\times$. □

Exercise **(3.8)**. — Let A be a local ring. Find its idempotents e.

Solution: Let $\mathfrak{m}$ be the maximal ideal. Then $1 \notin \mathfrak{m}$, so either $e \notin \mathfrak{m}$ or $1-e \notin \mathfrak{m}$. Say $e \notin \mathfrak{m}$. Then e is a unit by **(3.6)**. But $e(1-e) = 0$. Thus $e = 1$. Similarly, if $1 - e \notin \mathfrak{m}$, then $e = 0$.

Alternatvely, **(3.7)** implies that A is not the product of two nonzero rings. So **(1.13)** implies that either $e = 0$ or $e = 1$. □

Exercise **(3.9)**. — 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 $y \in A - \mathfrak{m}$. 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 **(3.6)**.

No, 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 **(3.13)**. — 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 **(3.12)**. 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 **(3.14)**. — Use Zorn's lemma to prove that any prime ideal $\mathfrak{p}$ contains a prime ideal $\mathfrak{q}$ that is minimal containing any given subset $\mathfrak{s} \subset \mathfrak{p}$.

Solution: Let $\mathcal{S}$ be the set of all prime ideals $\mathfrak{q}$ such that $\mathfrak{s} \subset \mathfrak{q} \subset \mathfrak{p}$. 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 $\{\mathfrak{q}_\lambda\}$ of prime ideals, the intersection $\mathfrak{q} := \bigcap \mathfrak{q}_\lambda$ is a prime ideal. Plainly $\mathfrak{q}$ is always an ideal. So take $x, y \notin \mathfrak{q}$. Then there exists λ such that $x, y \notin \mathfrak{q}_\lambda$. Since $\mathfrak{q}_\lambda$ is prime, $xy \notin \mathfrak{q}_\lambda$. So $xy \notin \mathfrak{q}$. Thus $\mathfrak{q}$ is prime. □

Exercise **(3.16)**. — Let R be a ring, S a subset. Show that S is saturated multiplicative if and only if $R - S$ is a union of primes.

Solution: First, assume S is saturated multiplicative. Take $x \in R - S$. Then $xy \notin S$ for all $y \in R$; in other words, $\langle x \rangle \cap S = \emptyset$. Then **(3.12)** gives a prime $\mathfrak{p} \supset \langle x \rangle$ with $\mathfrak{p} \cap S = \emptyset$. Thus $R - S$ is a union of primes.

Conversely, assume $R - S$ is a union of primes $\mathfrak{p}$. Then $1 \in S$ as 1 lies in no $\mathfrak{p}$. Take $x, y \in R$. Then $x, y \in S$ if and only if x, y lie in no $\mathfrak{p}$; if and only if xy lies in no $\mathfrak{p}$, as every $\mathfrak{p}$ is prime; if and only if $xy \in S$. Thus S is saturated multiplicative. □

Exercise **(3.17)**. — Let R be a ring, and S a multiplicative subset. Define its **saturation** to be the subset

$$\overline{S} := \{\, x \in R \mid \text{there is } y \in R \text{ with } xy \in S \,\}.$$

(1) Show (a) that $\overline{S} \supset S$, and (b) that $\overline{S}$ is saturated multiplicative, and (c) that any saturated multiplicative subset T containing S also contains $\overline{S}$.

(2) Show that $R - \overline{S}$ is the union U of all the primes $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$.

(3) Let $\mathfrak{a}$ be an ideal; assume $S = 1 + \mathfrak{a}$; set $W := \bigcup_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. Show $R - \overline{S} = W$.

(4) Given $f \in R$, let $\overline{S}_f$ denote the saturation of the multiplicative subset of all powers of f. Given $f, g \in R$, show $\overline{S}_f \subset \overline{S}_g$ if and only if $\sqrt{\langle f \rangle} \supset \sqrt{\langle g \rangle}$.

Solution: Consider (1). Trivially, if $x \in S$, then $x \cdot 1 \in S$. Thus (a) holds.

Hence $1 \in \overline{S}$ as $1 \in S$. Now, take $x, x' \in \overline{S}$. Then there are $y, y' \in R$ with $xy,\ x'y' \in S$. But S is multiplicative. So $(xx'')(yy') \in S$. Hence $xx' \in \overline{S}$. Thus $\overline{S}$ is multiplicative. Further, take $x, x' \in R$ with $xx' \in \overline{S}$. Then there is $y \in R$ with $xx'y \in S$. So $x, x' \in \overline{S}$. Thus S is saturated. Thus (b) holds

Finally, consider (c). Given $x \in \overline{S}$, there is $y \in R$ with $xy \in S$. So $xy \in T$. But T is saturated multiplicative. So $x \in T$. Thus $T \supset \overline{S}$. Thus (c) holds.

Consider (2). Plainly, $R - U$ contains S. Further, $R - U$ is saturated multiplicative by **(3.16)**. So $R - U \supset \overline{S}$ by (1)(c). Thus $U \subset R - \overline{S}$. Conversely, $R - \overline{S}$ is a union of primes $\mathfrak{p}$ by **(3.16)**. Plainly, $\mathfrak{p} \cap S = \emptyset$ for all $\mathfrak{p}$. So $U \supset R - \overline{S}$. Thus (2) holds.

For (3), first take a prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $1 \notin \mathfrak{p} + \mathfrak{a}$; else, $1 = p + a$ with $p \in \mathfrak{p}$ and $a \in \mathfrak{a}$, and so $1 - p = a \in \mathfrak{p} \cap S$. So $\mathfrak{p} + \mathfrak{a}$ lies in a maximal ideal $\mathfrak{m}$ by **(3.12)**. Then $\mathfrak{a} \subset \mathfrak{m}$; so $\mathfrak{m} \subset W$. But also $\mathfrak{p} \subset \mathfrak{m}$. Thus $U \subset W$.

Conversely, take $\mathfrak{p} \supset \mathfrak{a}$. Then $1 + \mathfrak{p} \subset 1 + \mathfrak{a} = S$. But $\mathfrak{p} \cap (1 + \mathfrak{p}) = \emptyset$. So $\mathfrak{p} \cap S = \emptyset$. Thus $U \supset W$. Thus $U = W$. Thus (2) yields (3).

Consider (4). By (1), $\overline{S}_f \subset \overline{S}_g$ if and only if $f \in \overline{S}_g$. By definition of saturation, $f \in \overline{S}_g$ if and only if $hf = g^n$ for some h and n. By definition of radical, $hf = g^n$ for some h and n if and only if $g \in \sqrt{\langle f \rangle}$. Plainly, $g \in \sqrt{\langle f \rangle}$ if and only if $\sqrt{\langle g \rangle} \subset \sqrt{\langle f \rangle}$. Thus (4) holds. □

Exercise **(3.18)**. — Let R be a nonzero ring, S a subset. Show S is maximal in the set $\mathfrak{S}$ of multiplicative subsets T of R with $0 \notin T$ if and only if $R - S$ is a **minimal** prime — that is, it is a prime containing no smaller prime.

Solution: First, assume S is maximal in $\mathfrak{S}$. Then S is equal to its saturation $\overline{S}$, as $S \subset \overline{S}$ and $\overline{S}$ is multiplicative by **(3.17)** (1)(a),(b) and as $0 \in \overline{S}$ would imply $0 = 0 \cdot y \in S$ for some y. So $R - S$ is a union of primes $\mathfrak{p}$ by **(3.16)**. Fix a $\mathfrak{p}$. Then **(3.14)** yields in $\mathfrak{p}$ a minimal prime $\mathfrak{q}$. Then $S \subset R - \mathfrak{q}$. But $R - \mathfrak{q} \in \mathfrak{S}$ by **(2.1)**. As S is maximal, $S = R - \mathfrak{q}$, or $R - S = \mathfrak{q}$. Thus $R - S$ is a minimal prime.

Conversely, assume $R - S$ is a minimal prime $\mathfrak{q}$. Then $S \in \mathfrak{S}$ by **(2.1)**. Given $T \in \mathfrak{S}$ with $S \subset T$, note $R - \overline{T} = \bigcup \mathfrak{p}$ with $\mathfrak{p}$ prime by **(3.16)**. Fix a $\mathfrak{p}$. Now, $S \subset T \subset \overline{T}$. So $\mathfrak{q} \supset \mathfrak{p}$. But $\mathfrak{q}$ is minimal. So $\mathfrak{q} = \mathfrak{p}$. But $\mathfrak{p}$ is arbitrary, and

$\bigcup \mathfrak{p} = R - \overline{T}$. Hence $\mathfrak{q} = R - \overline{T}$. So $S = \overline{T}$. Hence $S = T$. Thus S is maximal. □

Exercise **(3.20)**. — Let k be a field, $\mathcal{S} \subset k$ a subset of cardinality d at least 2.

(1) Let $P := k[X_1, \dots, X_n]$ be the polynomial ring, $f \in P$ nonzero. Assume the highest power of any X_i in f is less than d. Proceeding by induction on n, show there are $a_1, \dots, a_n \in \mathcal{S}$ with $f(a_1, \dots, a_n) \neq 0$.

(2) Let V be a k-vector space, and $W_1, \dots, W_r$ proper subspaces. Assume $r < d$. Show $\bigcup_i W_i \neq V$.

(3) In (2), let $W \subset \bigcup_i W_i$ be a subspace. Show $W \subset W_i$ for some i.

(4) Let R a k-algebra, $\mathfrak{a}, \mathfrak{a}_1, \dots, \mathfrak{a}_r$ ideals with $\mathfrak{a} \subset \bigcup_i \mathfrak{a}_i$. Show $\mathfrak{a} \subset \mathfrak{a}_i$ for some i.

Solution: For (1), first assume $n = 1$. Then f has degree at most d, so at most d roots by [**2**, (1.8), p. 392]. So there's $a_1 \in \mathcal{S}$ with $f(a_1) \neq 0$.

Assume $n > 1$. Say $f = \sum_j g_j X_1^j$ with $g_j \in k[X_2, \dots, X_n]$. But $f \neq 0$. So $g_i \neq 0$ for some i. By induction, there are $a_2, \dots, a_n \in \mathcal{S}$ with $g_i(a_2, \dots, a_n) \neq 0$. So there's $a_1 \in \mathcal{S}$ with $f(a_1, \dots, a_n) = \sum_j g_j(a_2, \dots, a_n) a_1^j \neq 0$. Thus (1) holds.

For (2), for all i, take $v_i \in V - W_i$. Form their span $V' \subset V$. Set $n := \dim V'$ and $W'_i := W_i \cap V'$. Then $n < \infty$, and it suffices to show $\bigcup_i W'_i \neq V'$.

Identify V' with k^n. Form the polynomial ring $P := k[X_1, \dots, X_n]$. For each i, take a linear form $f_i \in P$ that vanishes on W'_i. Set $f := f_1 \cdots f_r$. Then r is the highest power of any variable in f. But $r < d$. So (1) yields $a_1, \dots, a_n \in \mathcal{S}$ with $f(a_1, \dots, a_n) \neq 0$. Then $(a_1, \dots, a_n) \in V' - \bigcup_i W'_i$.

For (3), for all i, set $U_i := W \cap W_i$. Then $\bigcup_i U_i = W$. So (2) implies $U_i = W$ for some i. Thus $W \subset W_i$.

Finally, (4) is a special case of (3), as every ideal is a k-vector space. □

Exercise **(3.21)**. — Let k be a field, $R := k[X, Y]$ the polynomial ring in two variables, $\mathfrak{m} := \langle X, Y \rangle$. Show $\mathfrak{m}$ is a union of strictly smaller primes.

Solution: Since R is a UFD, and $\mathfrak{m}$ is maximal, so prime, any nonzero $f \in \mathfrak{m}$ has a prime factor $p \in \mathfrak{m}$. Thus $\mathfrak{m} = \bigcup_p \langle p \rangle$, but $\mathfrak{m} \neq \langle p \rangle$ as $\mathfrak{m}$ is not principal. □

Exercise **(3.23)**. — 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 **(3.24)**. — Let R be a ring. (1) Assume every ideal not contained in $\operatorname{nil}(R)$ contains a nonzero idempotent. Prove that $\operatorname{nil}(R) = \operatorname{rad}(R)$. (2) Assume R is Boolean. Prove that $\operatorname{nil}(R) = \operatorname{rad}(R) = \langle 0 \rangle$.

Solution: or (1), recall **(3.22.1)**, that $\operatorname{nil}(R) \subset \operatorname{rad}(R)$. To prove the opposite inclusion, set $R' := R/\operatorname{nil}(R)$. Assume $\operatorname{rad}(R') \neq \langle 0 \rangle$. Then there is a nonzero idempotent $e \in \operatorname{rad}(R')$. Then $e(1-e) = 0$. But $1 - e$ is a unit by **(3.2)**. So $e = 0$, a contradiction. Hence $\operatorname{rad}(R') = \langle 0 \rangle$. Thus **(1.9)** yields (1).

For (2), recall from **(1.2)** that every element of R is idempotent. So $\operatorname{nil}(R) = \langle 0 \rangle$, and every nonzero ideal contains a nonzero idempotent. Thus (1) yields (2). □

Exercise **(3.25)**. — 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 **(3.38)**. — Let R be a ring, X a variable. Show that

$$\operatorname{rad}(R[X]) = \operatorname{nil}(R[X]) = \operatorname{nil}(R)R[X].$$

Solution: First, recall that $\operatorname{rad}(R[X]) \supset \operatorname{nil}(R[X])$ by **(3.22.1)**. Next, recall that $\operatorname{nil}(R[X]) \supset \operatorname{nil}(R)R[X]$ by **(3.31)**. Finally, given $f := a_0 + \cdots + a_n X^n$ in $\operatorname{rad}(R[X])$, note that $1 + Xf$ is a unit by **(3.2)**. So $a_0, \dots, a_n$ are nilpotent by **(3.36)**(2). So $f \in \operatorname{nil}(R)R[X]$. Thus $\operatorname{nil}(R)R[X] \supset \operatorname{rad}(R[X])$, as desired. □

Exercise **(3.26)**. — Let $e, e' \in \operatorname{Idem}(R)$. Assume $\sqrt{\langle e \rangle} = \sqrt{\langle e' \rangle}$. Show $e = e'$.

Solution: By hypothesis, $e^n \in \langle e' \rangle$ for some $n \geq 1$. But $e^2 = e$, so $e^n = e$. So $e = xe'$ for some x. So $e = xe'^2 = ee'$. By symmetry, $e' = e'e$. Thus $e = e'$. □

Exercise **(3.27)**. — Let R be a ring, $\mathfrak{a}_1, \mathfrak{a}_2$ comaximal ideals with $\mathfrak{a}_1\mathfrak{a}_2 \subset \operatorname{nil}(R)$. Show there are complementary idempotents e_1 and e_2 with $e_i \in \mathfrak{a}_i$.

Solution: Since $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are comaximal, there are $x_i \in \mathfrak{a}_i$ with $x_1 + x_2 = 1$. Given $n \geq 1$, expanding $(x_1 + x_2)^{2n-1}$ and collecting terms yields $a_1 x_1^n + a_2 x_2^n = 1$ for suitable $a_i \in R$. Now, $x_1 x_2 \in \operatorname{nil}(R)$; take $n \geq 1$ so that $(x_1 x_2)^n = 0$. Set $e_i := a_i x_i^n \in \mathfrak{a}_i$. Then $e_1 + e_2 = 1$ and $e_1 e_2 = 0$. Thus e_1 and e_2 are complementary idempotents by **(1.11)**. □

Exercise **(3.28)**. — Let R be a ring, $\mathfrak{a}$ an ideal, $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Assume $\mathfrak{a} \subset \operatorname{nil}(R)$. Prove that $\operatorname{Idem}(\kappa)$ is bijective.

Solution: Note that $\operatorname{Idem}(\kappa)$ is injective by **(3.22.1)** and **(3.4)**.

As to surjectivity, given $e' \in \operatorname{Idem}(R/\mathfrak{a})$, take $z \in R$ with residue e'. Then $\langle z \rangle$ and $\langle 1 - z \rangle$ are trivially comaximal. And $\langle z \rangle \langle 1 - z \rangle \subset \mathfrak{a} \subset \operatorname{nil}(R)$ as $\kappa(z - z^2) = 0$. So **(3.27)** yields complementary idempotents $e_1 \in \langle z \rangle$ and $e_2 \in \langle 1 - z \rangle$.

Say $e_1 = xz$ with $x \in R$. Then $\kappa(e_1) = xe'$. So $\kappa(e_1) = xe'^2 = \kappa(e_1)e'$. Similarly, $\kappa(e_2) = \kappa(e_2)(1 - e')$. So $\kappa(e_2)e' = 0$. But $\kappa(e_2) = 1 - \kappa(e_1)$. So $(1 - \kappa(e_1))e' = 0$, or $e' = \kappa(e_1)e'$. But $\kappa(e_1) = \kappa(e_1)e'$. So $\kappa(e_1) = e'$. Thus $\operatorname{Idem}(\kappa)$ is surjective. □

Exercise **(3.30)**. — Let R be a ring. Prove the following statement equivalent:

(1) R has exactly one prime $\mathfrak{p}$;
(2) every element of R is either nilpotent or a unit;
(3) $R/\operatorname{nil}(R)$ is a field.

Solution: Assume (1). Let $x \in R$ be a nonunit. Then $x \in \mathfrak{p}$. So x is nilpotent by the Scheinnullstellensatz **(3.29)**. Thus (2) holds.

Assume (2). Then every $x \notin \operatorname{nil}(R)$ has an inverse. Thus (3) holds.

Assume (3). Then $\operatorname{nil}(R)$ is maximal by **(2.15)**. But any prime of R contains $\operatorname{nil}(R)$ by **(3.29)**. Thus (1) holds. □

Exercise **(3.32)**. — Let R be a ring, and $\mathfrak{a}$ an ideal. Assume $\sqrt{\mathfrak{a}}$ is finitely generated. Show $\left(\sqrt{\mathfrak{a}}\right)^n \subset \mathfrak{a}$ for all large n.

Solution: Let $x_1, \dots, x_m$ be generators of $\sqrt{\mathfrak{a}}$. For each i, there is n_i such that $x_i^{n_i} \in \mathfrak{a}$. Let $n > \sum(n_i - 1)$. 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 $j_i \geq n_i$ 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 **(3.33)**. — 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 **(3.32)**. 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 **(3.35)**. — Let R be a ring. Assume R is reduced and has finitely many minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Prove that $\varphi\colon R \to \prod(R/\mathfrak{p}_i)$ is injective, and for each i, there is some $(x_1, \dots, x_n) \in \operatorname{Im}(\varphi)$ 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, **(3.29)** and **(3.14)** 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 $j \neq i$. So take $(x_1, \dots, x_n) := \varphi(a)$. □

Exercise **(3.36)**. — Let R be a ring, X a variable, $f := a_0 + a_1 X + \cdots + a_n X^n$ and $g := b_0 + b_1 X + \cdots + b_m X^m$ polynomials with $a_n \neq 0$ and $b_m \neq 0$. Call f **primitive** if $\langle a_0, \dots, a_n \rangle = R$. Prove the following statements:

(1) Then f is nilpotent if and only if $a_0, \dots, a_n$ are nilpotent.
(2) Then f is a unit if and only if a_0 is a unit and $a_1, \dots, a_n$ are nilpotent.
(3) If f is a zerodivisor, then there is a nonzero $b \in R$ with $bf = 0$; in fact, if $fg = 0$ with m minimal, then $fb_m = 0$ (or $m = 0$).
(4) Then fg is primitive if and only if f and g are primitive.

Solution: In (1), if $a_0, \dots, a_n$ are nilpotent, so is f owing to **(3.31)**. Conversely, say $a_i \notin \operatorname{nil}(R)$. Then the Scheinnullstellensatz **(3.29)** yields a prime $\mathfrak{p} \subset R$ with $a_i \notin \mathfrak{p}$. So $f \notin \mathfrak{p}R[X]$. But $\mathfrak{p}R[X]$ is prime by **(2.18)**. So plainly $f \notin \operatorname{nil}(R[X])$.

Alternatively, say $f^k = 0$. Then $(a_n X^n)^k = 0$. So $f - a_n X^n$ is nilpotent owing to **(3.31)**. So $a_0, \dots, a_{n-1}$ are nilpotent by induction on n. Thus (1) holds.

For (2), suppose a_0 is a unit and $a_1, \dots, a_n$ are nilpotent. Then $a_1 X + \cdots + a_n X^n$ is nilpotent by (1), so belongs to $\operatorname{rad}(R)$ by **(3.22.1)**. Thus f is a unit by **(3.2)**.

Conversely, suppose $fg = 1$. Then $a_0 b_0 = 1$. Thus a_0 and b_0 are units.

Further, given a prime $\mathfrak{p} \subset R$, let $\kappa_\mathfrak{p}\colon R[X] \to (R/\mathfrak{p})[X]$ be the canonical map. Then $\kappa_\mathfrak{p}(f)\kappa_\mathfrak{p}(g) = 1$. But $R/\mathfrak{p}$ is a domain by **(2.9)**. So $\deg \kappa_\mathfrak{p}(f) = 0$ owing to **(2.3.1)**. So $a_1, \dots, a_n \in \mathfrak{p}$. But $\mathfrak{p}$ is arbitrary. Thus $a_1, \dots, a_n \in \operatorname{nil}(R)$ by **(3.2)**.

Alternatively, let's prove $a_n^{r+1} b_{m-r} = 0$ by induction on r. Set $c_i := \sum_{j+k=i} a_j b_k$. Then $\sum c_i X^i = fg$. But $fg = 1$. So $c_i = 0$ for $i > 0$. Taking $i := m + n$ yields $a_n b_m = 0$. Then $c_{m+n-r} = 0$ yields $a_n b_{m-r} + a_{n-1} b_{m-(r-1)} + \cdots = 0$. Multiplying by a_n^r yields $a_n^{r+1} b_{m-r} = 0$ by induction. So $a_n^{m+1} b_0 = 0$. But b_0 is a unit. So $a_n^{m+1} = 0$. So $a_n X^n \in \operatorname{rad}(R[X])$ by **(3.22.1)**. But f is a unit. So $f - a_n X^n$ is a unit by **(3.3)**. So $a_1, \dots, a_{n-1}$ are nilpotent by induction on n. Thus (2) holds.

For (3), suppose $fb_m \neq 0$. Say $a_r b_m \neq 0$, but $a_{r+i} b_m = 0$ for all $i > 0$. Fix $i > 0$ and set $h := a_{r+i} g$. Then $fh = 0$ if $fg = 0$. Also $h = 0$ or $\deg(h) < m$. So $h = 0$ if m is minimal. In particular, $a_{r+i} b_{m-i} = 0$. But $i > 0$ is arbitrary. Also $fg = 0$ yields $a_r b_m + a_{r+1} b_{m-1} + \cdots = 0$. So $a_r b_m = 0$, a contradiction. Thus (3) holds.

For (4), given $\mathfrak{m} \subset R$ maximal, let $\kappa_\mathfrak{m}\colon R[X] \to (R/\mathfrak{m})[X]$ be the canonical map. Then $h \in R[X]$ is primitive if and only if $\kappa_\mathfrak{m}(h) \neq 0$ for all $\mathfrak{m}$, owing to **(2.30)**. But $R/\mathfrak{m}$ is a field by **(2.17)**. So $(R/\mathfrak{m})[X]$ is a domain by **(2.3)**. Hence $\kappa_\mathfrak{p}(fg) = 0$ if and only if $\kappa_\mathfrak{p}(f) = 0$ or $\kappa_\mathfrak{p}(g) = 0$. Thus (4) holds. □

Exercise **(3.37)**. — Generalize **(3.36)** to the polynomial ring $P := R[X_1, \dots, X_r]$. For (3), reduce to the case of one variable Y via this standard device: take d suitably large, and define $\varphi\colon P \to R[Y]$ by $\varphi(X_i) := Y^{d^i}$.

Solution: Let $f, g \in P$. Write $f = \sum a_{(i)} X^{(i)}$ where $(i) := (i_1, \dots, i_r)$ and $X^{(i)} := X_1^{i_1} \cdots X_r^{i_r}$. Call f **primitive** if the $a_{(i)}$ generate R. Set $(0) := (0, \dots, 0)$. Then (1)–(4) generalize as follows:

(1′) Then f is nilpotent if and only if $a_{(i)}$ is nilpotent for all (i).
(2′) Then f is a unit if and only if $a_{(0)}$ is a unit and $a_{(i)}$ is nilpotent for $(i) \neq (0)$.
(3′) Assume f is a zerodivisor. Then there is a nonzero $c \in R$ with $cf = 0$.
(4′) Then fg is primitive if and only if f and g are primitive.

To prove (1′)–(2′), set $R' := R[X_2, \dots, X_r]$, and say $f = \sum f_i X_1^i$ with $f_i \in R'$.

In (1′), if f is nilpotent, so are all f_i by **(3.36)**(1); hence by induction on r, so are all $a_{(i)}$. Conversely, if all $a_{(i)}$ are nilpotent, so is f by **(3.31)**. Thus (1′) holds.

In (2′), if $a_{(0)}$ is a unit and $a_{(i)}$ is nilpotent for $(i) \neq (0)$, then $\sum_{(i) \neq (0)} a_{(i)} X^{(i)}$ is nilpotent by (1), so belongs to $\operatorname{rad}(R)$ by **(3.22.1)**. Then f is a unit by **(3.2)**.

Conversely, suppose f is a unit. Then f_0 is a unit, and f_i is nilpotent for $i > 0$ by **(3.36)**(2). So $a_{(0)}$ is a unit, and $a_{(i)}$ is nilpotent if $i_1 = 0$ and $(i) \neq (0)$, by induction on r. Also, $a_{(i)}$ is nilpotent if $i_1 > 0$ by (1′). Thus (2′) holds.

In (3′), there's a nonzero $g \in P$ with $fg = 0$. Take d larger than any exponent of any X_i found in f or g. Form the R-algebra map $\varphi\colon P \to R[Y]$ with $\varphi(X_i) = Y^{d^{i-1}}$. Then $\varphi(f)\varphi(g) = 0$. But $\varphi(X^{(i)}) = Y^{i_1 + \cdots + i_r d^{r-1}}$. So φ carries distinct monomials in f to distinct monomials in $\varphi(f)$, and the same for g. So $\varphi(f)$ has the same coefficients as f, and $\varphi(g)$ the same as g. So $\varphi(g) \neq 0$. Hence $\varphi(f)$ is a zerodivisor. So **(3.36)**(3) yields a nonzero $c \in R$ with $c\varphi(f) = 0$. Hence $ca_{(i)} = 0$ for all $a_{(i)}$. So $cf = 0$. Thus (3′) holds.

For (4′), use the solution of **(3.36)**(4) with X replaced by $X_1, \dots, X_r$. □

Exercise **(3.39)**. — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $R[[X]]$ the formal power series ring, $\mathfrak{M} \subset R[[X]]$ an ideal, and $f := \sum a_n X^n \in R[[X]]$. Set $\mathfrak{m} := \mathfrak{M} \cap R$ and $\mathfrak{A} := \{\sum b_n X^n \mid b_n \in \mathfrak{a}\}$. Prove the following statements:

(1) If f is nilpotent, then a_n is nilpotent for all n. The converse is false.
(2) Then $f \in \operatorname{rad}(R[[X]])$ if and only if $a_0 \in \operatorname{rad}(R)$.
(3) Assume $X \in \mathfrak{M}$. Then X and $\mathfrak{m}$ generate $\mathfrak{M}$.
(4) Assume $\mathfrak{M}$ is maximal. Then $X \in \mathfrak{M}$ and $\mathfrak{m}$ is maximal.
(5) If $\mathfrak{a}$ is finitely generated, then $\mathfrak{a}R[[X]] = \mathfrak{A}$. The converse may fail.

Solution: For (1), assume f and a_i for $i < n$ are nilpotent. Set $g := \sum_{i \geq n} a_i X^i$. Then $g = f - \sum_{i<n} a_i X^i$. So g is nilpotent by **(3.31)**; say $g^m = 0$ with $m \geq 1$. Then $a_n^m = 0$. Thus by induction a_n is nilpotent for all n.

The converse is false. For example, set $P := \mathbb{Z}[X_2, X_3, \dots]$ for variables X_n. Set

$R := P/\langle X_2^2, X_3^3, \dots \rangle$. Let a_n be the residue of X_n. Then $a_n^n = 0$, but $\sum a_n X^n$ is not nilpotent. Thus (1) holds.

For (2), given $g = \sum b_n X^n \in \operatorname{rad}(R[[X]])$, note that $1 + fg$ is a unit if and only if $1 + a_0 b_0$ is a unit by **(3.10)**. Thus **(3.2)** yields (2) holds.

For (3), note $\mathfrak{M}$ contains X and $\mathfrak{m}$, so the ideal they generate. But $f = a_0 + Xg$ for some $g \in R[[X]]$. So if $f \in \mathfrak{M}$, then $a_0 \in \mathfrak{M} \cap R = \mathfrak{m}$. Thus (3) holds.

For (4), note that $X \in \operatorname{rad}(R[[X]])$ by (2). So X and $\mathfrak{m}$ generate $\mathfrak{M}$ by (3). So $P/\mathfrak{n} = R/\mathfrak{m}$ by **(3.10)**. Thus **(2.17)** yields (4).

In (5), plainly $\mathfrak{a}R[[X]] \subset \mathfrak{A}$. Now, assume $f := \sum a_n X^n \in \mathfrak{A}$, or all $a_n \in \mathfrak{a}$. Say $b_1, \dots, b_m \in \mathfrak{a}$ generate. Then $a_n = \sum_{i=1}^m c_{ni} b_i$ for some $c_{ni} \in R$. Thus, as desired,

$$f = \sum_{n\ge 0}\Big(\sum_{i=1}^m c_{ni} b_i\Big) X^n = \sum_{i=1}^m b_i \Big(\sum_{n\ge 0} c_{ni} X^n\Big) \in \mathfrak{a}R[[X]].$$

For a counterexample, take $a_0, a_1, \dots$ to be variables. Take $R := \mathbb{Z}[a_1, a_2, \dots]$ and $\mathfrak{a} := \langle a_1, a_2, \dots \rangle$. Given $g \in \mathfrak{a}R[[X]]$, say $g = \sum_{i=1}^m b_i g_i$ with $b_i \in \mathfrak{a}$ and $g_i = \sum_{n\ge 0} b_{in} X^n$. Choose p greater than the maximum n such that a_n occurs in any b_i. Then $\sum_{i=1}^m b_i b_{in} \in \langle a_1, \dots, a_{p-1} \rangle$, but $a_p \notin \langle a_1, \dots, a_{p-1} \rangle$. Therefore, $g \ne f := \sum a_n X^n$. Thus $f \notin \mathfrak{a}R[[X]]$, but $f \in \mathfrak{A}$. □

4. Modules

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

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

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

Solution: First off, ρ is R-linear, because

$$\rho(x\theta + x'\theta') = (x\theta + x'\theta')(1) = x\theta(1) + x'\theta'(1) = x\rho(\theta) + x'\rho(\theta').$$

Set $H := \operatorname{Hom}(R, M)$. Define $\alpha\colon M \to H$ by $\alpha(m)(x) := xm$. It is easy to check that $\alpha\rho = 1_H$ and $\rho\alpha = 1_M$. Thus ρ and α 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 **(4.13)**. — A finitely generated free module has finite rank.

Solution: Say e_λ for $\lambda \in \Lambda$ form a free basis, and $m_1, \dots, m_r$ generate. Then $m_i = \sum x_{ij} e_{\lambda_j}$ for some x_{ij}. Consider the e_{λ_j} that occur. Plainly, they are finite in number, and generate. So they form a finite free basis, as desired. □

Exercise **(4.16)**. — Let Λ be an infinite set, R_λ a nonzero 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 (x_λ) can be a multiplicative identity in $\bigoplus R_\lambda$; indeed, because Λ is infinite, x_μ must be zero for some μ. So $(x_\lambda) \cdot (y_\lambda) \ne (y_\lambda)$ if $y_\mu \ne 0$. □

Exercise **(4.17)**. — Let R be a ring, M a module, and M', M'' submodules. Show that $M = M' \oplus M''$ if and only if $M = M' + M''$ and $M' \cap M'' = 0$.

Solution: Assume $M = M' \oplus M''$. Then M is the set of pairs (m', m'') with $m' \in M'$ and $m'' \in M''$ by **(4.15)**; further, M' is the set of $(m', 0)$, and M' is that of $(0, m'')$. So plainly $M = M' + M''$ and $M' \cap M'' = 0$.

Conversely, consider the map $M' \oplus M'' \to M$ given by $(m', m'') \mapsto m' + m''$. It is surjective if $M = M' + M''$. It is injective if $M' \cap M'' = 0$; indeed, if $m' + m'' = 0$, then $m' = -m'' \in M' \cap M'' = 0$, and so $(m', m'') = 0$ as desired. □

Exercise **(4.18)**. — Let L, M, and N be 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 **(4.19)**. — Let L be a module, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove that the injections $\iota_\kappa\colon M_\kappa \to \bigoplus M_\lambda$ induce an injection

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

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

Solution: For $\lambda \in \Lambda$, let $\alpha_\lambda\colon L \to M_\lambda$ be maps, almost all 0. Then

$$\big(\sum \iota_\lambda\alpha_\lambda\big)(l) = \big(\alpha_\lambda(l)\big) \in \bigoplus M_\lambda.$$

So if $\sum \iota_\lambda\alpha_\lambda = 0$, then $\alpha_\lambda = 0$ for all λ. Thus the ι_κ induce an injection.

Assume L is finitely generated, say by $l_1, \dots, l_k$. Let $\alpha\colon L \to \bigoplus M_\lambda$ be a map. Then each $\alpha(l_i)$ lies in a finite direct subsum of $\bigoplus M_\lambda$. So $\alpha(L)$ 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 $\bigoplus \operatorname{Hom}(L, M_\lambda)$, and $\sum \iota_\kappa\alpha_\kappa = \alpha$. Thus the ι_κ induce a surjection, so an isomorphism. □

Exercise **(4.20)**. — Let $\mathfrak{a}$ be an ideal, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove $\mathfrak{a}(\bigoplus M_\lambda) = \bigoplus \mathfrak{a}M_\lambda$. Prove $\mathfrak{a}(\prod M_\lambda) = \prod \mathfrak{a}M_\lambda$ if $\mathfrak{a}$ is finitely generated.

Solution: First, $\mathfrak{a}(\bigoplus M_\lambda) \subset \bigoplus \mathfrak{a}M_\lambda$ because $a \cdot (m_\lambda) = (am_\lambda)$. Conversely, $\mathfrak{a}(\bigoplus M_\lambda) \supset \bigoplus \mathfrak{a}M_\lambda$ because $(a_\lambda m_\lambda) = \sum a_\lambda \iota_\lambda m_\lambda$ since the sum is finite.

Second, $\mathfrak{a}(\prod M_\lambda) \subset \prod \mathfrak{a}M_\lambda$ as $a(m_\lambda) = (am_\lambda)$. Conversely, say $\mathfrak{a}$ is generated by $f_1, \dots, f_n$. Then $\mathfrak{a}(\prod M_\lambda) \supset \prod \mathfrak{a}M_\lambda$. 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 $a_{\lambda j} = \sum_{i=1}^{n} x_{\lambda j i} f_i$ with the $x_{\lambda j i}$ scalars. Then

$$(m'_\lambda) = \Bigl(\sum_{j=1}^{n_\lambda} \sum_{i=1}^{n} f_i x_{\lambda j i} m_{\lambda j}\Bigr) = \sum_{i=1}^{n} f_i \Bigl(\sum_{j=1}^{n_\lambda} x_{\lambda j i} m_{\lambda j}\Bigr) \in \mathfrak{a}\Bigl(\prod M_\lambda\Bigr). \qquad \square$$

5. Exact Sequences

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

Solution: By **(5.2)**(1) and **(5.3)**, 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 **(5.4)**, the sequence

$$0 \to N \to M' \oplus M'' \to (M'/N) \oplus M'' \to 0$$

is exact. Thus **(5.3)** yields the assertion. $\square$

Exercise **(5.6)**. — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. 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. $\square$

Exercise **(5.11)**. — 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, $\pi_{M''}N = N''$. $\square$

Exercise **(5.12)**. — Criticize the following misstatement of **(5.9)**: given a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$, there is an isomorphism $M \simeq M' \oplus M''$ if and only if there is a section $\sigma\colon M'' \to M$ of β and α is injective.

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 [**2**, (6.4), p. 472], [**8**, 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, **(5.11)** 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 $M \simeq M' \oplus M''$. $\square$

Exercise **(5.14)**. — Referring to **(4.8)**, give an alternative proof that β is an isomorphism by applying the Snake Lemma to the diagram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d, "\kappa"'] & N/M \arrow[r] \arrow[d, "\beta"'] & 0 \\
0 \arrow[r] & M/L \arrow[r] & N/L \arrow[r, "\lambda"] & (N/L)/(M/L) \arrow[r] & 0
\end{tikzcd}$$

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. $\square$

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

$$\begin{tikzcd}
M_4 \arrow[r, "\alpha_4"] \arrow[d, "\gamma_4"'] & M_3 \arrow[r, "\alpha_3"] \arrow[d, "\gamma_3"'] & M_2 \arrow[r, "\alpha_2"] \arrow[d, "\gamma_2"'] & M_1 \arrow[r, "\alpha_1"] \arrow[d, "\gamma_1"'] & M_0 \arrow[d, "\gamma_0"'] \\
N_4 \arrow[r, "\beta_4"] & N_3 \arrow[r, "\beta_3"] & N_2 \arrow[r, "\beta_2"] & N_1 \arrow[r, "\beta_1"] & N_0
\end{tikzcd}$$

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. $\square$

Exercise **(5.16)** (*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 **(5.13)** applied to the bottom two rows. The converse is proved similarly. □

Exercise **(5.17)**. — Consider this commutative diagram with exact rows:

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

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 **(5.22)**. — 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 **(5.24)**. — Let R be a ring, P and N finitely generated modules with P projective. Prove $\operatorname{Hom}(P, N)$ is finitely generated, and is finitely presented if N is.

Solution: Since P is finitely generated, there is a surjection $R^{\oplus m} \xrightarrow{\alpha} P$ for some m by **(4.10)**. Set $K := \operatorname{Ker}(\alpha)$. Since P is projective, the sequence

$$0 \to K \to R^{\oplus m} \to P \to 0$$

splits by **(5.23)**. Hence $\operatorname{Hom}(P,N) \oplus \operatorname{Hom}(K,N) = \operatorname{Hom}(R^{\oplus m},N)$ by **(4.15.2)**. But $\operatorname{Hom}(R^{\oplus m},N) = \operatorname{Hom}(R,N)^{\oplus m} = N^{\oplus m}$ by **(4.15.2)** and **(4.3)**. So since N is finitely generated, $\operatorname{Hom}(R^{\oplus m},N)$ is finitely generated too. Now, $\operatorname{Hom}(P,N)$ is a quotient of $\operatorname{Hom}(R^{\oplus m},N)$ by **(5.9)**. So $\operatorname{Hom}(P,N)$ is finitely generated too.

Suppose now there is a finite presentation $F_2 \to F_1 \to N \to 0$. Then **(5.22)** and **(5.23)** yield the exact sequence

$$\operatorname{Hom}(R^{\oplus m},F_2) \to \operatorname{Hom}(R^{\oplus m},F_1) \to \operatorname{Hom}(R^{\oplus m},N) \to 0.$$

But the $\operatorname{Hom}(R^{\oplus m},F_i)$ are free of finite rank by **(4.15.1)** and **(4.15.2)**. Thus $\operatorname{Hom}(R^{\oplus m},N)$ is finitely presented.

As above, $\operatorname{Hom}(K,N)$ is finitely generated. Consider the (split) exact sequence

$$0 \to \operatorname{Hom}(K,N) \to \operatorname{Hom}(R^{\oplus m},N) \to \operatorname{Hom}(P,N) \to 0.$$

Thus **(5.28)** implies $\operatorname{Hom}(P,N)$ is finitely presented. □

Exercise **(5.26)**. — Let R be a ring, and $0 \to L \to R^n \to M \to 0$ an exact sequence. Prove M is finitely presented if and only if L is finitely generated.

Solution: Assume M is finitely presented; say $R^l \to R^m \to M \to 0$ is a finite presentation. Let L' be the image of R^l. Then $L' \oplus R^n \simeq L \oplus R^m$ by Schanuel's Lemma **(5.25)**. Hence L is a quotient of $R^l \oplus R^n$. Thus L is finitely generated.

Conversely, assume L is generated by ℓ elements. They yield a surjection $R^\ell \twoheadrightarrow L$ by **(4.10)**(1). It yields a sequence $R^\ell \to R^n \to M \to 0$. The latter is, plainly, exact. Thus M is finitely presented. □

Exercise **(5.27)**. — Let R be a ring, $X_1, X_2, \ldots$ infinitely many variables. Set $P := R[X_1, X_2, \ldots]$ and $M := P/\langle X_1, X_2, \ldots\rangle$. Is M finitely presented? Explain.

Solution: No, otherwise by **(5.26)**, the ideal $\langle X_1, X_2, \ldots\rangle$ would be generated by some $f_1, \ldots, f_n \in P$, so also by $X_1, \ldots, X_m$ for some m, but plainly it isn't. □

Exercise **(5.29)**. — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with M finitely generated and N finitely presented. Prove L is finitely generated.

Solution: Let R be the ground ring. Say M is generated by m elements. They yield a surjection $\mu\colon R^m \twoheadrightarrow M$ by **(4.10)**(1). As in **(5.28)**, μ induces the following commutative diagram, with λ surjective:

$$\begin{array}{ccccccccc}
0 & \to & K & \to & R^m & \to & N & \to & 0 \\
 & & {\scriptstyle\lambda}\downarrow & & {\scriptstyle\mu}\downarrow & & {\scriptstyle 1_N}\downarrow & & \\
0 & \to & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \to & 0
\end{array}$$

By **(5.26)**, K is finitely generated. Thus L is too, as λ is surjective. □

Exercise **(5.36)**. — Let R be a ring, and $a_1, \ldots, a_m \in R$ with $\langle a_1\rangle \supset \cdots \supset \langle a_m\rangle$. Set $M := (R/\langle a_1\rangle) \oplus \cdots \oplus (R/\langle a_m\rangle)$. Show that $F_r(M) = \langle a_1 \cdots a_{m-r}\rangle$.

Solution: Form the presentation $R^m \xrightarrow{\alpha} R^m \to M \to 0$ where α has matrix

$$\mathbf{A} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_m \end{pmatrix}$$

Set $s := m - r$. Now, $a_i \in \langle a_{i-1}\rangle$ for all $i > 1$. Hence $a_{i_1} \cdots a_{i_s} \in \langle a_1 \cdots a_s\rangle$ for all $1 \le i_1 < \cdots < i_s \le m$. Thus $I_s(\mathbf{A}) = \langle a_1 \cdots a_s\rangle$, as desired. □

Exercise **(5.37)**. — In the setup of **(5.36)**, assume a_1 is a nonunit.

(1) Show that m is the smallest integer such that $F_m(M) = R$.

(2) Let n be the largest integer such that $F_n(M) = \langle 0\rangle$; set $k := m - n$. Assume R is a domain. Show (a) that $a_i \neq 0$ for $i < k$ and $a_i = 0$ for $i \geq k$, and (b) that M determines each a_i up to unit multiple.

Solution: For (1), note there's a presentation $R^m \to R^m \to M \to 0$; see the solution to **(5.36)**. So $F_m(M) = R$ by **(5.35)**. On the other hand, $F_{m-1}(M) = \langle a_1\rangle$ by **(5.36)**. So $F_{m-1}(M) \neq R$ as a_1 is a nonunit. Thus (1) holds.

For (2)(a), note $F_{n+1}(M) \neq \langle 0\rangle$ and $F_n(M) = \langle 0\rangle$. Hence $a_1 \cdots a_{k-1} \neq 0$ and $a_1 \cdots a_k = 0$ by **(5.36)**. But R is a domain. Hence $a_1, \ldots, a_i \neq 0$ for $i < k$ and $a_k = 0$. But $\langle a_k\rangle \supset \cdots \supset \langle a_m\rangle$. Hence $a_i = 0$ for $i \geq k$. Thus (2)(a) holds.

For (2)(b), given $b_1, \ldots, b_p \in R$ with b_1 a nonunit, with $\langle b_1\rangle \supset \cdots \supset \langle b_p\rangle$ and $M = (R/\langle b_1\rangle) \oplus \cdots \oplus (R/\langle b_p\rangle)$, note that (1) yields $p = m$ and that (2)(a) yields $b_i \neq 0$ for $i < k$ and $b_i = 0$ for $i \geq k$.

Given i, **(5.36)** yields $\langle a_1 \cdots a_i\rangle = \langle b_1 \cdots b_i\rangle$. But R is a domain. So **(2.12)** yields a unit u_i such that $a_1 \cdots a_i = u_i b_1 \cdots b_i$. So

$$u_{i-1} b_1 \cdots b_{i-1} a_i = u_r b_1 \cdots b_i.$$

If $i < k$, then $b_1 \cdots b_{i-1} \neq 0$; whence, $u_{i-1} a_i = u_i b_i$. Thus (2)(b) holds. □

6. Direct Limits

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

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B, C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B), F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A, C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A), F(C)\big) \end{array} \tag{6.3.1}$$

(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: In **(6.3.1)**, 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 **(6.3.1)** commutes. Thus (1) holds if and only if **(6.3.1)**.

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 $F'Fg \circ \eta_A = \varphi_{A,FB}(Fg)$ in $\mathrm{Hom}_{\mathcal{C}}(A, F'FB)$. Follow 1_{FB} out of the upper right corner to find $\varphi_{A,FB}(Fg) = \eta_B \circ g$ 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:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}'}(FA, FA) & \xrightarrow{f'_*} & \mathrm{Hom}_{\mathcal{C}'}(FA, A') \\ {\scriptstyle \varphi_{A,FA}}\downarrow & & \downarrow{\scriptstyle \varphi_{A,A'}} \\ \mathrm{Hom}_{\mathcal{C}}(A, F'FA) & \xrightarrow{(F'f')_*} & \mathrm{Hom}_{\mathcal{C}}(A, F'A') \end{array}$$

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:

$$\psi_{A,A'}\colon \mathrm{Hom}_{\mathcal{C}'}(FA, A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(A, F'A').$$

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 $X_1, \ldots, X_n$, then $\eta_A(X_i)$ is just X_i viewed in $R[X_1, \ldots, X_n]$. □

Exercise **(6.9)**. — Let $\alpha\colon L \to M$ and $\beta\colon L \to N$ be two maps in a category $\mathcal{C}$. Their **pushout** is defined as the object of $\mathcal{C}$ universal among objects 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 ((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-mod)), the pushout is equal to 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 nonidentity 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

$$\begin{tikzcd} N \arrow[d, "\eta_\nu"'] & L \arrow[l, "\beta"'] \arrow[r, "\alpha"] \arrow[d, "\eta_\lambda"'] & M \arrow[d, "\eta_\mu"'] \\ Q & Q \arrow[l, "1_R"'] \arrow[r, "1_R"] & Q \end{tikzcd} \quad \text{as} \quad \begin{tikzcd} L \arrow[r, "\alpha"] \arrow[d, "\beta"'] & M \arrow[d, "\eta_\mu"'] \\ N \arrow[r, "\eta_\nu"] & Q \end{tikzcd}$$

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 $\gamma' : M \to P$ and $\delta' : N \to P$, 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 $\iota_M\alpha(\ell) - \iota_N\beta(\ell) = (\alpha(\ell), -\beta(\ell))$. Hence $\iota_M\alpha(\ell) - \iota_N\beta(\ell)$ is in $\mathrm{Im}(L)$. Hence, $\iota_M\alpha(\ell)$ and $\iota_N\beta(\ell)$ have the same image in the quotient. Thus $\gamma\alpha = \delta\beta$. Given $\gamma' : M \to P$ and $\delta' : N \to P$, they define a unique map $M \oplus N \to P$, and it factors through the quotient if and only if $\gamma'\alpha = \delta'\beta$. Thus $(M \oplus N)/\mathrm{Im}(L)$ 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: Consider (1). 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 $\theta_{\sigma,\lambda} : M_{\sigma,\lambda} \to N_{\sigma,\lambda}$ such that, for every map $(\sigma, \lambda) \to (\tau, \mu)$, the square

$$\begin{tikzcd} M_{\sigma\lambda} \arrow[r] \arrow[d, "\theta_{\sigma,\lambda}"'] & M_{\tau\mu} \arrow[d, "\theta_{\tau,\mu}"] \\ N_{\sigma\lambda} \arrow[r] & N_{\tau\mu} \end{tikzcd}$$

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.

As to (2), 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 $\varinjlim_{\lambda\in\Lambda} : \mathcal{C}^\Lambda \to \mathcal{C}$ and $\varinjlim_{\sigma\in\Sigma} : (\mathcal{C}^\Lambda)^\Sigma \to \mathcal{C}^\Lambda$ 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-mod)), and $\{\theta_\lambda : M_\lambda \to N_\lambda\}$ a natural transformation. Show

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

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

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\mu_2"] \arrow[d, "\mu_2"] & \mathbb{Z} \arrow[r] \arrow[d, "\mu_2"] & \mathbb{Z}/\langle 2\rangle \arrow[r] \arrow[d, "\mu_2"] & 0 \\ \mathbb{Z} \arrow[r, "\mu_2"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/\langle 2\rangle \arrow[r] & 0 \end{tikzcd}$$

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 λ, $\mu \in \Lambda$, 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 $M = \varinjlim M_\lambda$.

Solution: Let us prove that M has the UMP characterizing $\varinjlim M_\lambda$. Given homomorphisms $\beta_\lambda : M_\lambda \to P$ with $\beta_\lambda = \beta_\nu|M_\lambda$ when $\lambda \le \nu$, define $\beta : M \to P$ 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 $M_\lambda, M_\mu \subset M_\nu$, then $\beta_\lambda(m) = \beta_\nu(m) = \beta_\mu(m)$; so β is well defined. Clearly, $\beta : M \to P$ 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)**. $\square$

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 $\alpha^m_n \colon N_m \to N_n$ by $\alpha^m_n(x) := xs \pmod{n}$. Show $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$.

Solution: For each $n \in \Lambda$, set $Q_n := M_n/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. If $n = ms$, then clearly Diagram **(7.5.1)** induces this one:

$$\begin{array}{ccc} N_m & \xrightarrow{\alpha^m_n} & N_n \\ {\scriptstyle\gamma_m}\downarrow{\scriptstyle\simeq} & & {\scriptstyle\gamma_n}\downarrow{\scriptstyle\simeq} \\ Q_m & \xhookrightarrow{\eta^m_n} & Q_n \end{array}$$

where η^m_n 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 $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$. $\square$

Exercise **(7.9)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings.

(1) Prove that $R = 0$ if and only if $R_\lambda = 0$ for some λ.
(2) Assune that each R_λ is a domain. Prove that R is a domain.
(3) Assume that each R_λ is a field. Prove that R is a field.

Solution: For (1), first assume $R = 0$. Fix any κ. Then $1 \in R_\kappa$ maps to $0 \in R$. So **(7.8)**(3) with $\mathbb{Z}$ for R yields some transition map $\alpha^\kappa_\lambda \colon R_\kappa \to R_\lambda$ with $\alpha^\kappa_\lambda 1 = 0$. But $\alpha^\kappa_\lambda 1 = 1$. Thus $1 = 0$ in R_λ. So $R_\lambda = 0$ by **(1.1)**.

Conversely, assume $R_\lambda = 0$. Then $1 = 0$ in R_λ. So $1 = 0$ in R, as the transition map $\alpha_\lambda \colon R_\lambda \to R$ carries 1 to 1 and 0 to 0. Thus $R = 0$ by **(1.1)**. Thus (1) holds.

In (2), given $x, y \in R$ with $xy = 0$, we can lift x, y back to some $x_\lambda, y_\lambda \in R_\lambda$ for some λ by **(7.8)**(1) and **(7.1)**(1). Then $x_\lambda y_\lambda$ maps to $0 \in R$. So **(7.8)**(3) yields a transition map α^λ_μ with $\alpha^\lambda_\mu(x_\lambda y_\lambda) = 0$ in R_μ. But $\alpha^\lambda_\mu(x_\lambda y_\lambda) = \alpha^\lambda_\mu(x_\lambda)\alpha^\lambda_\mu(y_\lambda)$, and R_μ is a domain. So either $\alpha^\lambda_\mu(x_\lambda) = 0$ or $\alpha^\lambda_\mu(y_\lambda) = 0$. Hence, either $x = 0$ or $y = 0$. Thus R is a domain. Thus (2) holds.

For (3), given $x \in R - 0$, we can lift x back to some $x_\lambda \in R_\lambda$ for some λ by **(7.8)**(1). Then $x_\lambda \neq 0$ as $x \neq 0$. But R_λ is a field. So there is $y_\lambda \in R_\lambda$ with $x_\lambda y_\lambda = 1$. Say y_λ maps to $y \in R$. Then $xy = 1$. So R is a field. Thus (3) holds. $\square$

Exercise **(7.10)**. — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha^\lambda_\mu \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$. For each λ, let $N_\lambda \subset M_\lambda$ be a submodule, and let $N \subset M$ be a submodule. Prove that $N_\lambda = \alpha_\lambda^{-1}N$ for all λ if and only if (a) $N_\lambda = (\alpha^\lambda_\mu)^{-1}N_\mu$ for all α^λ_μ and (b) $\bigcup \alpha_\lambda N_\lambda = N$.

Solution: First, assume $N_\lambda = \alpha_\lambda^{-1}N$ for all λ. Recall $\alpha_\lambda = \alpha_\mu\alpha^\lambda_\mu$ for all α^λ_μ. So $\alpha_\lambda^{-1}N = (\alpha^\lambda_\mu)^{-1}\alpha_\mu^{-1}N$. Thus (a) holds.

Further, $N_\lambda = \alpha_\lambda^{-1}N$ implies $\alpha_\lambda N_\lambda \subset N$. So $\bigcup \alpha_\lambda N_\lambda \subset N$. Finally, for any $m \in M$, there is λ and $m_\lambda \in M_\lambda$ with $m = \alpha_\lambda m_\lambda$ by **(7.8)**(1). But $N_\lambda := \alpha_\lambda^{-1}N$; hence, if $m \in N$, then $m_\lambda \in N_\lambda$, so $m \in \alpha_\lambda N_\lambda$. Thus (b) holds too.

Conversely, assume (b). Then $\alpha_\lambda N_\lambda \subset N$, or $N_\lambda \subset \alpha_\lambda^{-1}N$, for all λ.

Assume (a) too. Given λ and $m_\lambda \in \alpha_\lambda^{-1}N$, note $\alpha_\lambda m_\lambda \in N = \bigcup \alpha_\mu N_\mu$. So there is μ and $n_\mu \in N_\mu$ with $\alpha_\mu n_\mu = \alpha_\lambda m_\lambda$. So **(7.8)**(2) yields ν and α^μ_ν and α^λ_ν with $\alpha^\mu_\nu n_\mu = \alpha^\lambda_\nu m_\lambda$. But $\alpha^\mu_\nu N_\mu \subset N_\nu$ and $(\alpha^\lambda_\nu)^{-1}N_\nu = N_\lambda$ by (a). Hence $m_\lambda \in N_\lambda$. Thus $N_\lambda \supset \alpha_\lambda^{-1}N$. Thus $N_\lambda = \alpha_\lambda^{-1}N$, as desired. $\square$

Exercise **(7.15)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings, $\mathfrak{a}_\lambda \subset R_\lambda$ an ideal for each λ. Assume $\alpha^\lambda_\mu \mathfrak{a}_\lambda \subset \mathfrak{a}_\mu$ for each transition map α^λ_μ. Set $\mathfrak{a} := \varinjlim \mathfrak{a}_\lambda$. If each $\mathfrak{a}_\lambda$ is prime, show $\mathfrak{a}$ is prime. If each $\mathfrak{a}_\lambda$ is maximal, show $\mathfrak{a}$ is maximal.

Solution: The functor $\lambda \mapsto \mathfrak{a}_\lambda$ induces functors $\lambda \mapsto \mathfrak{a}_\lambda$ and $\lambda \mapsto (R_\lambda/\mathfrak{a}_\lambda)$. So **(7.7)** implies that $\mathfrak{a} := \varinjlim \mathfrak{a}_\lambda$ and $\varinjlim(R_\lambda/\mathfrak{a}_\lambda)$ exist, and **(7.14)** implies that $\varinjlim(R_\lambda/\mathfrak{a}_\lambda) = R/\mathfrak{a}$. Thus **(7.9)** yields the assertions. $\square$

Exercise **(7.16)**. — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha^\lambda_\mu \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$. Let $N_\lambda \subset M_\lambda$ be a be a submodule for all λ. Assume $\alpha^\lambda_\mu N_\lambda \subset N_\mu$ for all α^λ_μ. Prove $\varinjlim N_\lambda = \bigcup \alpha_\lambda N_\lambda$.

Solution: The functor $\lambda \mapsto M_\lambda$ induces a functor $\lambda \mapsto N_\lambda$. So $\varinjlim N_\lambda$ exists by **(7.7)**. Also, by **(7.14)**, the inclusions $N_\lambda \hookrightarrow M_\lambda$ induce an injection $\varinjlim N_\lambda \hookrightarrow M$ such that the insertions $\alpha_\lambda \colon M_\lambda \to M$ restrict to the insertions $\mathbb{N}_\lambda \to \varinjlim N_\lambda$. Hence $\varinjlim N_\lambda \supset \bigcup \alpha_\lambda N_\lambda$. Finally, let $n \in \varinjlim N_\lambda$. Then **(7.8)**(1) yields a λ and a $n_\lambda \in N_\lambda$ with $n = \alpha_\lambda n_\lambda \in \alpha_\lambda N_\lambda$. Thus $\varinjlim N_\lambda = \bigcup \alpha_\lambda N_\lambda$. $\square$

Exercise **(7.17)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Prove that

$$\varinjlim \operatorname{nil}(R_\lambda) = \operatorname{nil}(R).$$

Solution: Set $\mathfrak{n}_\lambda := \operatorname{nil}(R_\lambda)$ and $\mathfrak{n} := \operatorname{nil}(R)$. As usual, denote the transition maps by $\alpha^\lambda_\mu \colon R_\lambda \to R_\mu$ and the insertions by $\alpha_\lambda \colon R_\lambda \to R$. Then $\alpha^\lambda_\mu \mathfrak{n}_\lambda \subset \mathfrak{n}_\mu$ for all α^λ_μ. So **(7.16)** yields $\varinjlim \mathfrak{n}_\lambda = \bigcup \alpha_\lambda \mathfrak{n}_\lambda$. Now, $\alpha_\lambda \mathfrak{n}_\lambda \subset \mathfrak{n}$ for all λ. So $\bigcup \alpha_\lambda \mathfrak{n}_\lambda \subset \mathfrak{n}$.

Conversely, given $x \in \mathfrak{n}$, say $x^n = 0$. Then **(7.8)**(1) yields λ and $x_\lambda \in R_\lambda$ with $\alpha_\lambda x_\lambda = x$. So $\alpha_\lambda x_\lambda^n = 0$. So **(7.8)**(3) yields α^λ_μ with $\alpha^\lambda_\mu x_\lambda^n = 0$. Set $x_\mu := \alpha^\lambda_\mu x_\lambda$. Then $x_\mu^n = 0$. So $x_\mu \in \mathfrak{n}_\mu$. Thus $x \in \alpha_\mu \mathfrak{n}_\mu$. Thus $\bigcup \alpha_\lambda \mathfrak{n}_\lambda = \mathfrak{n}$, as desired. $\square$

Exercise **(7.18)**. — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Assume each ring R_λ is local, say with maximal ideal $\mathfrak{m}_\lambda$, and assume each transition map $\alpha^\lambda_\mu \colon R_\lambda \to R_\mu$ is local. Set $\mathfrak{m} := \varinjlim \mathfrak{m}_\lambda$. Prove that R is local with maximal ideal $\mathfrak{m}$ and that each insertion $\alpha_\lambda \colon R_\lambda \to R$ is local.

Solution: As each α^λ_μ is local, $(\alpha^\lambda_\mu)^{-1}\mathfrak{m}_\lambda = \mathfrak{m}_\mu$. So $\alpha^\lambda_\mu \mathfrak{m}_\lambda \subset \mathfrak{m}_\mu$. So **(7.16)** yields $\mathfrak{m} = \bigcup \alpha_\lambda \mathfrak{m}_\lambda$. Now, given $x \in R - \mathfrak{m}$, there is λ and $x_\lambda \in R_\lambda$ with $\alpha_\lambda x_\lambda = x$ by **(7.8)**(1). Then $x_\lambda \notin \mathfrak{m}_\lambda$ as $x \notin \mathfrak{m} = \bigcup \alpha_\lambda \mathfrak{m}_\lambda$. So x_λ is invertible as R_λ is local with maximal ideal $\mathfrak{m}_\lambda$. Hence x is invertible. Thus R is local with maximal ideal $\mathfrak{m}$ by **(3.5)**. Finally, **(7.10)** yields $\alpha_\lambda^{-1}\mathfrak{m} = \mathfrak{m}_\lambda$; that is, α_λ is local. $\square$

Exercise **(7.20)**. — 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 **(7.21)**. — Show that every R-module M is the filtered direct limit over a directed set of finitely presented modules.

Solution: By **(5.20)**, 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 $M_\lambda := \mathrm{Coker}(\alpha_\lambda)$. Then M_λ is finitely presented.

For $i = 1, 2$, the projection $C_i\colon \Lambda \to \Lambda_i$ is surjective, so cofinal. Hence, **(7.20)** 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 **(8.4)**. — Let R be a ring, R' an R- algebra, and M an R'-module. Set $M' := R' \otimes_R M$. Define $\alpha\colon M \to M'$ by $\alpha m := 1 \otimes m$. Prove M is a direct summand of M' with $\alpha = \iota_M$, and find the retraction (projection) $\pi_M\colon M' \to M$.

Solution: As the canonical map $R' \times M \to M'$ is bilinear, α is linear. Define $\mu\colon M \times R' \to M$ by $\mu(x, m) := xm$. Plainly μ is R-bilinear. So μ induces an R-linear map $\rho : M' \to M$. Then ρ is a retraction of α, as $\rho(\alpha(m)) = 1 \cdot m$. Let $\beta\colon M \to \mathrm{Coker}(\alpha)$ be the quotient map. Then **(5.9)** implies that M is a direct summand of M' with $\alpha = \iota_M$ and $\rho = \pi_M$. □

Exercise **(8.7)**. — Let R be a domain, $\mathfrak{a}$ a nonzero ideal. Set $K := \mathrm{Frac}(R)$. Show that $\mathfrak{a} \otimes_R K = K$.

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 **(8.9)**. — 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 is equal to $\mathrm{Ker}(\tau)$, and τ is surjective. Show τ 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 **(8.8)**, there is an R'-structure on $M \otimes_R N$ with $y'(m \otimes n) = m \otimes (y'n)$, and so by **(8.6)**(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 $\mathrm{Ker}(\tau)$ 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 $\mathrm{Ker}(\tau)$ vanishes. Thus τ is an isomorphism. □

Exercise **(8.12)**. — In the setup of **(8.11)**, find the unit η_M of each adjunction.

Solution: Consider the left adjoint $FM := M \otimes_R R'$ of restriction of scalars. A map $\theta\colon FM \to P$ corresponds to the map $M \to P$ carrying m to $\theta(m \otimes 1_{R'})$. Take $P := FM$ and $\theta := 1_{FM}$. Thus $\eta_M\colon M \to FM$ is given by $\eta_M m = m \otimes 1_{R'}$.

Consider the right adjoint $F'P := \mathrm{Hom}_R(R', P)$ of restriction of scalars. A map $\mu\colon M \to P$ corresponds to the map $M \to F'P$ carrying m to the map $\nu : R' \to P$ defined by $\nu x := x(\mu m)$. Take $P := M$ and $\mu := 1_M$. Thus $\eta_M\colon M \to F'M$ is given by $(\eta_M m)(x) = xm$. □

Exercise **(8.15)**. — Let M and N be nonzero k-vector spaces. Prove $M\otimes N \neq 0$.

Solution: Vector spaces are free modules; say $M = k^{\oplus\Phi}$ and $N = k^{\oplus\Psi}$. Then **(8.13)** yields $M \otimes N = k^{\oplus(\Phi\times\Psi)}$ as $k \otimes k = k$ by **(8.6)**(2). Thus $M \otimes N \neq 0$. □

Exercise **(8.16)**. — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module.

(1) Use **(8.13)** 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 **(8.13)** 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 **(8.6)**(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 $\mathfrak{a}(R/\mathfrak{b}) = (\mathfrak{a} + \mathfrak{b})/\mathfrak{b}$ by **(4.8.1)**. So

$$R/\mathfrak{a} \otimes R/\mathfrak{b} = (R/\mathfrak{b})\big/((\mathfrak{a} + \mathfrak{b})/\mathfrak{b}).$$

The latter is equal to $R/(\mathfrak{a} + \mathfrak{b})$ by **(4.8.2)**. □

Exercise **(8.17)**. — Show $\mathbb{Z}/\langle m\rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle n\rangle = 0$ if m and n are relatively prime.

Solution: The hypothesis yields $\langle m\rangle + \langle n\rangle = \mathbb{Z}$. Thus **(8.16)**(2) yields

$$\mathbb{Z}/\langle m\rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle n\rangle = \mathbb{Z}/\big(\langle m\rangle + \langle n\rangle\big) = 0. \qquad \square$$

Exercise **(8.19)**. — 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 from the characterization of the direct sum of two modules in terms of maps **(4.18)**, since F preserves the relations there.

The second assertion follows from the first via the second part of the proof of Watt's Theorem **(8.18)**, but with Σ and Λ finite. $\square$

Exercise **(8.24)**. — Let R be a ring, M a module, X a variable. Let $M[X]$ be the set of polynomials in X with coefficients in M, that is, expressions of the form $\sum_{i=0}^{n} m_i X^i$ with $m_i \in M$. Prove $M \otimes_R R[X] = M[X]$ as $R[X]$-modules.

Solution: Plainly, $M[X]$ is an $R[X]$-module. Define $b\colon M \times R[X] \to M[X]$ by $b(m, \sum a_i X^i) := \sum a_i m X^i$. Then b is R-bilinear, so induces an R-linear map $\beta\colon M \otimes_R R[X] \to M[X]$. Plainly, β is $R[X]$-linear. By **(8.21)**, any $t \in M \otimes_R R[X]$ can be written as $t = \sum m_i \otimes X^i$ for some $m_i \in M$. Then $\beta t = \sum m_i X^i$. If $\beta t = 0$, then $m_i = 0$ for all i, and so $t = 0$. Given $u := \sum m_i X^i \in M[X]$, set $t := \sum m_i \otimes X^i$. Then $\beta t = u$. Thus β is bijective, as desired.

Alternatively, for any $R[X]$-module P, define an R-linear map

$$\varphi_{M,P}\colon \operatorname{Hom}_{R[X]}(M[X], P) \to \operatorname{Hom}_R(M, P) \quad \text{by} \quad \varphi_{M,P}\alpha := \alpha|M.$$

If $\varphi_{M,P}\alpha = 0$, then $\alpha(\sum m_i X^i) = \sum (\alpha m_i) X^i = 0$, because α is $R[X]$-linear and $\alpha|M = 0$; thus $\varphi_{M,P}$ is injective. Given $\gamma\colon M \to P$, define $\alpha\colon M[X] \to P$ by $\alpha(\sum m_i X^i) = \sum \gamma(m_i) X^i$. Then α is $R[X]$-linear, and $\varphi_{M.P}\alpha = \gamma$. Thus $\varphi_{M,P}$ is surjective, so bijective. Thus $M \mapsto M[X]$ is a left adjoint of restriction of scalars. But $M \mapsto M \otimes_R R[X]$ is too by **(8.11)**. Thus $M[X] = M \otimes_R R[X]$. $\square$

Exercise **(8.25)**. — Let R be a ring, $(R'_\sigma)_{\sigma\in\Sigma}$ a family of algebras. For each finite subset J of Σ, let R'_J be the tensor product of the R'_σ for $\sigma \in J$. Prove that the assignment $J \mapsto R'_J$ extends to a filtered direct system and that $\varinjlim R'_J$ exists and is the coproduct of the family $(R'_\sigma)_{\sigma\in\Sigma}$.

Solution: Let Λ be the set of subsets of Σ, partially ordered by inclusion. Then Λ is a filtered small category by **(7.1)**. Further, the assignment $J \mapsto R'_J$ extends to a functor from Λ to $((R\text{-alg}))$ as follows: by induction, **(8.22)** implies that R'_J is the coproduct of the family $(R'_\sigma)_{\sigma\in J}$, so that, first, for each $\sigma \in J$, there is a canonical algebra map $\iota_\sigma\colon R'_\sigma \to R'_J$, and second, given $J \subset K$, the ι_σ for $\sigma \in K$ induce an algebra map $\alpha^J_K\colon R'_J \to R'_K$. So $\varinjlim R'_J$ exists in $((R\text{-alg}))$ by **(7.7)**.

Given a family of algebra maps $\varphi_\sigma\colon R'_\sigma \to R''$, for each J, there is a compatible map $\varphi_J\colon R'_J \to R''$, since R'_J is the coproduct of the R'_σ. Further, the various φ_J are compatible, so they induce a compatible map $\varphi\colon \varinjlim R'_J \to R''$. Thus $\varinjlim R'_J$ is the coproduct of the R'_σ. $\square$

Exercise **(8.26)**. — 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 **(8.23)**. So **(8.6)**(2) and **(8.11)** and **(8.16)**(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:

$$X^3 - 2 = \big(X - \sqrt[3]{2}\big)\big(X - \omega\sqrt[3]{2}\big)\big(X - \omega^2\sqrt[3]{2}\big).$$

So the Chinese Remainder Theorem, **(1.14)**, 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 **(1.8)**. $\square$

9. Flatness

Exercise **(9.4)**. — Let R be a ring, R' an algebra, F an R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Assume F is exact. Prove the following equivalent:

(1) F is faithful.
(2) An R-module M vanishes if FM does.
(3) $F(R/\mathfrak{m}) \neq 0$ for every maximal ideal $\mathfrak{m}$ of R.
(4) A sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ is exact if $FM' \xrightarrow{F\alpha} FM \xrightarrow{F\beta} FM''$ is.

Solution: To prove (1) implies (2), suppose $FM = 0$. Then $1_{FM} = 0$. But always $1_{FM} = F(1_M)$. Hence (1) yields $1_M = 0$. So $M = 0$. Thus (2) holds.

Conversely, assume (2). Given $\alpha\colon M \to N$ with $F\alpha = 0$, set $I := \operatorname{Im}(\alpha)$. As F is exact, **(9.3)** yields $FI = \operatorname{Im}(F\alpha)$. Hence $FI = 0$. So (2) yields $I = 0$. Thus $\alpha = 0$. Thus (1) holds. Thus (1) and (2) are equivalent.

To prove (2) implies (3), take $M := R/\mathfrak{m}$.

Conversely, assume (3). Given $0 \neq m \in M$, form $\alpha\colon R \to M$ by $\alpha(x) := xm$. Set $\mathfrak{a} := \operatorname{Ker}(\alpha)$. Let $\mathfrak{m} \supset \mathfrak{a}$ be a maximal ideal. We get a surjection $R/\mathfrak{a} \twoheadrightarrow R/\mathfrak{m}$ and an injection $R/\mathfrak{a} \hookrightarrow M$. They induce a surjection $F(R/\mathfrak{a}) \twoheadrightarrow F(R/\mathfrak{m})$ and an injection $F(R/\mathfrak{a}) \hookrightarrow FM$ as F is exact. But $F(R/\mathfrak{m}) \neq 0$ by (3). So $F(R/\mathfrak{a}) \neq 0$. So $FM \neq 0$. Thus (2) holds. Thus (1) and (2) and (3) are equivalent.

To prove (1) implies (4), set $I := \operatorname{Im}(\alpha)$ and $K := \operatorname{Ker}(\beta)$. Now, $F(\beta\alpha) = 0$. So (1) yields $\beta\alpha = 0$. Hence $I \subset K$. But F is exact; so $F(K/I) = FK/FI$, and **(9.3)** yields $FI = \operatorname{Im}(F\alpha)$ and $FK = \operatorname{Ker}(F\beta)$. Hence $F(K/I) = 0$. But (1) implies (2). So $K/I = 0$. Thus (4) holds.

Conversely, assume (4). Given $\alpha\colon M \to N$ with $F\alpha = 0$, set $K := \operatorname{Ker}(\alpha)$. As F is exact, **(9.3)** yields $FK = \operatorname{Ker}(F\alpha)$. Hence $FK \to FM \to 0$ is exact. So (4) implies $K \to M \to 0$ is exact. So $\alpha = 0$. Thus (1) holds, as desired. $\square$

Exercise **(9.8)**. — Show that a ring of polynomials P is faithfully flat.

Solution: The monomials form a free basis, so P is faithfully flat by **(9.7)**. □

Exercise **(9.10)**. — Let R be a ring, M and N flat modules. Show that $M \otimes N$ is flat. What if "flat" is replaced everywhere by "faithfully flat"?

Solution: Associativity **(8.10)** yields $(M \otimes N) \otimes \bullet = M \otimes (N \otimes \bullet)$; in other words, $(M \otimes N) \otimes \bullet = (M \otimes \bullet) \circ (N \otimes \bullet)$. So $(M \otimes N) \otimes \bullet$ is the composition of two exact functors. Hence it is exact. Thus $M \otimes N$ is flat.

Similarly if M and N are faithfully flat, then $M \otimes N \otimes \bullet$ is faithful and exact. So $M \otimes N$ is faithfully flat. □

Exercise **(9.11)**. — Let R be a ring, M a flat module, R' an algebra. Show that $M \otimes_R R'$ is flat over R'. What if "flat" is replaced everywhere by "faithfully flat"?

Solution: Cancellation **(8.11)** yields $(M \otimes_R R') \otimes_{R'} \bullet = M \otimes_R \bullet$. But $M \otimes_R \bullet$ is exact, as M is flat over R. Thus $M \otimes_R R'$ is flat over R'.

Similarly, if M is faithfully flat over R, then $M \otimes_R \bullet$ is faithful too. Thus $M \otimes_R R'$ is faithfully flat over R'. □

Exercise **(9.12)**. — Let R be a ring, R' a flat algebra, M a flat R'-module. Show that M is flat over R. What if "flat" is replaced everywhere by "faithfully flat"?

Solution: Cancellation **(8.11)** yields $M \otimes_R \bullet = M \otimes_{R'} (R' \otimes_R \bullet)$. But $R' \otimes_R \bullet$ and $M \otimes_{R'} \bullet$ are exact; so their composition $M \otimes_R \bullet$ is too. Thus M is flat over R.

Similarly, as the composition of two faithful functors is, plainly, faithful, the assertion remains true if "flat" is replaced everywhere by "faithfully flat." □

Exercise **(9.13)**. — Let R be a ring, R' an algebra, R'' an R'-algebra, and M an R''-module. Assume that M is flat over R and faithfully flat over R'. Prove that R' is flat over R.

Solution: Let $N' \to N$ be an injective map of R-modules. Then the map $N' \otimes_R M \to N \otimes_R M$ is injective as M is flat over R. But by Cancellation **(8.11)**, that map is equal to this one:

$$(N' \otimes_R R') \otimes_{R'} M \to (N \otimes_R R') \otimes_{R'} M.$$

And M is faithfully flat over R'. Hence the map $N' \otimes_R R' \to N \otimes_R R'$ is injective by **(9.4)**. Thus R' is flat over R. □

Exercise **(9.14)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $R/\mathfrak{a}$ is flat. Show $\mathfrak{a} = \mathfrak{a}^2$.

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 **(8.16)**. Hence $\mathfrak{a}/\mathfrak{a}^2 = 0$. Thus $\mathfrak{a} = \mathfrak{a}^2$. □

Exercise **(9.15)**. — Let R be a ring, R' a flat algebra. Prove equivalent:

(1) R' is faithfully flat over R.
(2) For every R-module M, the map $M \xrightarrow{\alpha} M \otimes_R R'$ by $\alpha m = m \otimes 1$ is injective.
(3) Every ideal $\mathfrak{a}$ of R is the contraction of its extension, or $\mathfrak{a} = \varphi^{-1}(\mathfrak{a}R')$.
(4) Every prime $\mathfrak{p}$ of R is the contraction of some prime $\mathfrak{q}$ of R', or $\mathfrak{p} = \varphi^{-1}\mathfrak{q}$.
(5) Every maximal ideal $\mathfrak{m}$ of R extends to a proper ideal, or $\mathfrak{m}R' \neq R'$.
(6) Every nonzero R-module M extends to a nonzero module, or $M \otimes_R R' \neq 0$.

Solution: Assume (1). In (2), set $K := \operatorname{Ker} \alpha$. Then the canonical sequence

$$0 \longrightarrow K \otimes R' \longrightarrow M \otimes R' \xrightarrow{\alpha \otimes 1} M \otimes R' \otimes R'$$

is exact. But $\alpha \otimes 1$ has a retraction, namely $m \otimes x \otimes y \mapsto m \otimes xy$. So $\alpha \otimes 1$ is injective. Hence $K \otimes_R R' = 0$. So (1) implies $K = 0$ by **(9.4)**. Thus (2) holds.

Assume (2). Then $R/\mathfrak{a} \to (R/\mathfrak{a}) \otimes R'$ is injective. But $(R/\mathfrak{a}) \otimes R' = R'/\mathfrak{a}R'$ by **(8.16)**(1). So $\varphi^{-1}(\mathfrak{a}R') = \mathfrak{a}$. Thus (3) holds.

Assume (3). Then **(3.13)**(2) yields (4).

Assume (4). Then every maximal ideal $\mathfrak{m}$ of R is the contraction of some prime $\mathfrak{q}$ of R'. So $\mathfrak{m}R' \subset \mathfrak{q}$. Thus (5) holds.

Assume (5). Consider (6). Take a nonzero $m \in M$, and set $M' := Rm$. As R' is flat, the inclusion $M' \hookrightarrow M$ yields an injection $M' \otimes R' \hookrightarrow M \otimes R'$.

Note $M' = R/\mathfrak{a}$ for some $\mathfrak{a}$ by **(4.7)**. So $M' \otimes_R R' = R'/\mathfrak{a}R'$ by **(8.16)**(1). Take a maximal ideal $\mathfrak{m} \supset \mathfrak{a}$. Then $\mathfrak{a}R' \subset \mathfrak{m}R'$. But $\mathfrak{m}R' \subsetneqq R'$ by (5). Hence $R'/\mathfrak{a}R' \neq 0$. So $M' \otimes_R R' \neq 0$. Hence $M \otimes R' \neq 0$. Thus (6) holds.

Finally, (6) and (1) are equivalent by **(9.4)**. □

Exercise **(9.17)**. — Let R be a ring, $0 \to M' \xrightarrow{\alpha} M \to M'' \to 0$ an exact sequence with M flat. Assume $N \otimes M' \xrightarrow{N \otimes \alpha} N \otimes M$ is injective for all N. Prove M'' is flat.

Solution: Let $\beta\colon N \to P$ be an injection. It yields the following commutative diagram with exact rows by hypothesis and by **(8.13)**:

$$\begin{tikzcd}
0 \arrow[r] & N \otimes M' \arrow[r] \arrow[d, "\beta \otimes M'"'] & N \otimes M \arrow[r] \arrow[d, "\beta \otimes M"'] & N \otimes M'' \arrow[r] \arrow[d, "\beta \otimes M''"] & 0 \\
0 \arrow[r] & P \otimes M' \arrow[r] \arrow[d] & P \otimes M \arrow[r] \arrow[d] & P \otimes M'' \arrow[r] & 0 \\
0 \arrow[r] & P/N \otimes M' \arrow[r] & P/N \otimes M & &
\end{tikzcd}$$

Since M is flat, $\operatorname{Ker}(\beta \otimes M) = 0$. So the Snake Lemma **(5.13)** applied to the top two rows yields $\operatorname{Ker}(\beta \otimes M'') = 0$. Thus M'' is flat. □

Exercise **(9.18)**. — Prove that an R-algebra R' is faithfully flat if and only if the structure map $\varphi\colon R \to R'$ is injective and the quotient $R'/\varphi R$ is flat over R.

Solution: Assume R' is faithfully flat. Then for every R-module M, the map $M \xrightarrow{\alpha} M \otimes_R R'$ is injective by **(9.15)**. Taking $M := R$ shows φ is injective. And, since R' is flat, $R'/\varphi(R)$ is flat by **(9.17)**.

Conversely, assume φ is injective and $R'/\varphi(R)$ is flat. Then $M \to M \otimes_R R'$ is injective for every module M by **(9.16)**(1), and R' is flat by **(9.16)**(2). Thus R' is faithfully flat by **(9.15)** □

Exercise **(9.21)**. — 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 **(9.20)**, put $P := N \otimes_R R'$ in the second equation in **(8.11)**, and combine the two results. □

Exercise **(9.25)** (*Equational Criterion for Flatness*). — Prove that Condition **(9.24)**(4) can be reformulated as follows: Given any 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

$$\textstyle\sum_j x_{ij} y'_j = y_i \text{ for all } i \text{ and } \sum_i x_{ij} x_i = 0 \text{ for all } j. \qquad \textbf{(9.25.1)}$$

Solution: Assume **(9.24)**(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 **(9.24)**(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 **(9.25.1)** holds.

Conversely, given $\alpha\colon R^m \to M$ and $k \in \mathrm{Ker}(\alpha)$, write $k = \sum x_i e_i$. Assume **(9.25.1)**. 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 **(9.24)**(4) holds. □

Exercise **(9.28)**. — Let R be a ring, M a module. Prove (1) if M is flat, then for $x \in R$ and $m \in M$ with $xm = 0$, necessarily $m \in \mathrm{Ann}(x)M$, and (2) the converse holds if R is a **Principal Ideal Ring** (PIR); that is, every ideal $\mathfrak{a}$ is principal.

Solution: For (1), assume M is flat and $xm = 0$. Then **(9.25)** yields $x_j \in R$ and $m_j \in M$ with $\sum x_j m_j = m$ and $x_j x = 0$ for all j. Thus $m \in \mathrm{Ann}(x)M$.

Alternatively, $0 \to \mathrm{Ann}(x) \to R \xrightarrow{\mu_x} R$ is always exact. Tensoring with M gives $0 \to \mathrm{Ann}(x) \otimes M \to M \xrightarrow{\mu_x} M$, which is exact as M is flat. So $\mathrm{Im}(\mathrm{Ann}(x) \otimes M)$ is $\mathrm{Ker}(\mu_x)$. But always $\mathrm{Im}(\mathrm{Ann}(x) \otimes M)$ is $\mathrm{Ann}(x)M$. Thus (1) holds.

For (2), it suffices, by **(9.26)**, to show $\alpha\colon \mathfrak{a} \otimes M \to \mathfrak{a}M$ is injective. Since R is a PIR, $\mathfrak{a} = \langle x \rangle$ for some $x \in R$. So, given $z \in \mathfrak{a} \otimes M$, there are $y_i \in R$ and $m_i \in M$ such that $z = \sum_i y_i x \otimes m_i$. Set $m := \sum_i y_i m_i$. Then

$$z = \textstyle\sum_i x \otimes y_i m_i = x \otimes \sum_i y_i m_i = x \otimes m.$$

Suppose $z \in \mathrm{Ker}(\alpha)$. Then $xm = 0$. Hence $m \in \mathrm{Ann}(x)M$ by hypothesis. So $m = \sum_j z_j n_j$ for some $z_j \in \mathrm{Ann}(x)$ and $n_j \in M$. Hence

$$z = x \otimes \textstyle\sum_j z_j n_j = \sum_j z_j x \otimes n_j = 0.$$

Thus α is injective. Thus (2) holds. □

10. Cayley–Hamilton Theorem

Exercise **(10.6)**. — Let R be a nonzero ring, $\alpha\colon R^m \to R^n$ a map of free modules. Assume α is surjective. Show that $m \ge n$.

Solution: Let $\mathfrak{m}$ be a maximal ideal. Then α induces a $R^m/\mathfrak{m}R^m \to R^n/\mathfrak{m}R^n$, which is surjective. Plainly, that map can be rewritten as $(R/\mathfrak{m})^m \twoheadrightarrow (R/\mathfrak{m})^n$. But $R/\mathfrak{m}$ is a field. Thus $m \ge n$. □

Exercise **(10.7)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a}$ is finitely generated and idempotent (or $\mathfrak{a} = \mathfrak{a}^2$). Prove there is a unique idempotent e with $\langle e \rangle = \mathfrak{a}$.

Solution: By **(10.3)** with $\mathfrak{a}$ for M, there is $e \in \mathfrak{a}$ such that $(1-e)\mathfrak{a} = 0$. So for all $x \in \mathfrak{a}$, we have $(1-e)x = 0$, or $x = ex$. Thus $\mathfrak{a} = \langle e \rangle$ and $e = e^2$.

Finally, e is unique by **(3.26)**. □

Exercise **(10.8)**. — Let R be a ring, $\mathfrak{a}$ an ideal. Prove the following 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 finitely generated and idempotent.
(4) $\mathfrak{a}$ is generated by an idempotent.
(5) $\mathfrak{a}$ is a direct summand of R.

Solution: Suppose (1) holds. Then $R/\mathfrak{a}$ is flat by **(9.7)**. Further, the sequence $0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$ splits by **(5.23)**. So **(5.9)** yields a surjection $\rho\colon R \to \mathfrak{a}$. Hence $\mathfrak{a}$ is principal. Thus (2) holds.

If (2) holds, then (3) holds by **(9.14)**. If (3) holds, then (4) holds by **(10.7)**. If (4) holds, then (5) holds by **(1.13)**. If (5) holds, then $R \simeq \mathfrak{a} \bigoplus R/\mathfrak{a}$, and so (1) holds by **(5.23)**. □

Exercise **(10.9)**. — Prove the following conditions on a ring R are equivalent:

(1) R is **absolutely flat**; that is, every module is flat.
(2) Every finitely generated ideal is a direct summand of R.
(3) Every finitely generated ideal is idempotent.
(4) Every principal ideal is idempotent.

Solution: Assume (1). Let $\mathfrak{a}$ be a finitely generated ideal. Then $R/\mathfrak{a}$ is flat by hypotheses. So $\mathfrak{a}$ is a direct summand of R by **(10.8)**. Thus (2) holds.

Conditions (2) and (3) are equivalent by **(10.8)**.

Trivially, if (3) holds, then (4) does. Conversely, assume (4). Given a finitely generated ideal $\mathfrak{a}$, say $\mathfrak{a} = \langle x_1, \dots, x_n \rangle$. Then each $\langle x_i \rangle$ is idempotent by hypothesis. So $\langle x_i \rangle = \langle f_i \rangle$ for some idempotent f_i by **(1.17)**(2). Then $\mathfrak{a} = \langle f_1, \dots, f_n \rangle$. Hence $\mathfrak{a}$ is idempotent by **(1.17)**(4), (1). Thus (3) holds.

Assume (2). Let M be a module, and $\mathfrak{a}$ a finitely generated ideal. Then $\mathfrak{a}$ is a direct summand of R by hypothesis. So $R/\mathfrak{a}$ is flat by **(9.6)**. Hence $\mathfrak{a} \otimes M \xrightarrow{\sim} \mathfrak{a}M$ by **(9.16)**(1); cf. the proof of **(8.16)**(1). So M is flat by **(9.26)**. Thus (1) holds. □

Exercise **(10.10)**. — Let R be a ring.

(1) Assume R is Boolean. Prove R is absolutely flat.
(2) Assume R is absolutely flat. Prove any quotient ring R' is absolutely flat.
(3) Assume R is absolutely flat. Prove every nonunit x is a zerodivisor.
(4) Assume R is absolutely flat and local. Prove R is a field.

Solution: In (1), as R is Boolean, every element is idempotent. Hence every principal ideal is idempotent by **(1.17)**(1). Thus **(10.9)** yields (1).

For (2), let $\mathfrak{b} \subset R'$ be principal, say $\mathfrak{b} = \langle \overline{x} \rangle$. Let $x \in R$ lift $\overline{x}$. Then $\langle x \rangle$ is idempotent by **(10.9)**. Hence $\mathfrak{b}$ is also idempotent. Thus **(10.9)** yields (2).

For (3) and (4), take a nonunit x. Then $\langle x \rangle$ is idempotent by **(10.9)**. So $x = ax^2$ for some a. Then $x(ax-1) = 0$. But x is a nonunit. So $ax - 1 \neq 0$. Thus (3) holds.

Suppose R is local, say with maximal ideal $\mathfrak{m}$. Since x is a nonunit, $x \in \mathfrak{m}$. So $ax \in \mathfrak{m}$. So $ax - 1 \notin \mathfrak{m}$. So $ax - 1$ is a unit. But $x(ax-1) = 0$. So $x = 0$. Thus 0 is the only nonunit. Thus (4) holds. □

Exercise **(10.14)**. — Let R be a ring, $\mathfrak{a}$ an ideal, and $\alpha\colon M \to N$ a map of modules. Assume that $\mathfrak{a} \subset \mathrm{rad}(R)$, that N is finitely generated, and that the induced map $\overline{\alpha}\colon M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective. Show that α is surjective.

Solution: Since $\overline{\alpha}$ is surjective, $\alpha(M)+\mathfrak{a}N = N$. Since N is finitely generated, so is $N/\alpha(N)$. Hence $\alpha(M) = N$ by **(10.13)**(1). Thus α is surjective. □

Exercise **(10.15)**. — Let R be a ring, $\mathfrak{m} \subset \mathrm{rad}(R)$ an ideal. Let $\alpha, \beta\colon M \rightrightarrows N$ be two maps of finitely generated modules. Assume that α is an isomorphism and that $\beta(M) \subset \mathfrak{m}N$. Set $\gamma := \alpha+\beta$. Show that γ is an isomorphism.

Solution: As α is surjective, given $n \in N$, there is $m \in M$ with $\alpha(m) = n$. So

$$n = \alpha(m) + \beta(m) - \beta(m) \in \gamma(M) + \mathfrak{m}N.$$

But M/N is finitely generated as M is. Hence $\gamma(M) = N$ by **(10.13)**(1). So $\alpha^{-1}\gamma$ is surjective, and therefore an isomorphism by **(10.4)**. Thus γ is an isomorphism. □

Exercise **(10.16)**. — 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 **(10.13)**, 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. □

Exercise **(10.17)**. — 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 **(8.16)**(1). So (1) is nothing but a form of Nakayama's Lemma **(10.11)**.

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 **(8.15)** and **(8.9)**. But $(M \otimes k) \otimes (N \otimes k) = (M \otimes N) \otimes (k \otimes k)$ by the associative and commutative laws, **(8.10)** and **(8.6)**. Finally, $k \otimes k = k$ by **(8.16)**(1). □

Exercise **(10.19)**. — Let $A \to B$ be a local homomorphism, M a finitely generated B-module. Prove that M is faithfully flat over A if and only if M is flat over A and nonzero. Conclude that, if B is flat over A, then B is faithfully flat over A.

Solution: Plainly, to prove the first assertion, it suffices to show that $M \otimes_A \bullet$ is faithful if and only if $M \neq 0$. Now, if $M \otimes_A \bullet$ is faithful, then $M \otimes N \neq 0$ whenever $N \neq 0$ by **(9.4)**. But $M \otimes A = M$ by the Unitary Law, and $A \neq 0$. Thus $M \neq 0$.

Conversely, suppose $M \neq 0$. Denote the maximal ideals of A and B by $\mathfrak{m}$ and $\mathfrak{n}$. Then $\mathfrak{n}M \neq M$ by Nakayama's Lemma **(10.11)**. But $\mathfrak{m}B \subset \mathfrak{n}$ as $A \to B$ is a local homomorphism. So $M/\mathfrak{m}M \neq 0$. But $M/\mathfrak{m}M = M \otimes (A/\mathfrak{m})$ by **(8.16)**(1). Thus **(9.4)** implies $M \otimes_A \bullet$ is faithful. Finally, the second assertion is the special case with $M := B$. □

Exercise **(10.22)**. — Let G be a finite group of automorphisms of a ring R. Form the subring R^G of invariants. Show that every $x \in R$ is integral over R^G, 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^G, in fact, over its subring R'. □

Exercise **(10.24)**. — 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 $f^2 - 2f_ef + f_e^2 - f_o^2 = 0$. □

Exercise **(10.29)**. — 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 by **(10.28)**. Hence $\prod_{i=1}^n R[y_i]$ is a module-finite R-subalgebra of $\prod_{i=1}^n R_i$ by **(4.16)** and induction on n. Now, $y \in \prod_{i=1}^n R[y_i]$. Therefore, y is integral over R by **(10.28)**. Thus $\prod_{i=1}^n R_i$ is integral over R. □

Exercise **(10.31)**. — 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 **(10.35)**. — 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 **(2.29)**. Hence R is a domain by **(2.9)**, but not a field by **(2.17)**.

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 **(10.28)**.

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 **(10.34)**(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 subset. 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 $1/3 = 1 - (2/3)$. Clearly $S^{-1}\mathbb{Z} = \mathbb{Z}[1/3]$.

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 subset **generated by** P, that is, the smallest multiplicative subset 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 **(1.6)**. □

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 $z \ne 0$, 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 $R'' \ne 0$. □

Exercise **(11.9)**. — Let R be a ring, $S \subset T$ a multiplicative subsets, $\overline{S}$ and $\overline{T}$ their saturations; see **(3.17)**. Set $U := (S^{-1}R)^{\times}$. Show the following:

(1) $U = \{x/s \mid x \in \overline{S} \text{ and } s \in S\}$. (2) $\varphi_S^{-1}U = \overline{S}$.
(3) $S^{-1}R = T^{-1}R$ if and only if $\overline{S} = \overline{T}$. (4) $\overline{S}^{-1}R = S^{-1}R$.

Solution: In (1), given $x \in \overline{S}$ and $s \in S$, take $y \in R$ such that $xy \in S$. Then $x/s \cdot sy/xy = 1$ in $S^{-1}R$. Thus $x/s \in U$. Conversely, say $x/s \cdot y/t = 1$ in $S^{-1}R$ with $x, y \in R$ and $s, t \in S$. Then there's $u \in S$ with $xyu = stu$ in R. But $stu \in S$. Thus $x \in \overline{S}$. Thus (1) holds.

For (1), set $V := \varphi_S^{-1}T$. Then V is saturated multiplicative by **(3.15)**. Further, $V \supset S$ by **(11.1)**. Thus (1)(c) of **(3.17)** yields $V \supset \overline{S}$. Conversely, take $x \in V$. Then $x/1 \in T$. So (1) yields $x/1 = y/s$ with $y \in \overline{S}$ and $s \in S$. So there's $t \in S$ with $xst = yt$ in R. But $\overline{S} \supset S$ by (1)(a) of **(3.17)**, and $\overline{S}$ is multiplicative by (1)(b) of **(3.17)**; so $yt \in \overline{S}$. But $\overline{S}$ is saturated again by (1)(b). Thus $x \in \overline{S}$. Thus $V = \overline{S}$.

In (3), if $S^{-1}R = T^{-1}R$, then (2) implies $\overline{S} = \overline{T}$. Conversely, if $\overline{S} = \overline{T}$, then (4) implies $S^{-1}R = T^{-1}R$.

As to (4), note that, in any ring, a product is a unit if and only if each factor is. So a ring map $\varphi\colon R \to R'$ carries $\overline{S}$ into $R'^{\times}$ if and only if φ carries S into $R'^{\times}$. Thus $\overline{S}^{-1}R$ and $S^{-1}R$ are characterized by equivalent UMPs. Thus (4) holds. □

Exercise **(11.10)**. — Let R be a ring, $S \subset T \subset U$ and W multiplicative subsets.

(1) Show there's a unique R-algebra map $\varphi_T^S\colon S^{-1}R \to T^{-1}R$ and $\varphi_U^T\varphi_T^S = \varphi_U^S$.

(2) Given a map $\varphi\colon S^{-1}R \to W^{-1}R$, show $S \subset \overline{S} \subset \overline{W}$ and $\varphi = \varphi_W^S$.

(3) Let Λ be a set, $S_\lambda \subset S$ a multiplicative subset for all $\lambda \in \Lambda$. Assume $\bigcup S_\lambda = S$. Assume given $\lambda, \mu \in \Lambda$, there is ν such that $S_\lambda, S_\mu \subset S_\nu$. Order Λ by inclusion: $\lambda \le \mu$ if $S_\lambda \subset S_\mu$. Using (1), show $\varinjlim S_\lambda^{-1}R = S^{-1}R$.

Solution: For (1), note $\varphi_T S \subset \varphi_T T \subset (T^{-1}R)^{\times}$. So **(11.5)** yields a unique R-algebra map $\varphi_T^S\colon S^{-1}R \to T^{-1}R$. By uniqueness, $\varphi_U^T\varphi_T^S = \varphi_U^S$. Thus (1) holds.

For (2), note $\varphi(S^{-1}R)^{\times} \subset (W^{-1}R)^{\times}$. So $\varphi_S^{-1}(S^{-1}R)^{\times} \subset \varphi_W^{-1}(W^{-1}R)^{\times}$. But $\varphi_S^{-1}(S^{-1}R)^{\times} = \overline{S}$ and $\varphi_W^{-1}(W^{-1}R)^{\times} = \overline{W}$ by **(11.9)**. Also $S \subset \overline{S}$ by **(3.17)**(a). Thus (2) holds.

For (3), notice Λ is directed. Given $\lambda \le \mu$, set $\alpha_\mu^\lambda := \varphi_{S_\mu}^{S_\lambda}$. Then $\alpha_\nu^\mu\alpha_\mu^\lambda = \alpha_\nu^\lambda$ if $\lambda \le \mu \le \nu$. Thus $\varinjlim S_\lambda^{-1}R$ exists as a filtered direct limit of R-algebras by **(7.7)**.

Given λ, set $\beta_\lambda := \varphi_S^{S_\lambda}$. Then $\beta_\mu\alpha_\mu^\lambda = \beta_\lambda$. So the β_λ induce an R-algebra map $\beta\colon \varinjlim S_\lambda^{-1}R \to S^{-1}R$ with $\beta_\lambda = \beta\alpha_\lambda$ where α_λ is the insertion of $S_\lambda^{-1}R$.

Take $x \in \mathrm{Ker}(\beta)$. There are λ and $x_\lambda/s_\lambda \in S_\lambda^{-1}R$ such that $\alpha_\lambda(x_\lambda/s_\lambda) = x$ by **(7.8)**(1). Then $\beta_\lambda(x_\lambda/s_\lambda) = 0$. So there is $s \in S$ with $sx_\lambda = 0$. But $s \in S_\mu$ for some $\mu \ge \lambda$. Hence $\alpha_\mu^\lambda(x_\lambda/s_\lambda) = 0$. So $x = \alpha_\mu\alpha_\mu^\lambda(x_\lambda/s_\lambda) = 0$. Thus β is injective.

As to surjectivity, take $x/s \in S^{-1}R$. Then $s \in S_\lambda$ for some λ, so $x/s \in S_\lambda^{-1}R$. Hence $\beta_\lambda(x/s) = x/s$. Thus β is surjective, so an isomorphism. Thus (3) holds. □

Exercise **(11.11)**. — Let R be a ring, S_0 the set of nonzerodivisors.

(1) Show S_0 is the largest multiplicative subset S with $\varphi_S\colon R \to S^{-1}R$ injective.

(2) Show every element x/s of $S_0^{-1}R$ is either a zerodivisor or a unit.

(3) Suppose every element of R is either a zerodivisor or a unit. Show $R = S_0^{-1}R$.

Solution: For (1), let $s \in S$ and $x \in R$ with $sx = 0$. Then $\varphi_S(sx) = 0$. So $\varphi_S(s)\varphi_S(x) = 0$. But $\varphi_S(s)$ is a unit. So $\varphi_S(x) = 0$. But φ_S is injective. So $x = 0$. Thus $S \subset S_0$; that is, (1) holds.

For (2), take $x/s \in S_0^{-1}R$, and suppose it is a nonzerodivisor. Then $x/1$ is also a nonzerodivisor. Hence $x \in S_0$, for if $xy = 0$, then $x/1\cdot y/1 = 0$, so $\varphi_{S_0}(y) = y/1 = 0$, so $y = 0$ as φ_{S_0} is injective. Therefore, x/s is a unit. Thus (2) holds.

In (3), by hypothesis, $S_0 \subset R^{\times}$. So $R \xrightarrow{\sim} S_0^{-1}R$ by **(11.6)**; that is, (3) holds. □

Exercise **(11.17)**. — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Show (1) if $\mathfrak{a} \subset \mathfrak{b}$, then $\mathfrak{a}^S \subset \mathfrak{b}^S$; (2) $(\mathfrak{a}^S)^S = \mathfrak{a}^S$; and (3) $(\mathfrak{a}^S\mathfrak{b}^S)^S = (\mathfrak{a}\mathfrak{b})^S$.

Solution: For (1), take $x \in \mathfrak{a}^S$. Then there is $s \in S$ with $sx \in \mathfrak{a}$. If $\mathfrak{a} \subset \mathfrak{b}$, then $sx \in \mathfrak{b}$, and so $x \in \mathfrak{b}^S$. Thus (1) holds.

To show (2), proceed by double inclusion. First, note $\mathfrak{a}^S \supset \mathfrak{a}$ by **(11.16)**(2). So $(\mathfrak{a}^S)^S \supset \mathfrak{a}^S$ again by **(11.16)**(2). Conversely, given $x \in (\mathfrak{a}^S)^S$, there is $s \in S$ with $sx \in \mathfrak{a}^S$. So there is $t \in S$ with $tsx \in a$. But $ts \in S$. So $x \in \mathfrak{a}^S$. Thus (2) holds.

To show (3), proceed by double inclusion. First, note $\mathfrak{a} \subset \mathfrak{a}^S$ and $\mathfrak{b} \subset \mathfrak{b}^S$ by **(11.16)**(2). So $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}^S\mathfrak{b}^S$. Thus (1) yields $(\mathfrak{a}\mathfrak{b})^S \subset (\mathfrak{a}^S\mathfrak{b}^S)^S$.

Conversely, given $x \in \mathfrak{a}^S\mathfrak{b}^S$, say $x := \sum y_iz_i$ with $y_i \in \mathfrak{a}^S$ and $z_i \in \mathfrak{b}^S$. Then there are $s_i, t_i \in S$ such that $s_iy_i \in \mathfrak{a}$ and $t_iz_i \in \mathfrak{b}$. Set $u := \prod s_it_i$. Then $u \in S$ and $ux \in \mathfrak{a}\mathfrak{b}$. So $x \in (\mathfrak{a}\mathfrak{b})^S$. Thus $\mathfrak{a}^S\mathfrak{b}^S \subset (\mathfrak{a}\mathfrak{b})^S$. So $(\mathfrak{a}^S\mathfrak{b}^S)^S \subset ((\mathfrak{a}\mathfrak{b})^S)^S$ by (1). But $((\mathfrak{a}\mathfrak{b})^S)^S = (\mathfrak{a}\mathfrak{b})^S$ by (2). Thus (3) holds. □

Exercise **(11.18)**. — Let R be a ring, S a multiplicative subset. 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 **(11.14)**(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 **(11.16)**(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 **(11.14)**(1). Thus $\operatorname{nil}(R)(S^{-1}R) \supset \operatorname{nil}(S^{-1}R)$. □

Exercise **(11.24)**. — 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 **(11.25)**. — 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

$$x^n + y_1x^{n-1} + \cdots + y_n = 0$$

with $y_i \in K$. Write $y_i = a_i/a$ with $a_1, \ldots, a_n, a \in R$. Then

$$(ax)^n + a_1(ax)^{n-1} + \cdots + a^{n-1}a_0 = 0.$$

Set $b := ax$. Then $b \in \overline{R}$ and $x = b/a$. □

Exercise **(11.26)**. — 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 **(11.25)**, 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 module finite over R_f by **(10.28)**. □

Exercise **(11.29)**. — Let R be a ring, S and T multiplicative subsets.

(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

$$T^{-1}(S^{-1}R) = S^{-1}(T^{-1}R) = U^{-1}R.$$

Solution: A proof similar to that of **(11.27)** shows $T^{-1}R = T'^{-1}(S^{-1}R)$. By **(11.23)**, $T'^{-1}(S^{-1}R) = T^{-1}(S^{-1}R)$. 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, $U^{-1}RS^{-1}(T^{-1}R)$. Thus (2) holds. □

Exercise **(11.32)** (*Localization and normalization commute*). — Given a domain R and a multiplicative subset 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 **(11.24)**. Thus $S^{-1}\overline{R} \subset \overline{S^{-1}R}$.

Conversely, given $x \in \overline{S^{-1}R}$, consider an equation of integral dependence:

$$x^n + a_1x^{n-1} + \cdots + a_n = 0.$$

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

$$(sx)^n + sa_1(sx)^{n-1} + \cdots + s^na_n = 0.$$

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 subset, 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 M is an $S^{-1}R$-module since $S^{-1}M$ is by **(12.3)**. 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 subsets, 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 subset. Show that S becomes a filtered category when equipped as follows: given $s, t \in S$, set

$$\operatorname{Hom}(s,t) := \{x \in R \mid xs = t\}.$$

Given a module M, define a functor $S \to ((R\text{-mod}))$ as follows: for $s \in S$, set $M_s := M$; to each $x \in \operatorname{Hom}(s,t)$, associate $\mu_x : M_s \to M_t$. Define $\beta_s : M_s \to S^{-1}M$ 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 $t \in \operatorname{Hom}(s,u)$ and $s \in \operatorname{Hom}(t,u)$. Given $x, y \in \operatorname{Hom}(s,t)$, we have $xs = t$ and $ys = t$. So $s \in \operatorname{Hom}(t,u)$ and $xs = ys$ in $\operatorname{Hom}(s,u)$. Thus S is filtered.

Further, given $x \in \operatorname{Hom}(s,t)$, we have $\beta_t \mu_x = \beta_s$ since $m/s = xm/t$ as $xs = t$. So the β_s induce a homomorphism $\beta : \varinjlim M_s \to S^{-1}M$. 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 subset, M a module. Prove $S^{-1}M = 0$ if $\operatorname{Ann}(M) \cap S \neq \emptyset$. Prove the converse if M is finitely generated.

Solution: Say $f \in \operatorname{Ann}(M) \cap S$. 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 $\prod f_i \in \operatorname{Ann}(M) \cap S$, as desired. □

Exercise **(12.8)**. — Let R be a ring, M a finitely generated module, $\mathfrak{a}$ an ideal.

(1) Set $S := 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ lies in the radical of $S^{-1}R$.

(2) Use (1), Nakayama's Lemma **(10.11)**, and **(12.7)**, but not the determinant trick **(10.2)**, to prove this part of **(10.3)**: if $M = \mathfrak{a}M$, then $sM = 0$ for an $s \in S$.

Solution: For (1), use **(3.2)** as follows. Take $a/(1+b) \in S^{-1}\mathfrak{a}$ with $a, b \in \mathfrak{a}$. Then for $x \in R$ and $c \in \mathfrak{a}$, we have

$$1 + \big(a/(1+b)\big)\big(x/(1+c)\big) = \big(1 + (b + c + bc + ax)\big)/(1+b)(1+c).$$

The latter is a unit in $S^{-1}R$, as $b + c + bc + ax \in \mathfrak{a}$. So $a/(1+b) \in \operatorname{rad}(S^{-1}R)$ by **(3.2)**. Thus (1) holds.

For (2), assume $M = \mathfrak{a}M$. Then $S^{-1}M = S^{-1}\mathfrak{a}S^{-1}M$ by **(12.2)**. So $S^{-1}M = 0$ by (1) and **(10.11)**. So **(12.7)** yields an $s \in S$ with $sM = 0$. Thus (2) holds. □

Exercise **(12.12)**. — Let R be a ring, S a multiplicative subset, P a projective module. Then $S^{-1}P$ is a projective $S^{-1}R$-module.

Solution: By **(5.23)**, there is a module K such that $F := K \oplus P$ is free. So **(12.10)** yields that $S^{-1}F = S^{-1}P \oplus S^{-1}K$ and that $S^{-1}F$ is free over $S^{-1}R$. Hence $S^{-1}P$ is a projective $S^{-1}R$-module again by **(5.23)**. □

Exercise **(12.14)**. — Let R be a ring, S a multiplicative subset, 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 **(12.13)**, $S^{-1}(M \otimes_R N) = S^{-1}R \otimes_R (M \otimes_R N)$. The latter is equal to $(S^{-1}R \otimes_R M) \otimes_R N$ by associativity **(8.10)**. Again by **(12.13)**, the latter is equal to $S^{-1}M \otimes_R N$. Thus the first equality holds.

By cancellation **(8.11)**, $S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} (S^{-1}R \otimes_R N)$, and the latter is equal to $S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ by **(12.13)**. Thus the second equality holds.

Finally by **(8.9)**, 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 **(12.15)**. — Let R be a ring, R' an algebra, S a multiplicative subset, M a finitely presented module, and r an integer. Show

$$F_r(M \otimes_R R') = F_r(M)R' \quad \text{and} \quad F_r(S^{-1}M) = F_r(M)S^{-1}R = S^{-1}F_r(M).$$

Solution: Let $R^n \xrightarrow{\alpha} R^m \to M \to 0$ be a presentation. Then, by **(8.13)**,

$$(R')^n \xrightarrow{\alpha \otimes 1} (R')^m \to M \otimes_R R' \to 0$$

is a presentation. Further, the matrix $\mathbf{A}$ of α induces the matrix of $\alpha \otimes 1$. Thus

$$F_r(M \otimes_R R') = I_{m-r}(\mathbf{A})R' = F_r(M)R'.$$

For the last equalities, take $R' := S^{-1}R$. Then $F_r(S^{-1}M) = F_r(M)S^{-1}R$ by **(12.13)**. Finally, $F_r(M)S^{-1}R = S^{-1}F_r(M)$ by **(12.2)**. □

Exercise **(12.18)**. — Let R be a ring, S a multiplicative subset.

(1) Let $M_1 \xrightarrow{\alpha} M_2$ be a map of modules, which restricts to a map $N_1 \to N_2$ of submodules. Show $\alpha(N_1^S) \subset N_2^S$; that is, there is an induced map $N_1^S \to N_2^S$.

(2) Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$ be a left exact sequence, which restricts to a left exact sequence $0 \to N_1 \to N_2 \to N_3$ of submodules. Show there is an induced left exact sequence of saturations: $0 \to N_1^S \to N_2^S \to N_3^S$.

Solution: For (1), take $m \in N_1^S$. Then there is $s \in S$ with $sm \in N_1$. So $\alpha(sm) \in N_2$. But $\alpha(sm) = s\alpha(m)$. Thus (1) holds.

In (2), $\alpha(N_1^S) \subset N_2^S$ and $\beta(N_2^S) \subset N_3^S$ by (1). Trivially, $\alpha|N_1^S$ is injective, and $\beta\alpha|N_1^S = 0$. Finally, given $m_2 \in \operatorname{Ker}(\beta|N_2^S)$, there is $s \in S$ with $sm_2 \in N_2$, and exactness yields $m_1 \in M_1$ with $\alpha(m_1) = m_2$. Then $\beta(sm_2) = s\beta(m_2) = 0$. So exactness yields $n_1 \in N_1$ with $\alpha(n_1) = sm_2$. Also $\alpha(sm_1) = s\alpha(m_1) = sm_2$. But α is injective. Hence $sm_1 = n_1$. So $m_1 \in N_1^S$, and $\alpha(m_1) = m_2$. Thus (2) holds. □

Exercise **(12.19)**. — Let R be a ring, M a module, and S a multiplicative subset. Set $T^S M := \langle 0 \rangle^S$. We call it the **$S$-torsion submodule of M**. Prove the following:

(1) $T^S(M/T^S M) = 0$. (2) $T^S M = \operatorname{Ker}(\varphi_S)$.

(3) Let $\alpha : M \to N$ be a map. Then $\alpha(T^S M) \subset T^S N$.

(4) Let $0 \to M' \to M \to M''$ be exact. Then so is $0 \to T^S M' \to T^S M \to T^S M''$.

(5) Let $S_1 \subset S$ be a multiplicative subset. Then $T^S(S_1^{-1}M) = S_1^{-1}(T^S M)$.

Solution: For (1), given an element of $T^S(M/T^S(M))$, let $m \in M$ represent it. Then there is $s \in S$ with $sm \in T^S(M)$. So there is $t \in S$ with $tsm = 0$. So $m \in T^S(M)$. Thus (1) holds. Assertion (2) holds by **(12.17)**(3).

Assertions (3) and (4) follow from **(12.18)**(1) and (2).

For (5), given $m/s_1 \in S_1^{-1}T^S(M)$ with $s_1 \in S_1$ and $m \in T^S(M)$, take $s \in S$ with $sm = 0$. Then $sm/s_1 = 0$. So $m/s_1 \in T^S(S_1^{-1}M)$. Thus $S_1^{-1}T^S(M) \subset T^S(S_1^{-1}M)$.

For the opposite inclusion, given $m/s_1 \in T^S(S_1^{-1}M)$ with $m \in M$ and $s_1 \in S_1$, take t/t_1 with $t \in S$ and $t_1 \in S_1$ and $t/t_1 \cdot m/s_1 = 0$. Then $tm/1 = 0$. So there is $s' \in S_1$ with $s'tm = 0$ by **(12.17)**(3). But $s't \in S$ as $S_1 \subset S$. So $m \in T^S(M)$. Thus $m/s_1 \in S_1^{-1}T^S(M)$. Thus (5) holds. □

Exercise **(12.28)**. — Set $R := \mathbb{Z}$ and $S = \mathbb{Z} - \langle 0\rangle$. Set $M := \bigoplus_{n\ge 2} \mathbb{Z}/\langle n\rangle$ and $N := M$. Show that the map σ of **(12.25)** 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 **(13.3)**. — Let R be a ring, and set $X := \mathrm{Spec}(R)$. Let $X_1, X_2 \subset X$ be closed subsets. Show that the following four conditions are equivalent:

(1) $X_1 \cup X_2 = X$ and $X_1 \cap X_2 = \emptyset$.
(2) There are complementary idempotents $e_1, e_2 \in R$ with $\mathbf{V}(\langle e_i\rangle) = X_i$.
(3) There are comaximal ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1\mathfrak{a}_2 = 0$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.
(4) There are ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = R$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.

Finally, given any e_i and $\mathfrak{a}_i$ satisfying (2) and either (3) or (4), necessarily $e_i \in \mathfrak{a}_i$.

Solution: Assume (1). Take ideals $\mathfrak{a}_1, \mathfrak{a}_2$ with $\mathbf{V}(\mathfrak{a}_i) = X_i$. Then **(13.1)** yields

$$\mathbf{V}(\mathfrak{a}_1\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1) \cup \mathbf{V}(\mathfrak{a}_2) = X = \mathbf{V}(0) \quad \text{and}$$
$$\mathbf{V}(\mathfrak{a}_1 + \mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1) \cap \mathbf{V}(\mathfrak{a}_2) = \emptyset = \mathbf{V}(R).$$

So $\sqrt{\mathfrak{a}_1\mathfrak{a}_2} = \sqrt{\langle 0\rangle}$ and $\sqrt{\mathfrak{a}_1 + \mathfrak{a}_2} = \sqrt{R}$ again by **(13.1)**. Hence **(3.27)** yields (2).

Assume (2). Set $\mathfrak{a}_i := \langle e_i\rangle$. As $e_1 + e_2 = 1$ and $e_1e_2 = 0$, plainly (3) holds.

Assume (3). As the $\mathfrak{a}_i$ are comaximal, the Chinese Remainder Theorem **(1.14)** yields $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$. But $\mathfrak{a}_1\mathfrak{a}_2 = 0$. So $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = R$ by **(4.17)**. Thus (4) holds.

Assume (4). Then **(13.1)** yields (1) as follows:

$$X_1 \cup X_2 = \mathbf{V}(\mathfrak{a}_1) \cup \mathbf{V}(\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1\mathfrak{a}_2) = \mathbf{V}(0) = X \quad \text{and}$$
$$X_1 \cap X_2 = \mathbf{V}(\mathfrak{a}_1) \cap \mathbf{V}(\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1 + \mathfrak{a}_2) = \mathbf{V}(R) = \emptyset.$$

Finally, say e_i and $\mathfrak{a}_i$ satisfy (2) and either (3) or (4). Then $\sqrt{\langle e_i\rangle} = \sqrt{\mathfrak{a}_i}$ by **(13.1)**. So $e_i^n \in \mathfrak{a}_i$ for some $n \ge 1$. But $e_i^2 = e_i$, so $e_i^n = e_1$. Thus $e_i \in \mathfrak{a}_i$. □

Exercise **(13.4)**. — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Prove these two statements:

(1) Every prime of R is a contraction of a prime if and only if φ^* is surjective.
(2) If every prime of R' is an extension of a prime, then φ^* is injective.

Is the converse of (2) true?

Solution: Note $\varphi^*(\mathfrak{q}) := \varphi^{-1}(\mathfrak{q})$ by **(13.1.2)**. Hence (1) holds.

Given two primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ that are extensions, if $\mathfrak{q}_1^c = \mathfrak{q}_2^c$, then $\mathfrak{q}_1 = \mathfrak{q}_2$ by **(1.5)**. Thus (2) holds.

The converse of (2) is false. Take R to be a domain. Set $R' := R[X]/\langle X^2\rangle$. Then $R'/\langle X\rangle = R$ by **(1.8)**. So $\langle X\rangle$ is prime by **(2.9)**. But $\langle X\rangle$ is not an extension, as $X \notin \mathfrak{a}R'$ for any proper ideal $\mathfrak{a}$ of R. Finally, every prime $\mathfrak{q}$ of R' contains the residue x of X, as $x^2 = 0$. Hence $\mathfrak{q}$ is generated by $\mathfrak{q} \cap R$ and x. But $\mathfrak{q} \cap R = \varphi^*(\mathfrak{q})$. Thus φ^* is injective. □

Exercise **(13.5)**. — Let R be a ring, S a multiplicative subset. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(S^{-1}R)$. Set $\varphi_S^* := \mathrm{Spec}(\varphi_S)$ and $S^{-1}X := \mathrm{Im}\,\varphi_S^* \subset X$. Show (1) that $S^{-1}X$ consists of the primes $\mathfrak{p}$ of R with $\mathfrak{p} \cap S = \emptyset$ and (2) that φ_S^* is a homeomorphism of Y onto $S^{-1}X$.

Solution: Note $\varphi_S^*(\mathfrak{q}) := \varphi_S^{-1}(\mathfrak{q})$ by **(13.1.2)**. Hence **(11.20)**(2) yields (1) and also the bijectivity of φ_S^*. But φ_S^* is continuous by **(13.1)**. So it remains to show that φ_S^* is closed. Given an ideal $\mathfrak{b} \subset S^{-1}R$, set $\mathfrak{a} := \varphi_S^{-1}(\mathfrak{b})$. It suffices to show

$$\varphi_S^*(\mathbf{V}(\mathfrak{b})) = S^{-1}X \bigcap \mathbf{V}(\mathfrak{a}). \qquad \textbf{(13.5.1)}$$

Given $\mathfrak{p} \in \varphi_S^*(\mathbf{V}(\mathfrak{b}))$, say $\mathfrak{p} = \varphi_S^*(\mathfrak{q})$ and $\mathfrak{q} \in \mathbf{V}(\mathfrak{b})$. Then $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{q})$ and $\mathfrak{q} \supset \mathfrak{b}$ by **(13.1)**. So $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{q}) \supset \varphi_S^{-1}(\mathfrak{b}) =: \mathfrak{a}$. So $\mathfrak{p} \in \mathbf{V}(\mathfrak{a})$. But $\mathfrak{p} \in \varphi_S^*(\mathbf{V}(\mathfrak{b})) \subset S^{-1}X$. Thus $\varphi_S^*(\mathbf{V}(\mathfrak{b})) \subset S^{-1}X \bigcap \mathbf{V}(\mathfrak{a})$.

Conversely, given $\mathfrak{p} \in S^{-1}X \bigcap \mathbf{V}(\mathfrak{a})$, say $\mathfrak{p} = \varphi_S^*(\mathfrak{q})$. Then $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{q})$ and $\mathfrak{p} \supset \mathfrak{a} := \varphi_S^{-1}(\mathfrak{b})$. So $\varphi_S^{-1}(\mathfrak{q}) \supset \varphi_S^{-1}(\mathfrak{b})$. So $\varphi_S^{-1}(\mathfrak{q})R \supset \varphi_S^{-1}(\mathfrak{b})R$. So $\mathfrak{q} \supset \mathfrak{b}$ by **(11.19)**(1)(b). So $\mathfrak{q} \in \mathbf{V}(\mathfrak{b})$. So $\mathfrak{p} = \varphi_S^*(\mathfrak{q}) \in \varphi_S^*(\mathbf{V}(\mathfrak{b}))$. Thus **(13.5.1)** holds, as desired. Thus (2) holds. □

Exercise **(13.6)**. — Let $\theta\colon R \to R'$ be a ring map, $S \subset R$ a multiplicative subset. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$ and $\theta^* := \mathrm{Spec}(\theta)$. Via **(13.5)**(2) and **(11.23)**, identify $\mathrm{Spec}(S^{-1}R)$ and $\mathrm{Spec}(S^{-1}R')$ with their images $S^{-1}X \subset X$ and $S^{-1}Y \subset Y$. Show (1) $S^{-1}Y = \theta^{*-1}(S^{-1}X)$ and (2) $\mathrm{Spec}(S^{-1}\theta) = \theta^*|S^{-1}Y$.

Solution: Given $\mathfrak{q} \in Y$, elementary set-theory shows that $\mathfrak{q} \cap \theta(S) = \emptyset$ if and only if $\theta^{-1}(\mathfrak{q}) \cap S = \emptyset$. So $\mathfrak{q} \in S^{-1}Y$ if and only if $\theta^{-1}(\mathfrak{q}) \in S^{-1}X$ by **(13.5)**(1) and **(11.23)**. But $\varphi_S^{-1}(\mathfrak{q}) =: \varphi_S^*(\mathfrak{q})$ by **(13.1.2)**. Thus (1) holds.

Finally, $(S^{-1}\theta)\varphi_S = \varphi_S\theta$ by **(12.9)**. So $\varphi_S^{-1}(S^{-1}\theta)^{-1}(\mathfrak{q}) = (S^{-1}\theta)^{-1}\varphi_S^{-1}(\mathfrak{q})$. Thus **(13.1.2)** yields (2). □

Exercise **(13.7)**. — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{a} \subset R$ an ideal. Set $\mathfrak{b} := \mathfrak{a}R'$. Let $\overline{\theta}\colon R/\mathfrak{a} \to R'/\mathfrak{b}$ be the induced map. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$. Set $\theta^* := \mathrm{Spec}(\theta)$ and $\overline{\theta}^* := \mathrm{Spec}(\overline{\theta})$. Via **(13.1)**, identify $\mathrm{Spec}(R/\mathfrak{a})$ and $\mathrm{Spec}(R'/\mathfrak{b})$ with $\mathbf{V}(\mathfrak{a}) \subset X$ and $\mathbf{V}(\mathfrak{b}) \subset Y$. Show (1) $\mathbf{V}(\mathfrak{b}) = \theta^{*-1}(\mathbf{V}(\mathfrak{a}))$ and (2) $\overline{\theta}^* = \theta^*|\,\mathbf{V}(\mathfrak{b})$.

Solution: Given $\mathfrak{q} \in Y$, observe that $\mathfrak{q} \supset \mathfrak{b}$ if and only if $\theta^{-1}(\mathfrak{q}) \supset \mathfrak{a}$, as follows. By **(1.5)**(1) in its notation, $\mathfrak{q} \supset \mathfrak{b} := \mathfrak{a}^e$ yields $\mathfrak{q}^c \supset \mathfrak{a}^{ec} \supset \mathfrak{a}$, and $\mathfrak{q}^c \supset \mathfrak{a}$ yields $\mathfrak{q} \supset \mathfrak{q}^{ce} \supset \mathfrak{a}^e$. Thus (1) holds.

Plainly, $\overline{\theta}(\mathfrak{q}/b) = (\theta^{-1}\mathfrak{q})/\mathfrak{a}$. Thus **(13.1.2)** yields (2). □

Exercise **(13.8)**. — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{p} \subset R$ a prime, k the residue field of $R_\mathfrak{p}$. Set $\theta^* := \mathrm{Spec}(\theta)$. Show (1) that $\theta^{*-1}(\mathfrak{p})$ is canonically homeomorphic to $\mathrm{Spec}(R' \otimes_R k)$ and (2) that $\mathfrak{p} \in \mathrm{Im}\,\theta^*$ if and only if $R' \otimes_R k \neq 0$.

Solution: First, take $S := R - \mathfrak{p}$ and apply **(13.6)** to obtain

$$\operatorname{Spec}(R'_{\mathfrak{p}}) = \theta^{*-1}(\operatorname{Spec}(R_{\mathfrak{p}})) \quad\text{and}\quad \operatorname{Spec}(\theta_{\mathfrak{p}}) = \theta^*\big|\operatorname{Spec}(R'_{\mathfrak{p}}).$$

Next, take $\mathfrak{a} := \mathfrak{p}R_{\mathfrak{p}}$ and apply **(13.7)** to $\theta_{\mathfrak{p}}\colon R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$ to obtain

$$\operatorname{Spec}(R'/\mathfrak{p}R') = \operatorname{Spec}(\theta_{\mathfrak{p}})^{-1}\,\mathbf{V}(\mathfrak{p}R_{\mathfrak{p}}).$$

But $\theta^{-1}(\mathfrak{p}R_{\mathfrak{p}}) = \mathfrak{p}$ by **(11.20)**(2); so $\mathbf{V}(\mathfrak{p}R_{\mathfrak{p}}) = \mathfrak{p}$. Therefore,

$$\operatorname{Spec}(R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}}) = \big(\theta^*\big|\operatorname{Spec}(R'_{\mathfrak{p}})\big)^{-1}(\mathfrak{p}) = \theta^{*-1}(\mathfrak{p}).$$

But $k := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. So $R'/\mathfrak{p}R' = k \otimes_R R'$. Thus (1) holds.

Finally, (1) implies $\mathfrak{p} \in \operatorname{Im}\theta^*$ if and only if $\operatorname{Spec}(R' \otimes_R k) \neq \emptyset$. Thus (2) holds. □

Exercise **(13.9)**. — Let R be a ring, $\mathfrak{p}$ a prime ideal. Show that the image of $\operatorname{Spec}(R_{\mathfrak{p}})$ in $\operatorname{Spec}(R)$ is the intersection of all open neighborhoods of $\mathfrak{p}$ in $\operatorname{Spec}(R)$.

Solution: By **(13.5)**, the image $X_{\mathfrak{p}}$ consists of the primes contained in $\mathfrak{p}$. Given $f \in R - \mathfrak{p}$, note that $\mathbf{D}(f)$ contains every prime contained in $\mathfrak{p}$, or $X_{\mathfrak{p}} \subset \mathbf{D}(f)$. But the principal open sets form a basis of the topology of X by **(13.1)**. Hence $X_{\mathfrak{p}}$ is contained in the intersection, Z say, of all open neighborhoods of $\mathfrak{p}$. Conversely, given a prime $\mathfrak{q} \not\subset \mathfrak{p}$, there is $g \in \mathfrak{q} - \mathfrak{p}$. So $\mathbf{D}(g)$ is an open neighborhood of $\mathfrak{p}$, and $\mathfrak{q} \notin \mathbf{D}(g)$. Thus $X_{\mathfrak{p}} = Z$, as desired. □

Exercise **(13.10)**. — Let $\varphi\colon R \to R'$ and $\psi\colon R \to R''$ be ring maps, and define $\theta\colon R \to R' \otimes_R R''$ by $\theta(x) := \varphi(x) \otimes \psi(x)$. Show

$$\operatorname{Im}\operatorname{Spec}(\theta) = \operatorname{Im}\operatorname{Spec}(\varphi) \bigcap \operatorname{Im}\operatorname{Spec}(\psi).$$

Solution: Given $\mathfrak{p} \in X$, set $k := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Then **(8.10)** and **(8.11)** yield

$$(R' \otimes_R R'') \otimes_R k = R' \otimes_R (R'' \otimes_R k) = (R' \otimes_R k) \otimes_k (R'' \otimes_R k).$$

So $(R' \otimes_R R'') \otimes_R k \neq 0$ if and only if $R' \otimes_R k \neq 0$ and $R'' \otimes_R k \neq 0$ by **(8.15)**. Hence **(13.8)**(2) implies that $\mathfrak{p} \in \operatorname{Im}\operatorname{Spec}(\theta)$ if and only if $\mathfrak{p} \in \operatorname{Im}\operatorname{Spec}(\varphi)$ and $\mathfrak{p} \in \operatorname{Im}\operatorname{Spec}(\psi)$, as desired. □

Exercise **(13.11)**. — Let R be a filtered direct limit of rings R_λ with transition maps α^λ_μ and insertions α_λ. For each λ, let $\varphi_\lambda\colon R' \to R_\lambda$ be a ring map with $\varphi_\mu = \alpha^\lambda_\mu \varphi_\lambda$ for all α^λ_μ, so that $\varphi := \alpha_\lambda\varphi_\lambda$ is independent of λ. Show

$$\operatorname{Im}\operatorname{Spec}(\varphi) = \textstyle\bigcap_\lambda \operatorname{Im}\operatorname{Spec}(\varphi_\lambda).$$

Solution: Given $\mathfrak{q} \in \operatorname{Spec}(R')$, set $k := R'_{\mathfrak{p}}/\mathfrak{q}R'_{\mathfrak{q}}$. Then **(8.13)** yields

$$R \otimes_{R'} k = \varinjlim (R_\lambda \otimes_{R'} k).$$

So $R \otimes_{R'} k \neq 0$ if and only if $R_\lambda \otimes_{R'} k \neq 0$ for all λ by **(7.9)**(1). Hence **(13.8)**(2) implies that $\mathfrak{p} \in \operatorname{Im}\operatorname{Spec}(\varphi)$ if and only if $\mathfrak{p} \in \operatorname{Im}\operatorname{Spec}(\varphi_\lambda)$ for all λ, as desired. □

Exercise **(13.12)**. — Let A be a domain with just one nonzero prime $\mathfrak{p}$. Set $K := \operatorname{Frac}(A)$ and $R := (A/\mathfrak{p}) \times K$. Define $\varphi\colon A \to R$ by $\varphi(x) := (x', x)$ with x' the residue of x. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Show φ^* is bijective, but not a homeomorphism.

Solution: Note $\mathfrak{p}$ is maximal; so $A/\mathfrak{p}$ is a field. The primes of R are $(0, K)$ and $(A/\mathfrak{p}, 0)$ by **(1.16)**. Plainly, $\varphi^{-1}(0, K) = \mathfrak{p}$ and $\varphi^{-1}(A/\mathfrak{p}, 0) = 0$. So φ^* is bijective. Finally, $\operatorname{Spec}(R)$ is discrete, but $\operatorname{Spec}(A)$ has $\mathfrak{p} \in \mathbf{V}(0)$; so φ^* is not a homeomorphism. □

Exercise **(13.13)**. — Let $\varphi\colon R \to R'$ be a ring map, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Show (1) that the closure $\overline{\varphi^*(\mathbf{V}(\mathfrak{b}))}$ in $\operatorname{Spec}(R)$ is equal to $\mathbf{V}(\varphi^{-1}\mathfrak{b})$ and (2) that $\varphi^*(\operatorname{Spec}(R'))$ is dense in $\operatorname{Spec}(R)$ if and only if $\operatorname{Ker}(\varphi) \subset \operatorname{nil}(R)$.

Solution: For (1), given $\mathfrak{p} \in \varphi^*(\mathbf{V}(\mathfrak{b}))$, say $\mathfrak{p} = \varphi^{-1}(\mathfrak{P})$ where $\mathfrak{P}$ is a prime of R' with $\mathfrak{P} \supset \mathfrak{b}$. Then $\varphi^{-1}\mathfrak{P} \supset \varphi^{-1}\mathfrak{b}$. So $\mathfrak{p} \supset \varphi^{-1}\mathfrak{b}$, or $\mathfrak{p} \in \mathbf{V}(\varphi^{-1}\mathfrak{b})$. Thus $\varphi^*(\mathbf{V}(\mathfrak{b})) \subset \mathbf{V}(\varphi^{-1}\mathfrak{b})$. But $\mathbf{V}(\varphi^{-1}\mathfrak{b})$ is closed. So $\overline{\varphi^*(\mathbf{V}(\mathfrak{b})} \subset \mathbf{V}(\varphi^{-1}\mathfrak{b})$.

Conversely, given $\mathfrak{p} \in \mathbf{V}(\varphi^{-1}\mathfrak{b})$, note $\mathfrak{p} \supset \sqrt{\varphi^{-1}\mathfrak{b}}$. Take a neighborhood $\mathbf{D}(f)$ of $\mathfrak{p}$; then $f \notin \mathfrak{p}$. Hence $f \notin \sqrt{\varphi^{-1}\mathfrak{b}}$. But $\sqrt{\varphi^{-1}\mathfrak{b}} = \varphi^{-1}(\sqrt{\mathfrak{b}})$ by **(3.25)**. Hence $\varphi(f) \notin \sqrt{\mathfrak{b}}$. So there's a prime $\mathfrak{P} \supset \mathfrak{b}$ with $\varphi(f) \notin \mathfrak{P}$ by the Scheinnullstellensatz **(3.29)**. So $\varphi^{-1}\mathfrak{P} \in \varphi^*(\mathbf{V}(\mathfrak{b}))$. Further, $f \notin \varphi^{-1}\mathfrak{P}$, or $\varphi^{-1}\mathfrak{P} \in \mathbf{D}(f)$. Therefore, $\varphi^{-1}\mathfrak{P} \in \varphi^*(\mathbf{V}(\mathfrak{b})) \cap \mathbf{D}(f)$. So $\varphi^*(\mathbf{V}(\mathfrak{b})) \cap \mathbf{D}(f) \neq \emptyset$. So $\mathfrak{p} \in \overline{\varphi^*(\mathbf{V}(\mathfrak{b}))}$. Thus (1) holds.

For (2), take $\mathfrak{b} := \langle 0 \rangle$. Then (1) yields $\overline{\varphi^*(\mathbf{V}(\mathfrak{b}))} = \mathbf{V}(\operatorname{Ker}(\varphi))$. But by **(13.1)**, $\mathbf{V}(\mathfrak{b}) = \operatorname{Spec}(R')$ and $\operatorname{Spec}(R) = \mathbf{V}(\langle 0 \rangle)$. So $\overline{\varphi^*(\operatorname{Spec}(R'))} = \operatorname{Spec}(R)$ if and only if $\mathbf{V}(\langle 0 \rangle) = \mathbf{V}(\operatorname{Ker}(\varphi))$. The latter holds if and only if $\operatorname{nil}(R) = \sqrt{\operatorname{Ker}(\varphi)}$ by **(13.1)**, so plainly if and only if $\operatorname{nil}(R) \supset \operatorname{Ker}(\varphi)$. Thus (2) holds. □

Exercise **(13.14)**. — Let R be a ring, R' a flat algebra with structure map φ. Show that R' is faithfully flat if and only if $\operatorname{Spec}(\varphi)$ is surjective.

Solution: Owing to the definition of $\operatorname{Spec}(\varphi)$ in **(13.1)**, the assertion amounts to the equivalence of (1) and (3) of **(9.15)**. □

Exercise **(13.15)**. — Let $\varphi\colon R \to R'$ be a flat map of rings, $\mathfrak{q}$ a prime of R', and $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Show that the induced map $\operatorname{Spec}(R'_{\mathfrak{q}}) \to \operatorname{Spec}(R_{\mathfrak{p}})$ is surjective.

Solution: Since $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$, clearly $\varphi(R - \mathfrak{p}) \subset (R' - \mathfrak{q})$. Thus φ induces a local homomorphism $R_{\mathfrak{p}} \to R'_{\mathfrak{q}}$. Moreover, $R'_{\mathfrak{p}}$ is flat over $R_{\mathfrak{p}}$ as $R'_{\mathfrak{p}} = R_{\mathfrak{p}} \otimes_R R'$ by **(12.13)**, and $R_{\mathfrak{p}} \otimes_R R'$ is flat over $R_{\mathfrak{p}}$ by **(9.11)**. Also $R'_{\mathfrak{q}}$ is flat over $R'_{\mathfrak{p}}$ by **(12.21)**. Hence $R'_{\mathfrak{q}}$ is flat over $R_{\mathfrak{p}}$ by **(9.12)**. So $R'_{\mathfrak{q}}$ is faithfully flat over $R_{\mathfrak{p}}$ by **(10.19)**. Hence $\operatorname{Spec}(R'_{\mathfrak{q}}) \to \operatorname{Spec}(R_{\mathfrak{p}})$ is surjective by **(9.15)**. □

Exercise **(13.16)**. — Let R be a ring. Given $f \in R$, set $S_f := \{f^n \mid n \geq 0\}$, and let $\overline{S}_f$ denote its saturation; see **(3.17)**. Given $f, g \in R$, show that the following conditions are equivalent:

(1) $\mathbf{D}(g) \subset \mathbf{D}(f)$. (2) $\mathbf{V}(\langle g \rangle) \supset \mathbf{V}(\langle f \rangle)$. (3) $\sqrt{\langle g \rangle} \subset \sqrt{\langle f \rangle}$.
(4) $\overline{S}_f \subset \overline{S}_g$. (5) $g \in \sqrt{\langle f \rangle}$. (6) $f \in \overline{S}_g$.
(7) there is a unique R-algebra map $\varphi^f_g\colon \overline{S}_f^{-1}R \to \overline{S}_g^{-1}R$.
(8) there is an R-algebra map $R_f \to R_g$.

Show that, if these conditions hold, then the map in (8) is equal to φ^f_g.

Solution: First, (1) and (2) are equivalent by **(13.1)**, and (2) and (3) are too. Plainly, (3) and (5) are equivalent. Further, (3) and (4) are equivalent by **(3.17)**(4). Always $f \in \overline{S}_f$; so (4) implies (6). Conversely, (6) implies $S_f \subset \overline{S}_g$; whence, **(3.17)**(1)(c) yields (4). Finally, (8) implies (4) by **(11.10)**(2). And (4) implies (7) by **(11.10)**(1). But $\overline{S}_f^{-1}R = S_f^{-1}R$ and $\overline{S}_g^{-1}R = S_g^{-1}R$ by **(11.9)**; whence, (7) implies both (8) and the last statement. □

Exercise **(13.17)**. — Let R be a ring. (1) Show that $\mathbf{D}(f) \mapsto R_f$ is a well-defined contravariant functor from the category of principal open sets and inclusions to ((R-alg)). (2) Given $\mathfrak{p} \in \operatorname{Spec}(R)$, show $\varinjlim_{\mathbf{D}(f)\ni\mathfrak{p}} R_f = R_{\mathfrak{p}}$.

Solution: Consider (1). By **(13.16)**, if $\mathbf{D}(g) \subset \mathbf{D}(f)$, then there is a unique R-algebra map $\varphi_g^f : \overline{S}_f^{-1}R \to \overline{S}_g^{-1}R$. By uniqueness, if $\mathbf{D}(h) \subset \mathbf{D}(g) \subset \mathbf{D}(f)$, then $\varphi_h^g\varphi_g^f\varphi_h^f$; also $\varphi_f^f = 1$. Further, if $\mathbf{D}(g) = \mathbf{D}(f)$, then $\overline{S}_f \subset \overline{S}_g$ and $\overline{S}_g \subset \overline{S}_f$, so $\overline{S}_f = \overline{S}_g$ and $\varphi_g^f = 1$. Finally, $R_f = \overline{S}_f^{-1}R$ by **(11.9)**. Thus (1) holds.

For (2), notice **(13.16)** yields an inclusion-reversing bijective correspondence between the principal open sets $D(f)$ and the saturated multiplicative subsets $\overline{S}_f$. Further, $\mathbf{D}(f) \ni \mathfrak{p}$ if and only if $f \notin \mathfrak{p}$ by **(13.1)**.

Set $S := R - \mathfrak{p}$. By **(3.16)**, S is saturated multiplicative. So $S \supset \overline{S}_f$ if and only if $f \notin \mathfrak{p}$ by **(3.17)**(1)(c). Also, $S = \bigcup_{f\notin\mathfrak{p}} \overline{S}_f$. But $R_f = \overline{S}_f^{-1}R_f$ by **(11.9)**. Thus

$$\varinjlim_{\mathbf{D}(f)\ni\mathfrak{p}} R_f = \varinjlim_{\overline{S}_f\subset S} \overline{S}_f^{-1}R.$$

By the definition of saturation in **(3.17)**, $\overline{S}_{fg} \ni f,\, g$. By **(3.17)**(1)(b), $\overline{S}_{fg}$ is saturated multiplicative. So $\overline{S}_{fg} \supset \overline{S}_f,\, \overline{S}_g$ by **(3.17)**(1)(c). So $\varinjlim \overline{S}_f^{-1}R = S^{-1}R$ by **(11.10)**(2). But $S^{-1}R = R_{\mathfrak{p}}$ by definition. Thus (2) holds. □

Exercise **(13.18)**. — A topological space is called **irreducible** if it's nonempty and if every pair of nonempty open subsets meet. Let R be a ring. Set $X := \operatorname{Spec}(R)$ and $\mathfrak{n} := \operatorname{nil}(R)$. Show that X is irreducible if and only if $\mathfrak{n}$ is prime.

Solution: Given $g \in R$, take $f := 0$. Plainly, $D(f) = \emptyset$; see **(13.1)**. So in **(13.17)** the equivalence of (1) and (5) means $\mathbf{D}(g) = \emptyset$ if and only if $g \in \mathfrak{n}$.

Suppose $\mathfrak{n}$ is not prime. Then there are $f,\, g \in R$ with $f,\, g \notin \mathfrak{n}$ but $fg \in \mathfrak{n}$. The above yields $\mathbf{D}(f) \neq \emptyset$ and $\mathbf{D}(g) \neq \emptyset$ but $\mathbf{D}(fg) = \emptyset$. Further, $\mathbf{D}(f)\cap\mathbf{D}(g) = \mathbf{D}(fg)$ by **(13.1.1)**. Thus X is not irreducible.

Suppose X is not irreducible, say U and V are nonempty open sets with $U\cap V = \emptyset$. By **(13.1)**, the $D(f)$ form a basis of the topology: fix $f,\, g \in R$ with $\emptyset \neq \mathbf{D}(f) \subset U$ and $\emptyset \neq \mathbf{D}(g) \subset V$. Then $\mathbf{D}(f)\cap\mathbf{D}(g) = \emptyset$. But $\mathbf{D}(f)\cap\mathbf{D}(g) = \mathbf{D}(fg)$ by **(13.1.1)**. Hence, the first paragraph implies $f,\, g \notin \mathfrak{n}$ but $fg \in \mathfrak{n}$. Thus $\mathfrak{n}$ is not prime. □

Exercise **(13.19)**. — Let X be a topological space, Y an irreducible subspace.

(1) Show that the closure $\overline{Y}$ of Y is also irreducible.

(2) Show that Y is contained in a maximal irreducible subspace.

(3) Show that the maximal irreducible subspaces of X are closed, and cover X. They are called its **irreducible components**. What are they if X is Hausdorff?

(4) Let R be a ring, and take $X := \operatorname{Spec}(R)$. Show that its irreducible components are the closed sets $\mathbf{V}(\mathfrak{p})$ where $\mathfrak{p}$ is a minimal prime.

Solution: For (1), let $U,\, V$ be nonempty open sets of $\overline{Y}$. Then $U\cap Y$ and $V\cap Y$ are open in Y, and nonempty. But Y is irreducible. So $(U\cap Y)\cap(V\cap Y) \neq \emptyset$. So $U\cap V \neq \emptyset$. Thus (1) holds.

For (2), let $\mathcal{S}$ be the set of irreducible subspaces containing Y. Then $Y \in \mathcal{S}$, and $\mathcal{S}$ is partially ordered by inclusion. Given a totally ordered subset $\{Y_\lambda\}$ of $\mathcal{S}$, set $Y' := \bigcup_\lambda Y_\lambda$. Then Y' is irreducible: given nonempty open sets $U,\, V$ of Y', there is Y_λ with $U\cap Y_\lambda \neq \emptyset$ and $V\cap Y_\lambda \neq \emptyset$; so $(U\cap Y_\lambda)\cap(V\cap Y_\lambda) \neq \emptyset$ as Y_λ is irreducible. Thus Zorn's Lemma yields (2).

For (3), note that (1) implies the maximal irreducible subspaces are closed, and that (2) implies they cover, as every point is irreducible. Finally, if X is Hausdorff, then any two points have disjoint open neighborhoods; hence, every irreducible subspace consists of a single point.

For (4), take Y to be an irreducible component. Then Y is closed by (1); so $Y = \operatorname{Spec}(R/\mathfrak{a})$ for some ideal $\mathfrak{a}$ by **(13.1.3)**. But Y is irreducible. So $\operatorname{nil}(R/\mathfrak{a})$ is prime by **(13.18)**. Hence $\sqrt{\mathfrak{a}}$ is prime. So $\sqrt{\mathfrak{a}}$ contains a minimal prime $\mathfrak{p}$ of R by **(3.14)**. Set $Z := \operatorname{Spec}(R/\mathfrak{p})$. Then $Z = \mathbf{V}(\mathfrak{p}) \supset \mathbf{V}(\sqrt{\mathfrak{a}}) = \mathbf{V}(\mathfrak{a}) = Y$ by **(13.1)**. Further, Z is irreducible by **(13.18)**. So $Z = Y$ by maximality. Thus $Y = \mathbf{V}(\mathfrak{p})$.

Conversely, given a minimal prime $\mathfrak{q}$, set $Z := \operatorname{Spec}(R/\mathfrak{q})$. Then Z is irreducible by **(13.18)**. So Z is contained, by (2), in a maximal irreducible subset, say Y. By the above, $Y = \mathbf{V}(\mathfrak{p})$ for some prime $\mathfrak{p}$. Then $\mathfrak{p} \subset \mathfrak{q}$ by **(13.1)**. Hence $\mathfrak{p} = \mathfrak{q}$ by minimality. Thus (4) holds. □

Exercise **(13.21)**. — Let R be a ring, $X := \operatorname{Spec}(R)$, and U an open subset. Show U is quasi-compact if and only if $X - U = \mathbf{V}(\mathfrak{a})$ 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. So $U = \bigcup_1^n \mathbf{D}(f_{\lambda_i})$ for some f_{λ_i}. Thus $X - U = \bigcap \mathbf{V}(f_{\lambda_i}) = \mathbf{V}(\langle f_{\lambda_1}, \dots, f_{\lambda_n}\rangle)$.

Conversely, assume $X - U = \mathbf{V}(\langle f_1, \dots, f_n\rangle)$. Then $U = \bigcup_{i=1}^n \mathbf{D}(f_i)$. But $\mathbf{D}(f_i) = \operatorname{Spec}(R_{f_i})$ by **(13.1)**. So by **(13.20)** with R_{f_i} for R, each $\mathbf{D}(f_i)$ is quasi-compact. Thus U is quasi-compact. □

Exercise **(13.22)**. — Let R be a ring, M a module, $m \in M$. Set $X := \operatorname{Spec}(R)$. Assume $X = \bigcup \mathbf{D}(f_\lambda)$ for some f_λ, and $m/1 = 0$ in M_{f_λ} for all λ. Show $m = 0$.

Solution: Since $m/1 = 0$ in R_{f_λ}, there is $n_\lambda > 0$ such that $f_\lambda^{n_\lambda}m = 0$. But $X = \bigcup \mathbf{D}(f_\lambda)$. Hence every prime excludes some f_λ, so also $f_\lambda^{n_\lambda}$. So there are $\lambda_1, \dots, \lambda_n$ and $x_1, \dots, x_n$ with $1 = \sum x_i f_{\lambda_i}^{n_{\lambda_i}}$. Thus $m = \sum x_i f_{\lambda_i}^{n_{\lambda_i}} m = 0$. □

Exercise **(13.23)**. — Let R be a ring; set $X := \operatorname{Spec}(R)$. Prove that the four following conditions are equivalent:

(1) $R/\operatorname{nil}(R)$ is absolutely flat.

(2) X is Hausdorff.

(3) X is T_1; that is, every point is closed.

(4) Every prime $\mathfrak{p}$ of R is maximal.

Assume (1) holds. Prove that X is **totally disconnected**; namely, no two distinct points lie in the same connected component.

Solution: Note $X = \operatorname{Spec}(R/\operatorname{nil}(R))$ as $X = \mathbf{V}(0) = \mathbf{V}(\sqrt{0}) = \operatorname{Spec}(R/\sqrt{0})$ by **(13.1)**. Hence we may replace R by $R/\operatorname{nil}(R)$, and thus assume $\operatorname{nil}(R) = 0$.

Assume (1). Given distinct primes $\mathfrak{p},\, \mathfrak{q} \in X$, take $x \in \mathfrak{p} - \mathfrak{q}$. Then $x \in \langle x^2\rangle$ by **(10.9)**(4). So there is $y \in R$ with $x = x^2y$. Set $\mathfrak{a}_1 := \langle x\rangle$ and $\mathfrak{a}_2 := \langle 1 - xy\rangle$. Set $X_i := \mathbf{V}(\mathfrak{a}_i)$. Then $\mathfrak{p} \in X_1$ as $x \in \mathfrak{p}$. Further, $\mathfrak{q} \in X_2$ as $1 - xy \in \mathfrak{q}$ since $x(1 - xy) = 0 \in \mathfrak{q}$, but $x \notin \mathfrak{q}$.

The $\mathfrak{a}_i$ are comaximal as $xy + (1 - xy) = 1$. Further $\mathfrak{a}_1\mathfrak{a}_2 = 0$ as $x(1 - xy) = 0$. So $X_1 \cup X_2 = X$ and $X_1 \cap X_2 = \emptyset$ by **(13.3)**. Hence the X_i are disjoint open and closed sets. Thus (2) holds, and X is totally disconnected.

In general, a Hausdorff space is T_1. Thus (2) implies (3).

Conditions (3) and (4) are equivalent by **(13.2)**.

Assume (4). Then every prime $\mathfrak{m}$ is both maximal and minimal. So $R_{\mathfrak{m}}$ is a local ring with $\mathfrak{m}R_{\mathfrak{m}}$ as its only prime by **(11.20)**. Hence $\mathfrak{m}R_{\mathfrak{m}} = \mathrm{nil}(R_{\mathfrak{m}})$ by the Scheinnullstellensatz **(3.29)**. But $\mathrm{nil}(R_{\mathfrak{m}}) = \mathrm{nil}(R)_{\mathfrak{m}}$ by **(11.18)**. And $\mathrm{nil}(R) = 0$. Thus $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} = R_{\mathfrak{m}}$. So $R_{\mathfrak{m}}$ is a field. Hence R is absolutely flat by **(13.48)**(2). Thus (1) holds. □

Exercise **(13.24)**. — Let B be a Boolean ring, and set $X := \mathrm{Spec}(B)$. Show a subset $U \subset X$ is both open and closed if and only if $U = \mathbf{D}(f)$ for some $f \in B$. Further, show X is a compact Hausdorff space. (Following Bourbaki, we shorten "quasi-compact" to "compact" when the space is Hausdorff.)

Solution: Let $f \in B$. Then $\mathbf{D}(f)\bigcup\mathbf{D}(1-f) = X$ whether B is Boolean or not; indeed, if $\mathfrak{p} \in X - \mathbf{D}(f)$, then $f \in \mathfrak{p}$, so $1 - f \notin \mathfrak{p}$, so $\mathfrak{p} \in \mathbf{D}(1-f)$. However, $\mathbf{D}(f)\bigcap\mathbf{D}(1-f) = \emptyset$; indeed, if $\mathfrak{p} \in \mathbf{D}(f)$, then $f \notin \mathfrak{p}$, but $f(1-f) = 0$ as B is Boolean, so $1 - f \in \mathfrak{p}$, so $\mathfrak{p} \notin \mathbf{D}(1-f)$. Thus $X - \mathbf{D}(f) = \mathbf{D}(1-f)$. Thus $\mathbf{D}(f)$ is closed as well as open.

Conversely, let $U \subset X$ be open and closed. Then U is quasi-compact, as U is closed and X is quasi-compact by **(13.20)**. So $X - U = \mathbf{V}(\mathfrak{a})$ where $\mathfrak{a}$ is finitely generated by **(13.21)**. Since B is Boolean, $\mathfrak{a} = \langle f\rangle$ for some $f \in B$ by **(1.17)**(5). Thus $U = \mathbf{D}(f)$.

Finally, let $\mathfrak{p}, \mathfrak{q}$ be prime ideals with $\mathfrak{p} \neq \mathfrak{q}$. Then there is $f \in \mathfrak{p} - \mathfrak{q}$. So $\mathfrak{p} \notin \mathbf{D}(f)$, but $\mathfrak{q} \in \mathbf{D}(f)$. By the above, $\mathbf{D}(f)$ is both open and closed. Thus X is Hausdorff. By **(13.20)**, X is quasi-compact, so compact as it is Hausdorff. □

Exercise **(13.25)** (*Stone's Theorem*). — Show every Boolean ring B is isomorphic to the ring of continuous functions from a compact Hausdorff space X to $\mathbb{F}_2$ with the discrete topology. Equivalently, show B is isomorphic to the ring R of open and closed subsets of X; in fact, $X := \mathrm{Spec}(B)$, and $B \xrightarrow{\sim} R$ is given by $f \mapsto \mathbf{D}(f)$.

Solution: The two statements are equivalent by **(1.2)**. Further, $X := \mathrm{Spec}(B)$ is compact Hausdorff, and its open and closed subsets are precisely the $\mathbf{D}(f)$ by **(13.24)**. Thus $f \mapsto D(f)$ is a well defined function, and is surjective.

This function preserves multiplication owing to **(13.1.1)**. To show it preserves addition, we must show that, for any $f, g \in B$,

$$\mathbf{D}(f+g) = (\mathbf{D}(f) - \mathbf{D}(g))\bigcup(\mathbf{D}(g) - \mathbf{D}(f)). \qquad \textbf{(13.25.1)}$$

Fix a prime $\mathfrak{p}$. There are four cases. First, if $f \notin \mathfrak{p}$ and $g \in \mathfrak{p}$, then $f + g \notin \mathfrak{p}$. Second, if $g \notin \mathfrak{p}$ but $f \in \mathfrak{p}$, then again $f + g \notin \mathfrak{p}$. In both cases, $\mathfrak{p}$ lies in the (open) sets on both sides of **(13.25.1)**.

Third, if $f \in \mathfrak{p}$ and $g \in \mathfrak{p}$, then $f + g \in \mathfrak{p}$. The first three cases do not use the hypothesis that B is Boolean. The fourth does. Suppose $f \notin \mathfrak{p}$ and $g \notin \mathfrak{p}$. Now, $B/\mathfrak{p} = \mathbb{F}_2$ by **(2.19)**. So the residues of f and g are both equal to 1. But $1 + 1 = 0 \in \mathbb{F}_2$. So again $f + g \in \mathfrak{p}$. Thus in both the third and fourth cases, $\mathfrak{p}$ lies in neither side of **(13.25.1)**. Thus **(13.25.1)** holds.

Finally, to show that $f \mapsto \mathbf{D}(f)$ is injective, suppose that $\mathbf{D}(f)$ is empty. Then $f \in \mathrm{nil}(B)$. But $\mathrm{nil}(B) = \langle 0\rangle$ by **(3.24)**. Thus $f = 0$.

Alternatively, if $\mathbf{D}(f) = D(g)$, then $\mathbf{V}(\langle f\rangle) = \mathbf{V}(\langle g\rangle)$, so $\sqrt{\langle f\rangle} = \sqrt{\langle g\rangle}$ by **(13.1)**. But $f, g \in \mathrm{Idem}(B)$ as B is Boolean. Thus $f = g$ by **(3.26)**. □

Exercise **(13.31)**. — Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Prove that

$$\mathrm{Supp}(M/\mathfrak{a}M) \subset \mathrm{Supp}(M) \cap \mathbf{V}(\mathfrak{a}),$$

with equality if M is finitely generated.

Solution: First, **(8.16)**(1) yields $M/\mathfrak{a}M = M \otimes R/\mathfrak{a}$. But $\mathrm{Ann}(R/\mathfrak{a}) = \mathfrak{a}$; hence **(13.27)**(3) yields $\mathrm{Supp}(R/\mathfrak{a}) = \mathbf{V}(\mathfrak{a})$. Thus **(13.30)** yields the assertion. □

Exercise **(13.32)**. — Let $\varphi\colon R \to R'$ be a map of rings, M an R-module. Prove

$$\mathrm{Supp}(M \otimes_R R') \subset \mathrm{Spec}(\varphi)^{-1}(\mathrm{Supp}(M)), \qquad \textbf{(13.32.1)}$$

with equality if M is finitely generated.

Solution: Fix a prime $\mathfrak{q} \subset R'$. Set $\mathfrak{p} := \varphi^{-1}\mathfrak{q}$, so $\mathrm{Spec}(\varphi)(\mathfrak{p}) = \mathfrak{q}$. Apply, in order, **(12.13)**, twice Cancellation **(8.11)**, and again **(12.13)** to obtain

$$\begin{aligned}(M \otimes_R R')_{\mathfrak{q}} &= (M \otimes_R R') \otimes_{R'} R'_{\mathfrak{q}} = M \otimes_R R'_{\mathfrak{q}}\\ &= (M \otimes_R R_{\mathfrak{p}}) \otimes_{R_{\mathfrak{p}}} R'_{\mathfrak{q}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R'_{\mathfrak{q}}.\end{aligned} \qquad \textbf{(13.32.2)}$$

First, assume $\mathfrak{q} \in \mathrm{Supp}(M \otimes_R R')$; that is, $(M \otimes_R R')_{\mathfrak{q}} \neq 0$. Then **(13.32.2)** implies $M_{\mathfrak{p}} \neq 0$; that is, $\mathfrak{p} \in \mathrm{Supp}(M)$. Thus **(13.32.1)** holds.

Conversely, assume $\mathfrak{q} \in \mathrm{Spec}(\varphi)^{-1}(\mathrm{Supp}(M))$. Then $\mathfrak{p} \in \mathrm{Supp}(M)$, or $M_{\mathfrak{p}} \neq 0$. Set $k := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Then $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} k$ and $R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}} = R'_{\mathfrak{p}} \otimes_A k$ by **(8.16)**(1). Hence Cancellation **(8.11)**, the Associative Law **(8.10)**, and **(13.32.2)** yield

$$\begin{aligned}(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}) \otimes_k (R'_{\mathfrak{q}}/\mathfrak{p}R'_{\mathfrak{q}}) &= (M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} k) \otimes_k (R'_{\mathfrak{q}} \otimes_{R_{\mathfrak{p}}} k)\\ &= M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} (R'_{\mathfrak{q}} \otimes_{R_{\mathfrak{p}}} k) = (M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R'_{\mathfrak{q}}) \otimes_{R_{\mathfrak{p}}} k\\ &= (M \otimes_R R')_{\mathfrak{q}} \otimes_{R_{\mathfrak{p}}} k.\end{aligned} \qquad \textbf{(13.32.3)}$$

Assume M is finitely generated. Then $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \neq 0$ by Nakayama's Lemma **(10.11)** over $R_{\mathfrak{p}}$. And $R'_{\mathfrak{q}}/\mathfrak{p}R'_{\mathfrak{q}} \neq 0$ by Nakayama's Lemma **(10.11)** over $R'_{\mathfrak{q}}$ as $\mathfrak{p}R' \subset \mathfrak{q}$. So $(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}) \otimes_k (R'_{\mathfrak{q}}/\mathfrak{p}R'_{\mathfrak{q}}) \neq 0$ by **(8.15)**. So **(13.32.3)** implies $(M \otimes_R R')_{\mathfrak{q}} \neq 0$, or $\mathfrak{q} \in \mathrm{Supp}(M \otimes_R R')$. Thus equality holds in **(13.32.1)**. □

Exercise **(13.33)**. — 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 **(11.29)**(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 **(13.34)**. — 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 **(12.20)**. 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 $\mathfrak{p}\mathbb{Z}_{\mathfrak{p}} \bigcap \mathbb{Z} = \mathfrak{p}$ by **(11.19)**. 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 **(13.36)**. — Let R be a domain, M a module, set $S := R - 0$, and set $T(M) := T^S(M)$. We call $T(M)$ the **torsion submodule** of M, and we say M is **torsionfree** if $T(M) = 0$.

Prove M is torsionfree if and only if $M_{\mathfrak{m}}$ is torsionfree for all maximal ideals $\mathfrak{m}$.

Solution: Given an $\mathfrak{m}$, note that $R-\mathfrak{m}\subset S$. So **(12.19)**(5) yields

$$T(M_{\mathfrak{m}})=T(M)_{\mathfrak{m}}. \tag{13.36.1}$$

Assume M is torsionfree. Then $M_{\mathfrak{m}}$ is torsionfree for all $\mathfrak{m}$ by **(13.36.1)**. Conversely, if $M_{\mathfrak{m}}$ is torsionfree for all $\mathfrak{m}$, then $T(M)_{\mathfrak{m}}=0$ for all $\mathfrak{m}$ by **(13.36.1)**. Hence $T(M)=0$ by **(13.35)**. Thus M is torsionfree. □

Exercise **(13.37)**. — Let R be a ring, P a module, M, N submodules. Assume $M_{\mathfrak{m}}=N_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Show $M=N$. First assume $M\subset N$.

Solution: If $M\subset N$, then **(12.20)** yields $(N/M)_{\mathfrak{m}}=N_{\mathfrak{m}}/M_{\mathfrak{m}}=0$ for each $\mathfrak{m}$; so $N/M=0$ by **(13.35)**. The general case follows by replacing N by $M+N$ owing to **(12.17)**(4), (5). □

Exercise **(13.38)**. — Let R be a ring, M a module, and $\mathfrak{a}$ an ideal. Suppose $M_{\mathfrak{m}}=0$ for all maximal ideals $\mathfrak{m}$ containing $\mathfrak{a}$. Show that $M=\mathfrak{a}M$.

Solution: Given any maximal ideal $\mathfrak{m}$, note that $(\mathfrak{a}M)_{\mathfrak{m}}=\mathfrak{a}_{\mathfrak{m}}M_{\mathfrak{m}}$ by **(12.2)**. But $M_{\mathfrak{m}}=0$ if $\mathfrak{m}\supset\mathfrak{a}$ by hypothesis. And $\mathfrak{a}_{\mathfrak{m}}=R_{\mathfrak{m}}$ if $\mathfrak{m}\not\supset\mathfrak{a}$ by **(11.14)**(2). Hence $M_{\mathfrak{m}}=(\mathfrak{a}M)_{\mathfrak{m}}$ in any case. Thus **(13.37)** yields $M=\mathfrak{a}M$.

Alternatively, form the ring $R/\mathfrak{a}$ and its module $M/\mathfrak{a}M$. Given any maximal ideal $\mathfrak{m}'$ of $R/\mathfrak{a}$, say $\mathfrak{m}'=\mathfrak{m}/\mathfrak{a}$. By hypothesis, $M_{\mathfrak{m}}=0$. But $M_{\mathfrak{m}}/(\mathfrak{a}M)_{\mathfrak{m}}=(M/\mathfrak{a}M)_{\mathfrak{m}}$ by **(12.22)**. Thus $(M/\mathfrak{a}M)_{\mathfrak{m}'}=0$. So $M/\mathfrak{a}M=0$ by **(13.35)**. Thus $M=\mathfrak{a}M$. □

Exercise **(13.39)**. — Let R be a ring, P a module, M a submodule, and $p\in P$ an element. Assume $p/1\in M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Show $p\in M$.

Solution: Set $N:=M+Rp$. Then $N_{\mathfrak{m}}=M_{\mathfrak{m}}+R_{\mathfrak{m}}\cdot p/1$ for every $\mathfrak{m}$. But $p/1\in M_{\mathfrak{m}}$. Hence $N_{\mathfrak{m}}=M_{\mathfrak{m}}$. So $N=M$ by **(13.37)**. Thus $p\in M$. □

Exercise **(13.40)**. — Let R be a domain, $\mathfrak{a}$ an ideal. Show $\mathfrak{a}=\bigcap_{\mathfrak{m}}\mathfrak{a}R_{\mathfrak{m}}$ where $\mathfrak{m}$ runs through the maximal ideals and the intersection takes place in $\mathrm{Frac}(R)$.

Solution: Plainly, $\mathfrak{a}\subset\bigcap\mathfrak{a}R_{\mathfrak{m}}$. Conversely, take $x\in\bigcap\mathfrak{a}R_{\mathfrak{m}}$. Then $x\in\mathfrak{a}R_{\mathfrak{m}}$ for every $\mathfrak{m}$. But $\mathfrak{a}R_{\mathfrak{m}}=\mathfrak{a}_{\mathfrak{m}}$ by **(12.2)**. So **(13.39)** yields $x\in\mathfrak{a}$ as desired. □

Exercise **(13.41)**. — 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 $\mathfrak{m}$.

If $R_{\mathfrak{m}}$ is a domain for all maximal ideals $\mathfrak{m}$, is R necessarily a domain?

Solution: Assume (1) holds. Then $\mathrm{nil}(R)=0$. But $\mathrm{nil}(R)(S^{-1}R)=\mathrm{nil}(S^{-1}R)$ by **(11.18)**. Thus (2) holds. Trivially (2) implies (3).

Assume (3) holds. Then $\mathrm{nil}(R_{\mathfrak{m}})=0$. Hence $\mathrm{nil}(R)_{\mathfrak{m}}=0$ by **(11.18)** and **(12.2)**. So $\mathrm{nil}(R)=0$ by **(13.35)**. Thus (1) holds. Thus (1)–(3) are equivalent.

Finally, the answer is no. For example, take $R:=k_1\times k_2$ with $k_i:=\mathbb{Z}/\langle 2\rangle$. The primes of R are $\mathfrak{p}:=\langle(1,0)\rangle$ and $\mathfrak{q}:=\langle(0,1)\rangle$ by **(2.11)**. Further, $R_{\mathfrak{q}}=k_1$ by **(11.7)**, as $R-\mathfrak{q}=\{(1,1),(1,0)\}$. Similarly $R_{\mathfrak{p}}=k_2$. But R is not a domain, as $(1,0)\cdot(0,1)=(0,0)$, although $R_{\mathfrak{m}}$ is a domain for all maximal ideals $\mathfrak{m}$.

In fact, take $R:=R_1\times R_2$ for any domains R_i. Then again R is not a domain, but $R_{\mathfrak{p}}$ is a domain for all primes $\mathfrak{p}$ by **(13.42)**(2) below. □

Exercise **(13.42)**. — 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 **(11.20)**. 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 **(13.41)**. 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 **(3.35)**, and surjective by (1) and the Chinese Remainder Theorem **(1.14)**. 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 **(12.11)**. 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 **(3.7)**. 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 **(13.44)**. — 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 **(13.43)**, it is surjective if and only if $\alpha_{\mathfrak{m}}\colon\big(R^{\oplus\{\lambda\}}\big)_{\mathfrak{m}}\to M_{\mathfrak{m}}$ is surjective for all $\mathfrak{m}$. But $\big(R^{\oplus\{\lambda\}}\big)_{\mathfrak{m}}=R_{\mathfrak{m}}^{\oplus\{\lambda\}}$ by **(12.11)**. Hence **(4.10)**(1) yields the assertion. □

Exercise **(13.47)**. — Let R be a ring, R' a flat algebra, $\mathfrak{p}'$ a prime in R', and $\mathfrak{p}$ its contraction in R. Prove that $R'_{\mathfrak{p}'}$ is a faithfully flat $R_{\mathfrak{p}}$-algebra.

Solution: First, $R'_{\mathfrak{p}}$ is flat over $R_{\mathfrak{p}}$ by **(13.46)**. Next, $R'_{\mathfrak{p}'}$ is flat over $R'_{\mathfrak{p}}$ by **(12.21)** and **(11.29)** as $R-\mathfrak{p}\subset R'-\mathfrak{p}'$. Hence $R'_{\mathfrak{p}'}$ is flat over $R_{\mathfrak{p}}$ by **(9.12)**. But a flat local homomorphism is faithfully flat by **(10.19)**. □

Exercise **(13.48)**. — Let R be a ring, S a multiplicative subset.

(1) Assume R is absolutely flat. Show $S^{-1}R$ is absolutely flat.
(2) Show R is absolutely flat if and only if $R_{\mathfrak{m}}$ is a field for each maximal $\mathfrak{m}$.

Solution: In (1), given $x\in R$, note that $\langle x\rangle$ is idempotent by **(10.9)**. Hence $\langle x\rangle=\langle x\rangle^2=\langle x^2\rangle$. So there is $y\in R$ with $x=x^2y$.

Given $a/s\in S^{-1}R$, there are, therefore, $b,t\in R$ with $a=a^2b$ and $s=s^2t$. So $s(st-1)=0$. So $(st-1)/1\cdot s/1=0$. But $s/1$ is a unit. Hence $s/1\cdot t/1-1=0$. So $a/s=(a/s)^2\cdot b/t$. So $a/s\in\langle a/s\rangle^2$. Thus $\langle a/s\rangle$ is idempotent. Hence $S^{-1}R$ is absolutely flat by **(10.9)**. Thus (1) holds.

Alternatively, given an $S^{-1}R$-module M, note M is also an R-module, so R-flat by (1). Hence $M\otimes S^{-1}R$ is $S^{-1}R$-flat by **(9.11)**. But $M\otimes S^{-1}R=S^{-1}M$ by **(12.13)**, and $S^{-1}M=M$ by **(12.4)**. Thus M is $S^{-1}R$-flat. Thus again (1) holds.

For (2), first assume R is absolutely flat. By (1), each $R_{\mathfrak{m}}$ is absolutely flat. So by **(10.10)**(4), each $R_{\mathfrak{m}}$ is a field.

Conversely, assume each $R_{\mathfrak{m}}$ is a field. Then, given an R-module M, each $M_{\mathfrak{m}}$ is $R_{\mathfrak{m}}$-flat. So M is R-flat by **(13.46)**. Thus (2) holds. □

Exercise **(13.52)**. — 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 **(13.51)**. 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 $p_1/f_1^{k_1}, \ldots, p_n/f_n^{k_n}$ 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 **(12.24)**(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 **(12.20)**. 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 **(13.43)** with R_f for R, as desired. □

Exercise **(13.53)**. — Let A be a semilocal ring, P a locally free module of rank n. Show that P is free of rank n.

Solution: As P is locally free, P is finitely presented by **(13.51)**, and $P_\mathfrak{m} \simeq A_\mathfrak{m}^n$ at each maximal $\mathfrak{m}$ by **(13.52)**. But A is semilocal. So $P \simeq A^n$ by **(13.45)**. □

Exercise **(13.54)**. — Let R be a ring, M a finitely presented module, $n \geq 0$. Show that M is locally free of rank n if and only if $F_{n-1}(M) = \langle 0\rangle$ and $F_n(M) = R$.

Solution: Assume M is locally free of rank n. Then so is $M_\mathfrak{m}$ for any maximal ideal $\mathfrak{m}$ by **(13.52)**. So $F_{n-1}(M_\mathfrak{m}) = \langle 0\rangle$ and $F_n(M_\mathfrak{m}) = R_\mathfrak{m}$ by **(5.39)**(2). But $F_r(M_\mathfrak{m}) = F_r(M)_\mathfrak{m}$ for all r by **(12.15)**. So $F_{n-1}(M_\mathfrak{m}) = \langle 0\rangle$ and $F_n(M_\mathfrak{m}) = R_\mathfrak{m}$ by **(13.37)**. The converse follows via reversing the above steps. □

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 **(11.24)**. Moreover, $R_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$ by **(11.22)**. 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 **(11.20)**(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 **(11.29)** 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 **(11.19)**(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 by **(10.28)** 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 **(3.29)** and **(3.14)**. So $y = 0$. Thus, if $x \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, then $x \notin \operatorname{z.div}(R)$. Thus $\operatorname{z.div}(R) \subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Thus $\operatorname{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Fix $\mathfrak{p} \in \Sigma$. Then $R_\mathfrak{p}$ is reduced by **(13.41)**. Further, $R_\mathfrak{p}$ has only one prime, namely $\mathfrak{p}R_\mathfrak{p}$, by **(11.20)**(2). Hence $R_\mathfrak{p}$ is a field, and $\mathfrak{p}R_\mathfrak{p}\langle 0\rangle$. But by **(12.23)**, $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \operatorname{Frac}(R/\mathfrak{p})$. Thus $R_\mathfrak{p} = \operatorname{Frac}(R/\mathfrak{p})$. □

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) $\operatorname{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, 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 $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$.

Solution: Assume (1) holds. Then **(14.12)** yields (2).

Assume (2) holds. Set $S := R - \operatorname{z.div}(R)$. Let $\mathfrak{q}$ be a prime of R with $\mathfrak{q} \cap S = \emptyset$. Then $\mathfrak{q} \subset \operatorname{z.div}(R)$. So (2) yields $\mathfrak{q} \subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. But Σ is finite. So $\mathfrak{q} \subset \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$ by Prime Avoidance **(3.19)**. Hence $\mathfrak{q} = \mathfrak{p}$ since $\mathfrak{p}$ is minimal. But $K = S^{-1}R$. Therefore, by **(11.20)**(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 **(12.22)**. So $S^{-1}(R/\mathfrak{p})$ is a field. But clearly $S^{-1}(R/\mathfrak{p}) \subset \operatorname{Frac}(R/\mathfrak{p})$. Therefore, $K/\mathfrak{p}K \operatorname{Frac}(R/\mathfrak{p})$ by **(2.3)**. Further, $S \subset R - \mathfrak{p}$. Hence **(11.20)**(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 **(11.27)**. But $R_\mathfrak{p} = \operatorname{Frac}(R/\mathfrak{p})$ 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, **(13.42)**(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 **(14.14)**. — Let A be a reduced local ring with residue field k and a finite set Σ of minimal primes. For each $\mathfrak{p} \in \Sigma$, set $K(\mathfrak{p}) := \operatorname{Frac}(A/\mathfrak{p})$. Let P be a finitely generated module. Show that P is free of rank r if and only if $\dim_k(P \otimes_A k) = r$ and $\dim_{K(\mathfrak{p})}(P \otimes_A K(\mathfrak{p})) = r$ for each $\mathfrak{p} \in \Sigma$.

Solution: If P is free of rank r, then $\dim(P \otimes k) = r$ and $\dim(P \otimes K(\mathfrak{p})) = r$ owing to **(8.13)**.

Conversely, suppose $\dim(P \otimes k) = r$. As P is finitely generated, **(10.16)** implies P is generated by r elements. So **(5.20)** yields an exact sequence

$$0 \to M \xrightarrow{\alpha} A^r \to P \to 0.$$

Momentarily, fix a $\mathfrak{p} \in \Sigma$. Since A is reduced, $K(\mathfrak{p}) = R_{\mathfrak{p}}$ by **(14.12)**. So $K(\mathfrak{p})$ is flat by **(12.21)**. So the induced sequence is exact:

$$0 \to M \otimes K(\mathfrak{p}) \to K(\mathfrak{p})^r \to P \otimes K(\mathfrak{p}) \to 0.$$

Suppose $\dim(P \otimes K(\mathfrak{p})) = r$ too. It then follows that $M \otimes_A K(\mathfrak{p}) = 0$.

Let K be the total quotient ring of A, and form this commutative square:

$$\begin{tikzcd} M \arrow[r, "\alpha"] \arrow[d, "\varphi_M"] & A^r \arrow[d, "\varphi_{A^r}"] \\ M \otimes K \arrow[r] & K^r \end{tikzcd}$$

Here α is injective. And φ_{A^r} is injective as $\varphi_A \colon A \to K$ is. Hence, φ_M is injective.

By hypothesis, A is reduced and Σ is finite; so $K = \prod_{\mathfrak{p} \in \Sigma} K(\mathfrak{p})$ by **(14.13)**. So $M \otimes K = \prod (M \otimes K(\mathfrak{p}))$. But $M \otimes_A K(\mathfrak{p}) = 0$ for each $\mathfrak{p} \in \Sigma$. So $M \otimes K = 0$. But $\varphi_M \colon M \to M \otimes K$ is injective. So $M = 0$. Thus $A^r \xrightarrow{\sim} P$, as desired. □

Exercise **(14.15)**. — Let A be a reduced semilocal ring with a finite set of minimal primes. Let P be a finitely generated A-module, and B an A-algebra such that $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective. For each prime $\mathfrak{q} \subset B$, set $L(\mathfrak{q}) = \operatorname{Frac}(B/\mathfrak{q})$. Given r, assume $\dim((P \otimes_A B) \otimes_B L(\mathfrak{q})) = r$ whenever $\mathfrak{q}$ is either maximal or minimal. Show that P is a free A-module of rank r.

Solution: Let $\mathfrak{p} \subset A$ be a prime. Since $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective, there is a prime $\mathfrak{q} \subset B$ whose contraction is $\mathfrak{p}$. Then the cancellation law yields

$$(P \otimes_A K(\mathfrak{p})) \otimes_{K(\mathfrak{p})} L(\mathfrak{q}) = (P \otimes_A B) \otimes_B L(\mathfrak{q}). \qquad \textbf{(14.15.1)}$$

If $\mathfrak{p}$ is minimal, take a minimal prime $\mathfrak{q}' \subset \mathfrak{q}$. Then the contraction of $\mathfrak{q}'$ is contained in $\mathfrak{p}$, so equal to $\mathfrak{p}$. Replace $\mathfrak{q}$ by $\mathfrak{q}'$. If $\mathfrak{p}$ is maximal, take a maximal ideal $\mathfrak{q}' \supset \mathfrak{q}$. Then the contraction of $\mathfrak{q}'$ contains $\mathfrak{p}$, so is equal to $\mathfrak{p}$. Again, replace $\mathfrak{q}$ by $\mathfrak{q}'$. Either way, $\dim((P \otimes_A B) \otimes_B L(\mathfrak{q})) = r$ by hypothesis. So **(14.15.1)** yields $\dim\big((P \otimes_A K(\mathfrak{p})) \otimes_{K(\mathfrak{p})} L(\mathfrak{q})\big) = r$. Hence $\dim(P \otimes_A K(\mathfrak{p})) = r$.

If A is local, then P is a free A-module of rank r by **(14.14)**. In general, let $\mathfrak{m} \subset A$ be a maximal ideal. Then $\operatorname{Spec}(B_{\mathfrak{m}}) \to \operatorname{Spec}(A_{\mathfrak{m}})$ is surjective by an argument like one in the proof of **(14.3)**(2), using **(11.20)**(2). Hence $P_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module of rank r by the preceding case. Thus P is free of rank r by **(13.53)**. □

Exercise **(14.17)**. — 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.

Solution: Assume (1). Let $\mathfrak{m}$ any maximal ideal. Then $R_{\mathfrak{m}}$ is a normal domain. So R is reduced by **(13.41)**.

Let S_0 be the set of nonzerodivisors of R, so that $K := S_0^{-1}R$. Set $S := R - \mathfrak{m}$, so that $R_{\mathfrak{m}} := S^{-1}R$. But $S^{-1}S_0^{-1}RS_0^{-1}S^{-1}R$ by **(11.29)**(2). So $S^{-1}K = S_0^{-1}R_{\mathfrak{m}}$.

Let $t \in S_0$. Then $t/1 \neq 0$ in $R_{\mathfrak{m}}$; else, there's $s \in S$ with $st = 0$, a contradiction as $s \neq 0$ and $t \in S_0$. Thus **(11.23)** and **(11.3)** yield $S_0^{-1}R_{\mathfrak{m}} \subset \operatorname{Frac}(R_{\mathfrak{m}})$.

Let $x \in K$ be integral over R. Then $x/1 \in S^{-1}K$ is integral over $S^{-1}R$ by **(11.24)**. But $S^{-1}R = R_{\mathfrak{m}}$, and $R_{\mathfrak{m}}$ is a normal domain. So $x/1 \in R_{\mathfrak{m}}$. Hence $x \in R$ by **(13.39)**. Thus (2) holds.

Assume (2). Set $R_i := R/\mathfrak{p}_i$ and $K_i := \operatorname{Frac}(R_i)$. 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 **(10.29)**, and the second, by **(10.31)**; whence, $R \subset \prod R_i'$ is integral by the tower property **(10.27)**. However, R is integrally closed in K by hypothesis. Hence $R = \prod R_i = \prod R_i'$. Thus (3) holds.

Assume (3). Let $\mathfrak{p}$ be any prime of R. Then $R_{\mathfrak{p}} = \prod (R_i)_{\mathfrak{p}}$ by **(12.11)**, and each $(R_i)_{\mathfrak{p}}$ is normal by **(11.32)**. But $R_{\mathfrak{p}}$ is local. So $R_{\mathfrak{p}} = (R_i)_{\mathfrak{p}}$ for some i by **(3.7)**. Hence $R_{\mathfrak{p}}$ is a normal domain. Thus (1) holds.

Finally, the last assertion results from **(13.42)**(2). □

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 **(10.23)**, 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

$$R := k[X, Y, Z]\big/\langle X^2 - Y^3 - 1,\ XZ - 1\rangle,$$

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, **(10.27)**, 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 **(10.28)**.

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

(10.34)(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 **(15.8)**. — Let k be a field, K an algebraically closed extension field. (So K contains a copy of every finite extension field.) Let $P := k[X_1, \ldots, X_n]$ be the polynomial ring, and $f, f_1, \ldots, f_r \in P$. Assume f vanishes at every zero in K^n of $f_1, \ldots, f_r$; in other words, if $(a) := (a_1, \ldots, a_n) \in K^n$ and $f_1(a) = 0, \ldots, f_r(a) = 0$, then $f(a) = 0$ too. Prove that there are polynomials $g_1, \ldots, g_r \in P$ and an integer N such that $f^N g_1 f_1 + \cdots + g_r f_r$.

Solution: Set $\mathfrak{a} := \langle f_1, \ldots, f_r \rangle$. 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 $(a) := (a_1, \ldots, a_n) \in K^n$. Then $f_1(a) = 0, \ldots, f_r(a) = 0$. Hence $f(a) = 0$ by hypothesis. Therefore, $f \in \mathfrak{m}$, as desired. □

Exercise **(15.11)**. — 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 **(15.12)**. — 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 **(15.17)**. — 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 **(11.13)**, as R_f is, by **(11.13)**, 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 $\operatorname{tr.deg}_k(K)$ by **(15.13)**. □

Exercise **(15.18)**. — 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 **(2.25)** or **(15.13)**. So $\langle 0 \rangle$ and $\mathfrak{p}R$ are the only primes in R by **(11.20)**. Thus $\dim(R) = 1$.

Set $K := \operatorname{Frac}(P)$. 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 $\dim(R_f) = 0$. □

Exercise **(15.19)**. — Let R be a ring, $R[X]$ the polynomial ring. Prove

$$1 + \dim(R) \le \dim(R[X]) \le 1 + 2\dim(R).$$

(In particular, $\dim(R[X]) = \infty$ if and only if $\dim(R) = \infty$.)

Solution: Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ be a chain of primes in R. Then

$$\mathfrak{p}_0 R[X] \subsetneqq \cdots \subsetneqq \mathfrak{p}_n R[X] \subsetneqq \mathfrak{p}_n R[X] + \langle X \rangle$$

is a chain of primes in $R[X]$ by **(2.18)**. Thus $1 + \dim(R) \le \dim(R[X])$.

Let $\mathfrak{p}$ be a prime of R, and $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r$ be a chain of primes of $R[X]$ with $\mathfrak{q}_i \cap R = \mathfrak{p}$ for each i. Then **(1.9)** yields a chain of primes of length r in $R[X]/\mathfrak{p}R[X]$. Further, as $\mathfrak{q}_i \cap R = \mathfrak{p}$ for each i, the latter chain gives rise to a chain of primes of length r in $k(\mathfrak{p})[X]$ where $k(\mathfrak{p}) = (R/\mathfrak{p})_{\mathfrak{p}}$ by **(11.30)** and **(11.20)**. But $k(\mathfrak{p})[X]$ is a PID. Hence $r \le 1$.

Take any chain $\mathfrak{P}_0 \subsetneqq \cdots \subsetneqq \mathfrak{P}_m$ of primes in $R[X]$. It contracts to a chain $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ in R. At most two $\mathfrak{P}_j$ contract to a given $\mathfrak{p}_i$ by the above discussion. So $m + 1 \le 2(n + 1)$, or $m \le 2n + 1$. Thus $\dim(R[X]) \le 1 + 2\dim(R)$. □

Exercise **(15.23)**. — Let X be a topological space. We say a subset Y is **locally closed** if Y is the intersection of an open set and a closed set; equivalently, Y is open in its closure $\overline{Y}$; equivalently, Y is closed in an open set containing it.

We say a subset X_0 of X is **very dense** if X_0 meets every nonempty locally closed subset Y. We say X is **Jacobson** if its set of closed points is very dense.

Show that the following conditions on a subset X_0 of X are equivalent:

(1) X_0 is very dense.
(2) Every closed set F of X satisfies $\overline{F \cap X_0} = F$.
(3) The map $U \mapsto U \cap X_0$ from the open sets of X to those of X_0 is bijective.

Solution: Assume (1). Given a closed set F, take any $x \in F$, and let U be an open neighborhood of x in X. Then $F \cap U$ is locally closed, so meets X_0. Hence $x \in \overline{F \cap X_0}$. Thus $F \subset \overline{F \cap X_0}$. The opposite inclusion is trivial. Thus (2) holds.

Assume (2). In (3), the map is trivially surjective. To check it's injective, suppose $U \cap X_0 = V \cap X_0$. Then $(X - U) \cap X_0 = (X - V) \cap X_0$. So (2) yields $X - U = X - V$. So $U = V$. Thus (3) holds.

Assume (3). Then the map $F \mapsto F \cap X_0$ of closed sets is bijective too; whence, so is the map $Y \mapsto Y \cap X_0$ of locally closed sets. In particular, if a locally closed set Y is nonempty, then so is $Y \cap X_0$. Thus (1) holds. □

Exercise **(15.24)**. — Let R be a ring, $X := \operatorname{Spec}(R)$, and X_0 the set of closed points of X. Show that the following conditions are equivalent:

(1) R is a Jacobson ring.
(2) X is a Jacobson space.
(3) If $y \in X$ is a point such that $\{y\}$ is locally closed, then $y \in X_0$.

Solution: Assume (1). Let $F \subset X$ be closed. Trivially, $F \supset \overline{F \cap X_0}$. To prove $F \subset \overline{F \cap X_0}$, say $F = \mathbf{V}(\mathfrak{a})$ and $\overline{F \cap X_0} = \mathbf{V}(\mathfrak{b})$. Then $F \cap X_0$ is the set of maximal ideals $\mathfrak{m}$ containing $\mathfrak{a}$ by **(13.2)**, and every such $\mathfrak{m}$ contains $\mathfrak{b}$. So (1) implies $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$. But $\mathbf{V}(\sqrt{\mathfrak{a}}) = F$. Thus $F \subset \overline{F \cap X_0}$. Thus **(15.23)** yields (2).

Assume (2). Let $y \in X$ be a point such that $\{y\}$ is locally closed. Then $\{y\} \bigcap X_0$ is nonempty by (2). So $(\{y\} \bigcap X_0) \ni y$. Thus (3) holds.

Assume (3). Let $\mathfrak{p}$ be a prime ideal of R such that $\mathfrak{p}R_f$ is maximal for some $f \notin \mathfrak{p}$. Then $\{\mathfrak{p}\}$ is closed in $\mathbf{D}(f)$ by **(13.1)**. So $\{\mathfrak{p}\}$ is locally closed in X. Hence $\{\mathfrak{p}\}$ is closed in X by (3). Thus $\mathfrak{p}$ is maximal. Thus **(15.22)** yields (1). □

Exercise **(15.28)**. — Let $P := \mathbb{Z}[X_1, \ldots, X_n]$ be the polynomial ring. Assume $f \in P$ vanishes at every zero in K^n of $f_1, \ldots, f_r \in P$ for every finite field K; that is, if $(a) := (a_1, \ldots, a_n) \in K^n$ and $f_1(a) = 0, \ldots, f_r(a) = 0$ in K, then $f(a) = 0$ too. Prove there are $g_1, \ldots, g_r \in P$ and $N \geq 1$ such that $f^N = g_1 f_1 + \cdots + g_r f_r$.

Solution: Set $\mathfrak{a} := \langle f_1, \ldots, f_r \rangle$. Suppose $f \notin \sqrt{\mathfrak{a}}$. Then f lies outside some maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$ by **(15.26)**(2) and **(15.20)**. Set $K := P/\mathfrak{m}$. Then K is a finite extension of $\mathbb{F}_p$ for some prime p by **(15.26)**(1). So K is finite. Let a_i be the residue of X_i, set $(a) := (a_1, \ldots, a_n) \in K^n$. Then $f_1(a) = 0, \ldots, f_r(a) = 0$. So $f(a) = 0$ by hypothesis. Thus $f \in \mathfrak{m}$, a contradiction. Thus $f \in \sqrt{\mathfrak{a}}$. □

Exercise **(15.29)**. — Let R be a ring, R' an algebra. Prove that if R' is integral over R and R is Jacobson, then R' is Jacobson.

Solution: Given an ideal $\mathfrak{a}' \subset R'$ and an f outside $\sqrt{\mathfrak{a}'}$, set $R'' := R[f]$. Then R'' is Jacobson by **(15.26)**(2). So R'' has a maximal ideal $\mathfrak{m}''$ that avoids f and contains $\mathfrak{a}' \cap R''$. But R' is integral over R''. So R' contains a prime $\mathfrak{m}'$ that contains $\mathfrak{a}'$ and that contracts to $\mathfrak{m}''$ by Going Up **(14.3)**(4). Then $\mathfrak{m}'$ avoids f as $\mathfrak{m}''$ does, and $\mathfrak{m}'$ is maximal by Maximality, **(14.3)**(1). Thus R' is Jacobson. □

Exercise **(15.30)**. — Let R be a Jacobson ring, S a multiplicative subset, $f \in R$. True or false: prove or give a counterexample to each of the following statements.

(1) The localized ring R_f is Jacobson.
(2) The localized ring $S^{-1}R$ is Jacobson.
(3) The filtered direct limit $\varinjlim R_\lambda$ of Jacobson rings is Jacobson.
(4) In a filtered direct limit of rings R_λ, necessarily $\varinjlim \operatorname{rad}(R_\lambda) = \operatorname{rad}(\varinjlim R_\lambda)$.

Solution: (1) True: $R_f = R[1/f]$ by **(11.13)**; so R_f is Jacobson by **(15.26)**(1).
(2) False: by **(15.21)**, $\mathbb{Z}$ is Jacobson, but $\mathbb{Z}_{\langle p \rangle}$ isn't for any prime number p.
(3) False: $Z_{\langle p \rangle}$ isn't Jacobson by **(15.21)**, but $Z_{\langle p \rangle} = \varinjlim \mathbb{Z}$ by **(12.6)**.
(4) False: $\operatorname{rad}(\mathbb{Z}_{\langle p \rangle}) = p\mathbb{Z}_{\langle p \rangle}$; but $\operatorname{rad}(\mathbb{Z}) = \langle 0 \rangle$, so $\varinjlim \operatorname{rad}(\mathbb{Z}) = \langle 0 \rangle$. □

Exercise **(15.31)**. — Let R be a reduced Jacobson ring with a finite set Σ of minimal primes, and P a finitely generated module. Show that P is locally free of rank r if and only if $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$ for any maximal ideal $\mathfrak{m}$.

Solution: Suppose P is locally free of rank r. Then given any maximal ideal $\mathfrak{m}$, there is an $f \in R - \mathfrak{m}$ such that P_f is a free R_f-module of rank r by **(13.49)**. But $P_\mathfrak{m}$ is a localization of P_f by **(12.5)**. So $P_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module of rank r by **(12.11)**. But $P_\mathfrak{m}/\mathfrak{m}P_\mathfrak{m} = (P/\mathfrak{m}P)_\mathfrak{m}$ by **(12.22)**. Also $R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m} = R/\mathfrak{m}$ by **(12.23)**. Thus $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$.

Consider the converse. Given a $\mathfrak{p} \in \Sigma$, set $K := \operatorname{Frac}(R/\mathfrak{p})$. Then $P \otimes_R K$ is a K-vector space, say of dimension n. Since R is reduced, $K = R_\mathfrak{p}$ by **(14.12)**. So by **(12.24)**, there is an $h \in R - \mathfrak{p}$ with P_h free of rank n. As R is Jacobson, there is a maximal ideal $\mathfrak{m}$ avoiding h, by **(15.20)**. Hence, as above, $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = n$. But, by hypothesis, $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$. Thus $n = r$.

Given a maximal ideal $\mathfrak{m}$, set $A := R_\mathfrak{m}$. Then A is reduced by **(13.41)**. Each minimal prime of A is of the form $\mathfrak{p}A$ where $\mathfrak{p} \in \Sigma$ by **(11.20)**(2). Further, it's not hard to see, essentially as above, that $P_\mathfrak{m} \otimes \operatorname{Frac}(A/\mathfrak{p}A) = P \otimes \operatorname{Frac}(R/\mathfrak{p})$. Hence **(14.14)** implies $P_\mathfrak{m}$ is a free A-module of rank r. Finally, **(13.52)** implies P is locally free of rank r. □

16. Chain Conditions

Exercise **(16.2)**. — Let M be a finitely generated module over an arbitrary ring. Show every set that generates M contains a finite subset that generates.

Solution: Say M is generated by $x_1, \ldots, x_n$ and also by the y_λ for $\lambda \in \Lambda$. Say $x_i = \sum_j z_j y_{\lambda_{ij}}$. Then the $y_{\lambda_{ij}}$ generate M. □

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 **(1.8)**; so R is Noetherian. □

Exercise **(16.9)**. — Let $R \subset R'$ be a ring extension with an R-linear retraction $\rho\colon R' \to R$. Assume R' is Noetherian, and prove R is too.

Solution: Let $\mathfrak{a} \subset R$ be an ideal. As R' is Noetherian, $\mathfrak{a}R'$ is finitely generated. But, by definition, $\mathfrak{a}$ generates $\mathfrak{a}R'$. So by **(16.2)** there are $a_1, \ldots, a_n$ that generate $\mathfrak{a}R'$. Hence, given any $a \in \mathfrak{a}$, there are $x_i' \in R'$ such that $a = a_1 x_1' + \cdots + a_n' x_n'$. Applying ρ yields $a = a_1 x_1 + \cdots + a_n x_n$ with $x_i := \rho(x_i') \in R$. Thus $\mathfrak{a}$ is finitely generated. Thus R is Noetherian.

Alternatively, let $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ be an ascending chain of ideals of R. Then $\mathfrak{a}_1 R' \subset \mathfrak{a}_2 R' \subset \cdots$ stabilizes as R' is Noetherian. So $\rho(\mathfrak{a}_1 R') \subset \rho(\mathfrak{a}_2 R') \subset \cdots$ stabilizes too. But $\rho(\mathfrak{a}_i R') = \mathfrak{a}_i \rho(R') = \mathfrak{a}_i$. Thus by **(16.5)**, R is Noetherian. □

Exercise **(16.15)**. — 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 **(16.18)**. — 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 **(16.17)**. 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 **(16.16)**(2). So R is a Noetherian ring by **(16.13)**. □

Exercise **(16.20)**. — Let R be a Noetherian ring, M and N finitely generated modules. Show that $\mathrm{Hom}(M,N)$ is finitely generated.

Solution: Say M is generated m elements. Then **(4.10)** yields a surjection $R^{\oplus m} \twoheadrightarrow M$. It yields an inclusion $\mathrm{Hom}(M,N) \hookrightarrow \mathrm{Hom}(R^m,N)$ by **(5.18)**. But $\mathrm{Hom}(R^{\oplus m},N) = \mathrm{Hom}(R,N)^{\oplus m} = N^{\oplus m}$ by **(4.15.2)** and **(4.3)**. Plainly $N^{\oplus m}$ is finitely generated as N is. Hence $\mathrm{Hom}(R^{\oplus m},N)$ is finitely generated, so Noetherian by **(16.19)**. Thus $\mathrm{Hom}(M,N)$ is finitely generated. □

Exercise **(16.24)**. — Let R be a domain, R' an algebra, and set $K := \mathrm{Frac}(R)$. Assume R is Noetherian.

(1) [**1**, Thm. 3] Assume R' is a field containing R. Show R'/R is algebra finite if and only if K/R is algebra finite and R'/K is (module) finite.

(2) [**1**, bot. p. 77] Let $K' \supset R$ be a field that embeds in R'. Assume R'/R is algebra finite. Show K/R is algebra finite and K'/K is finite.

Solution: For (1), first assume R'/R is algebra finite. Now, $R \subset K \subset R'$. So R'/K is algebra finite. Thus R'/K is (module) finite by **(15.4)** or **(16.22)**, and so K/R is algebra finite by **(16.21)**.

Conversely, say $x_1,\ldots,x_m$ are algebra generators for K/R, and say $y_1,\ldots,y_n$ are module generators for R'/K. Then clearly $x_1,\ldots,x_m,y_1,\ldots,y_n$ are algebra generators for R'/R. Thus (1) holds.

For (2), let $\mathfrak{m}$ be any maximal ideal of R', and set $L := R'/\mathfrak{m}$. Then L is a field, $R \subset K \subset K' \subset L$, and L/R is algebra finite. So K/R is algebra finite and L/K is finite by (1); whence, K'/K is finite too. Thus (2) holds. □

Exercise **(16.28)**. — 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 **(16.29)**. — 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 $0 \le r \le e$. Therefore, either $N = M$, or there is a largest integer $e \ge 0$ 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 $n_1 \ge n_2 \ge \cdots$ 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 **(16.30)**. — 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 $x^e a x^{e+1}$ 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 **(16.27)**(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 **(2.17)**. □

17. Associated Primes

Exercise **(17.6)**. — Given modules $M_1,\ldots,M_r$, set $M := M_1 \oplus \cdots \oplus M_r$. Prove

$$\mathrm{Ass}(M) = \mathrm{Ass}(M_1) \cup \cdots \cup \mathrm{Ass}(M_r).$$

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

$$\mathrm{Ass}(N),\ \mathrm{Ass}(M_1) \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(M_1).$$

So $\mathrm{Ass}(M) = \mathrm{Ass}(N) \cup \mathrm{Ass}(M_1)$. 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 $\mathrm{Ass}(M)$ and find two submodules $L,\ N \subset M$ with $L + N = M$ but $\mathrm{Ass}(L) \cup \mathrm{Ass}(N) \subsetneqq \mathrm{Ass}(M)$.

Solution: First, we have $\mathrm{Ass}(M) = \{\langle 0\rangle, \langle 2\rangle\}$ by **(17.6)** and **(17.4)**(2). Next, take $L := R\cdot(1,1)$ and $N := R\cdot(0,1)$. Then the canonical maps $R \to L$ and $R \to N$ are isomorphisms. Hence both $\mathrm{Ass}(L)$ and $\mathrm{Ass}(N)$ 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 **(17.8)**. — If a prime $\mathfrak{p}$ is sandwiched between two primes in $\mathrm{Ass}(M)$, is $\mathfrak{p}$ necessarily in $\mathrm{Ass}(M)$ too?

Solution: No, for example, let $R := k[X,Y]$ be the polynomial ring over a field. Set $M := R \oplus (R/\langle X,Y\rangle)$ and $\mathfrak{p} := \langle X\rangle$. Then $\mathrm{Ass}(M) = \mathrm{Ass}(R) \cup \mathrm{Ass}(R/\langle X,Y\rangle)$ by **(17.6)**. Further, $\mathrm{Ass}(R) = \langle 0\rangle$ and $\mathrm{Ass}(R/\langle X,Y\rangle) = \langle X,Y\rangle$ by **(17.4)**. □

Exercise **(17.11)**. — 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 $\mathfrak{p} \in \mathrm{Ass}(R)$. Then $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}(R_{\mathfrak{p}})$ by **(17.10)**. 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 **(11.20)**(2).

Alternatively, say $\mathfrak{p} = \mathrm{Ann}(x)$ with $x \in R$. Then $x/1 \ne 0$ in $R_{\mathfrak{p}}$; otherwise, there would be some $s \in R - \mathfrak{p}$ such that $sx = 0$, contradicting $\mathfrak{p} = \mathrm{Ann}(x)$. 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 $x/1 \ne 0$, 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 **(3.14)**. Suppose $\mathfrak{p} \ne \mathfrak{q}$. 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 **(17.16)**. — 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 $xM \cap N = xN$.

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 **(17.15)**, $x \notin \mathrm{z.div}(M/N)$. So $m' = 0$. So $m \in N$. So $xm \in xN$. Thus $xM \bigcap N \subset xN$, as desired. □

Exercise **(17.22)**. — 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 $\mathfrak{a} = \mathrm{Ann}(R/\mathfrak{a})$, the primes in question are the primes minimal in $\mathrm{Supp}(R/\mathfrak{a})$ by **(13.27)**(3). So they are associated to $\mathfrak{a}$ by **(17.18)**, and they are finite in number by **(17.21)**. □

Exercise **(17.23)**. — Take $R := \mathbb{Z}$ and $M := Z$ in **(17.20)**. Determine when a chain $0 \subset M_1 \subsetneqq M$ is acceptable, and show that then $\mathfrak{p}_2 \notin \mathrm{Ass}(M)$.

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 $M_1 = \mathrm{Ann}(M/M_1) = \mathfrak{p}_2$. 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, $\mathrm{Ass}(M) = 0$ by **(17.4)**. Further, as just observed, given any acceptable chain, $\mathfrak{p}_2 = M_1 \neq 0$. So $\mathfrak{p}_2 \notin \mathrm{Ass}(M)$. □

Exercise **(17.24)**. — Take $R := \mathbb{Z}$ and $M := Z/\langle 12\rangle$ in **(17.20)**. Find all three acceptable chains, and show that, in each case, $\{\mathfrak{p}_i\} = \mathrm{Ass}(M)$.

Solution: An acceptable chain in M corresponds to a 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 **(17.20.1)** yields $\mathrm{Ass}(M) \subset \{\langle 2\rangle, \langle 3\rangle\}$. For any M, if $0 \subset M_1 \subset \cdots \subset M$ is an acceptable chain, then **(17.5)** and **(17.4)**(2) yield $\mathrm{Ass}(M) \supset \mathrm{Ass}(M_1) = \{\mathfrak{p}_1\}$. Here, there's one chain with $\mathfrak{p}_1 = \langle 2\rangle$ and another with $\mathfrak{p}_1 = \langle 3\rangle$; hence, $\mathrm{Ass}(M) \supset \{\langle 2\rangle, \langle 3\rangle\}$. Thus $\mathrm{Ass}(M) = \{\langle 2\rangle, \langle 3\rangle\}$. □

Exercise **(17.26)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Show that the following conditions are equivalent:

(1) $\mathbf{V}(\mathfrak{a}) \cap \mathrm{Ass}(M) = \emptyset$;
(2) $\mathrm{Hom}(N, M) = 0$ for all finitely generated modules N with $\mathrm{Supp}(N) \subset \mathbf{V}(\mathfrak{a})$;
(3) $\mathrm{Hom}(N, M) = 0$ for some finitely generated module N with $\mathrm{Supp}(N) = \mathbf{V}(\mathfrak{a})$;
(4) $\mathfrak{a} \not\subset \mathrm{z.div}(M)$; that is, there is a nonzerodivisor x on M in $\mathfrak{a}$;
(5) $\mathfrak{a} \not\subset \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Ass}(M)$.

Solution: Assume (1). Then $\mathrm{Supp}(N) \cap \mathrm{Ass}(M) = \emptyset$ for any module N with $\mathrm{Supp}(N) \subset \mathbf{V}(\mathfrak{a})$. Hence $\mathrm{Ass}(\mathrm{Hom}(N, M)) = \emptyset$ by **(17.25)**. So $\mathrm{Hom}(N, M) = 0$ by **(17.13)**. Thus (2) holds. Clearly (2) with $N := R/\mathfrak{a}$ implies (3).

Assume (3). Then $\mathrm{Ass}(\mathrm{Hom}(N, M)) = \emptyset$ by **(17.13)**. So $\mathbf{V}(\mathfrak{a}) \cap \mathrm{Ass}(M) = \emptyset$ by **(17.25)**. Thus (1) holds. Clearly (1) and (5) are equivalent.

Finally, $\mathrm{z.div}(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$ by **(17.15)**. So (4) implies (5). Moreover, the union is finite by **(17.21)**; so **(3.19)** and (5) yield (4). □

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 $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by **(17.4)**(2). Hence **(17.5)** yields $\mathrm{Ass}(R/\mathfrak{p}^n) = \{\mathfrak{p}\}$ 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 **(3.33)**. 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 **(3.25)**. The converse can be proved similarly. □

Exercise **(18.17)**. — 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 **(18.18)**. — 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 **(18.22)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Consider the following submodule of M:

$$\Gamma_{\mathfrak{a}}(M) := \bigcup_{n\geq 1}\{m \in M \mid \mathfrak{a}^n m = 0 \text{ for some } n \geq 1\}.$$

(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 $\mathfrak{a} \subset \mathfrak{p}_j$. Then $\mathfrak{p}_j = \operatorname{nil}(M/Q_j)$ by **(18.3)**. So there is n_j with $\mathfrak{a}^{n_j} m \subset Q_j$. Set $n := \max\{n_j\}$. Then $\mathfrak{a}^n m \subset Q_i$ for all i, whether $\mathfrak{a} \subset \mathfrak{p}_i$ or not. Hence $\mathfrak{a}^n m \in \bigcap Q_i = 0$. 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 **(18.21)**. 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 **(18.26)**. — Let R be a Noetherian ring, M a finitely generated module, N a submodule. Prove $N = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(M/N)} \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$.

SOLUTION: **(18.21)** yields an irredundant primary decomposition $N = \bigcap_1^r Q_i$. Say Q_i is $\mathfrak{p}_i$-primary. Then $\{\mathfrak{p}_i\}_1^r = \operatorname{Ass}(M/N)$ by **(18.20)**. Also, **(18.24)** yields $\varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) = \bigcap_{\mathfrak{p}_j\subset\mathfrak{p}_i} Q_j$. Thus $\bigcap_1^r \varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) = \bigcap_1^r \big(\bigcap_{\mathfrak{p}_j\subset\mathfrak{p}_i} Q_j\big) = \bigcap_1^r Q_i = N$. □

EXERCISE **(18.27)**. — Let R be a Noetherian ring, $\mathfrak{p}$ a prime. Its n**th symbolic power** $\mathfrak{p}^{(n)}$ is defined as the saturation $(\mathfrak{p}^n)^S$ where $S := R - \mathfrak{p}$.

(1) Show $\mathfrak{p}^{(n)}$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^n$.
(2) Show $\mathfrak{p}^{(m+n)}$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^{(n)}\mathfrak{p}^{(m)}$.
(3) Show $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ if and only if $\mathfrak{p}^n$ is $\mathfrak{p}$-primary.
(4) Given a $\mathfrak{p}$-primary ideal $\mathfrak{q}$, show $\mathfrak{q} \supset \mathfrak{p}^{(n)}$ for all large n.

SOLUTION: Note $\mathfrak{p}$ is minimal in $\mathbf{V}(\mathfrak{p}^n)$. But $\mathbf{V}(\mathfrak{p}^n)\operatorname{Supp}(R/\mathfrak{p}^n)$ by **(13.27)**(3). Hence $\mathfrak{p}$ is minimal in $\operatorname{Ass}(R/\mathfrak{p}^n)$ by **(17.18)** and **(17.3)**. Thus **(18.25)** yields (1).

Notice **(11.17)**(3) yields $(\mathfrak{p}^{(m)}\mathfrak{p}^{(n)})^S = \mathfrak{p}^{(m+n)}$. Thus **(18.25)** yields (2).

If $\mathfrak{p}^{(n)} = \mathfrak{p}^n$, then $\mathfrak{p}^n$ is $\mathfrak{p}$-primary by (1). Conversely, if $\mathfrak{p}^n$ is $\mathfrak{p}$-primary, then $\mathfrak{p}^n = \mathfrak{p}^{(n)}$ because primary ideals are saturated by **(18.23)**. Thus (3) holds.

For (4), recall $\mathfrak{p} = \sqrt{\mathfrak{q}}$ by **(18.5)**. So $\mathfrak{q} \supset \mathfrak{p}^n$ for all large n by **(3.33)**. Hence $\mathfrak{q}^S \supset \mathfrak{p}^{(n)}$. But $\mathfrak{q}^S = \mathfrak{q}$ by **(18.23)** since $\mathfrak{p} \cap (R - \mathfrak{p}) = \emptyset$. Thus (4) holds. □

EXERCISE **(18.28)**. — Let R be a Noetherian ring, $\langle 0\rangle = \mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n$ an irredundant primary decomposition. Set $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ for $i = 1, \ldots, n$.

(1) Suppose $\mathfrak{p}_i$ is minimal for some i. Show $\mathfrak{q}_i = \mathfrak{p}_i^{(r)}$ for all large r.

(2) Suppose $\mathfrak{p}_i$ is not minimal for some i. Show that replacing $\mathfrak{q}_i$ by $\mathfrak{p}_i^{(r)}$ for large r gives infinitely many distinct irredundant primary decompositions of $\langle 0\rangle$.

SOLUTION: Set $A := R_{\mathfrak{p}_i}$ and $\mathfrak{m} := \mathfrak{p}_i A$. Then A is Noetherian by **(16.7)**. Suppose $\mathfrak{p}_i$ is minimal. Then $\mathfrak{m}$ is the only prime in A. So $\mathfrak{m} = \sqrt{\langle 0\rangle}$ by the Scheinnullstellensatz **(3.29)**. So $\mathfrak{m}^r = 0$ for all large r by **(3.32)**. So $p^{(r)} = \mathfrak{q}_i$ by Lemma **(18.23)** and the Second Uniqueness Theorem **(18.25)**. Thus (1) holds.

Suppose $\mathfrak{p}_i$ is not minimal. Assume $\mathfrak{m}^r = \mathfrak{m}^{r+1}$ for some r. Then $\mathfrak{m}^r = 0$ by Nakayama's Lemma **(10.11)**. Hence $\mathfrak{m}$ is minimal. So $\mathfrak{p}_i$ is too, contrary to hypothesis. Thus by **(11.19)**(1), the powers $\mathfrak{p}_i^{(r)}$ are distinct.

However, $\mathfrak{q}_i \supset \mathfrak{p}_i^{(r)}$ for all large r by **(18.27)**(4). Hence $\langle 0\rangle = \mathfrak{p}_i^{(r)} \cap \bigcap_{j\neq i}\mathfrak{q}_j$. But $\mathfrak{p}_i^{(r)}$ is $\mathfrak{p}_i$-primary by **(18.27)**(1). Thus replacing $\mathfrak{q}_i$ by $\mathfrak{p}_i^{(r)}$ for large r gives infinitely many distinct primary decompositions of $\langle 0\rangle$.

These decompositions are irredundant owing to two applications of **(18.19)**. A first yields $\{\mathfrak{p}_i\} = \operatorname{Ass}(R)$ as $\langle 0\rangle\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n$ is irredundant. So a second yields the desired irredundancy. □

EXERCISE **(18.30)**. — Let R be a Noetherian ring, $\mathfrak{m} \subset \operatorname{rad}(R)$ an ideal, M a finitely generated module, and M' a submodule. Considering M/M', 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 **(18.29)**, there is $x \in \mathfrak{m}$ such that $(1 + x)N = 0$. By **(3.2)**, $1 + x$ is a unit since $\mathfrak{m} \subset \operatorname{rad}(R)$. So $N = 0$. But $\mathfrak{m}^n(M/M')(\mathfrak{m}^n M + M')/M'$. 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 $\mathfrak{m} = \operatorname{Ann}(M)$.
(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 $\mathfrak{m} := \operatorname{Ann}(M)$ by **(4.7)**. Since M is simple, $\mathfrak{m}$ is maximal owing to the bijective correspondence of **(1.9)**. 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 **(16.16)**(1). Thus (3) holds. □

EXERCISE **(19.4)**. — Let R be a Noetherian ring, M a finitely generated module. Prove the equivalence of the following three conditions:

(1) that M has finite length;
(2) that $\operatorname{Supp}(M)$ consists entirely of maximal ideals;
(3) that $\operatorname{Ass}(M)$ consists entirely of maximal ideals.

Prove that, if the conditions hold, then $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ are equal and finite.

Solution: Assume (1). Then **(19.3)** yields (2).

Assume (2). Then **(17.20)** and **(19.2)**(2) yield (1). Further, **(17.3)** yields (3).

Finally, assume (3). Then **(17.3)** and **(17.17)** imply that $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ are equal and consist entirely of maximal ideals. In particular, (2) holds. However, $\mathrm{Ass}(M)$ is finite by **(17.21)**. Thus the last assertion holds. □

Exercise **(19.5)**. — Let R be a Noetherian ring, $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal. Consider chains of primary ideals from $\mathfrak{q}$ to $\mathfrak{p}$. Show (1) all such chains have length at most $\ell(A)-1$ where $A := (R/\mathfrak{q})_{\mathfrak{p}}$ and (2) all maximal chains have length exactly $\ell(A)-1$.

Solution: There is a natural bijective correspondence between the $\mathfrak{p}$-primary ideals containing $\mathfrak{q}$ and the $(\mathfrak{p}/\mathfrak{q})$-primary ideals of $R/\mathfrak{q}$, owing to **(18.8)**. In turn, there is one between the latter ideals and the ideals of A primary for its maximal ideal $\mathfrak{m}$, owing to **(18.8)** again and also to **(18.23)** with $M := A$.

However, $\mathfrak{p} = \sqrt{\mathfrak{q}}$ by **(18.5)**. So $\mathfrak{m} = \sqrt{\langle 0\rangle}$. Hence every ideal of A is $\mathfrak{m}$-primary by **(18.10)**. Further, $\mathfrak{m}$ is the only prime of A; so $\ell(A)$ is finite by **(19.4)** with $M := A$. Hence **(19.3)** with $M := A$ yields (1) and (2). □

Exercise **(19.8)**. — Let k be a field, R an algebra-finite extension. Prove that R is Artinian if and only if R is a finite-dimensional k-vector space.

Solution: As k is Noetherian by **(16.1)** and as R/k is algebra-finite, R is Noetherian by **(16.12)**. Assume R is Artinian. Then $\ell(R) < \infty$ by **(19.6)**. 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, as R is. Hence these fields are finite extension fields of k by the Zariski Nullstellensatz. Thus R is a finite-dimensional k-vector space. The converse holds by **(16.28)**. □

Exercise **(19.10)**. — Let k be a field, A a local k-algebra. Assume the map from k to the residue field is bijective. Given an A-module M, prove $\ell(M) = \dim_k(M)$.

Solution: If $M = 0$, then $\ell(M) = 0$ and $\dim_k(M) = 0$. If $M \simeq k$, then $\ell(M) = 1$ and $\dim_k(M) = 1$. Assume $1 \le \ell(M) < \infty$. Then M has a submodule M' with $M/M' \simeq k$. So Additivity of Length, **(19.9)**, 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 $m \ge 1$, there exists a chain of submodules,

$$M = M_0 \supsetneqq M_1 \supsetneqq \cdots \supsetneqq M_m = 0.$$

Hence $\dim_k(M) = \infty$. □

Exercise **(19.12)**. — Prove these conditions on a Noetherian ring R equivalent:

(1) that R is Artinian;
(2) that $\mathrm{Spec}(R)$ is discrete and finite;
(3) that $\mathrm{Spec}(R)$ is discrete.

Solution: Condition (1) holds, by **(19.11)**, if and only if $\mathrm{Spec}(R)$ consists of finitely points and each is a maximal ideal. But a prime $\mathfrak{p}$ is a maximal ideal if and only if $\{\mathfrak{p}\}$ is closed in $\mathrm{Spec}(R)$ by **(13.2)**. It follows that (1) and (2) are equivalent.

Trivially, (2) implies (3). Conversely, (3) implies (2), since $\mathrm{Spec}(R)$ is quasi-compact by **(13.20)**. Thus all three conditions are equivalent. □

Exercise **(19.13)**. — Let R be an Artinian ring. Show that $\mathrm{rad}(R)$ is nilpotent.

Solution: Set $\mathfrak{m} := \mathrm{rad}(R)$. Then $\mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots$ is a descending chain. So $\mathfrak{m}^r = \mathfrak{m}^{r+1}$ for some r. But R is Noetherian by **(19.11)**. So $\mathfrak{m}$ is finitely generated. Thus Nakayama's Lemma **(10.11)** yields $\mathfrak{m}^r = 0$.

Alternatively, R is Noetherian and $\dim R = 0$ by **(19.11)**. So $\mathrm{rad}(R)$ is finitely generated and $\mathrm{rad}(R) = \mathrm{nil}(R)$. Thus **(3.32)** implies $\mathfrak{m}^r = 0$ for some r. □

Exercise **(19.16)**. — 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 **(11.20)**(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 **(19.15)** or by **(16.28)**; hence, R' has only finitely many primes by **(19.11)**. Alternatively, every prime is now minimal by incomparability **(14.3)**(2). Further, R' is Noetherian by **(16.12)**; hence, R' has only finitely many minimal primes by **(17.22)**. □

Exercise **(19.18)**. — Let R be a Noetherian ring, and M a finitely generated module. Prove the following four conditions are equivalent:

(1) that M has finite length;
(2) that M is annihilated by some finite product of maximal ideals $\prod \mathfrak{m}_i$;
(3) that every prime $\mathfrak{p}$ containing $\mathrm{Ann}(M)$ is maximal;
(4) that $R/\mathrm{Ann}(M)$ is Artinian.

Solution: Assume (1). Let $M = M_0 \supset \cdots \supset M_m = 0$ be a composition series; set $\mathfrak{m}_i := \mathrm{Ann}(M_{i-1}/M_i)$. Then $\mathfrak{m}_i$ is maximal by **(19.2)**(2). Also, $\mathfrak{m}_i M_{i-1} \subset M_i$. Hence $\mathfrak{m}_i \cdots \mathfrak{m}_1 M_0 \subset M_i$. Thus (2) holds.

Assume (2). Let $\mathfrak{p}$ be a prime containing $\mathrm{Ann}(M)$. Then $\mathfrak{p} \supset \prod \mathfrak{m}_i$. So $\mathfrak{p} \supset \mathfrak{m}_i$ for some i by **(2.2)**. So $\mathfrak{p} = \mathfrak{m}_i$ as $\mathfrak{m}_i$ is maximal. Thus (3) holds.

Assume (3). Then $\dim(R/\mathrm{Ann}(M)) = 0$. But, by **(16.7)**, any quotient of R is Noetherian. Thus **(19.11)** yields (4).

If (4) holds, then **(19.14)** yields (1), because M is a finitely generated module over $R/\mathrm{Ann}(M)$. □

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 $n \ge 2$. Further, $\ell(\mathfrak{b}_1) = 0$, $\ell(\mathfrak{b}_2) = 2$, and $\ell(\mathfrak{b}_n) = \ell(\mathfrak{m}_n)$ for $n \ge 3$. 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

$$N' := \{\, m \in M \mid \text{there is } k_0 \text{ such that } R_k m \subset N \text{ for all } k \geq k_0 \,\}.$$

(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 containing N.

(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 **(19.11)** and **(16.12)**, R is Noetherian. So N' is finitely generated by **(16.19)**. Let $n_1, \ldots, n_r$ be homogeneous generators of N' with $n_i \in N_{k_i}$; set $k' := \max\{k_i\}$. There is k such that $R_k n_i \subset N$ 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 $R_k n \subset N$ 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 **(18.22)**,

$$\Gamma_{R_+}(M/N) = \bigcap_{\mathfrak{p}_i \not\supset R_+} (Q_i/N).$$

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, **(19.9)**, 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

$$h(R, n) = \tbinom{2+n}{2} - \tbinom{2-d+n}{2} = dn - (d-3)d/2. \qquad \square$$

Exercise **(20.10)**. — Under the conditions of **(20.8)**, assume there is a homogeneous nonzerodivisor $f \in R$ with $M_f = 0$. Prove $\deg h(R, n) > \deg h(M, n)$; 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 **(19.9)** 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 $\deg h(R, n) > \deg h(M, n)$.

In the general case, there is k with $f^k M = 0$ by **(12.7)**. Set $M' := R/\langle f^k \rangle$. Then generators $m_i \in M_{c_i}$ for $1 \leq i \leq r$ yield a surjection $\bigoplus_i M'(-c_i) \twoheadrightarrow M$. Hence $\sum_i \ell(M'_{n-c_i}) \geq \ell(M_n)$ for all n. But $\deg h(M'(-c_i), n) = \deg h(M', n)$.

Hence $\deg h(M', n) \geq \deg h(M, n)$. But $\deg h(R, n) > \deg h(M', n)$ by the first case. Thus $\deg h(R, n) > \deg h(M, n)$. □

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 **(3.32)**. Hence

$$\mathfrak{m}^n M \supset \mathfrak{q}^n M \supset \mathfrak{m}^{mn} M$$

for all $n \geq 0$. Dividing into M and extracting lengths yields

$$\ell(M/\mathfrak{m}^n M) \leq \ell(M/\mathfrak{q}^n M) \leq \ell(M/\mathfrak{m}^{mn} M).$$

Therefore, for large n, we get

$$p_{\mathfrak{m}}(M, n) \leq p_{\mathfrak{q}}(M, n) \leq p_{\mathfrak{m}}(M, nm).$$

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, **(18.29)**, from the Artin–Rees Lemma, **(20.18)**.

Solution: In the notation of **(18.29)**, 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 $\mathfrak{a}(N \cap \mathfrak{a}^m M) = N \cap \mathfrak{a}^{m+1} M$. But $N \cap \mathfrak{a}^n M = N$ for all $n \geq 0$. Thus $N = \mathfrak{a}N$. □

20. Appendix: Homogeneity

Exercise **(20.22)**. — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus_{n \geq n_0} M_n$ a graded module, $\mathfrak{a} \subset \bigoplus_{n>0} R_n$ a homogeneous ideal. Assume $M = \mathfrak{a}M$. Show $M = 0$.

Solution: Suppose $M \neq 0$; say $M_{n_0} \neq 0$. Note $M = \mathfrak{a}M \subset \bigoplus_{n>n_0} M_n$; hence $M_{n_0} = 0$, a contradiction. Thus $M = 0$. □

Exercise **(20.23)**. — Let $R = \bigoplus R_n$ be a Noetherian graded ring, $M = \bigoplus M_n$ a finitely generated graded R-module, $N = \bigoplus N_n$ a homogeneous submodule. Set

$$N' := \{\, m \in M \mid R_n m \in N \text{ for all } n \gg 0 \,\}.$$

Show that N' is the largest homogeneous submodule of M containing N and having, for all $n \gg 0$, its degree-n homogeneous component N'_n equal to N_n.

Solution: Given $m, m' \in N'$, say $R_n m$, $R_n m' \in N$ for $n \gg 0$. Let $x \in R$. Then $R_n(m + m')$, $R_n x m \in N$ for $n \gg 0$. So $N' \subset M$ is a submodule. Trivially $N \subset N'$. Let m_i be a homogeneous component of m. Then $R_n m_i \in N$ for $n \gg 0$ as N is homogeneous. Thus $N' \subset M$ is a homogeneous submodule containing N.

Since R is Noetherian and M is finitely generated, N' is finitely generated, say by $g, g', \ldots, g^{(r)}$. Then there is n_0 with $R_n g, R_n g', \ldots, R_n g^{(r)} \in N$ for $n \geq n_0$. Replace $g, g', \ldots, g^{(r)}$ by their homogeneous components. Say $g, g', \ldots, g^{(r)}$ are now of degrees $d, d', \ldots, d^{(r)}$ with $d \geq d' \geq \cdots \geq d^{(r)}$. Set $n_1 := d + n_0$.

Given $m \in N'_n$ with $n \geq n_1$, say $m = xg + x'g' + \cdots$ with $x \in R_{n-d}$ and $x' \in R_{n-d'}$ and so on. Then $n_0 \leq n - d \leq n - d' \leq \cdots$. Hence $m \in N_n$. Thus

$N'_n \subset N_n$. But $N' \supset N$. Thus $N'_n = N_n$ for $n \geq n_1$, as desired.

Let $N'' = \bigoplus N''_n \subset M$ be homogeneous with $N''_n = N_n$ for $n \geq n_2$. Let $m \in N''$ and $p \geq n_2$. Then $R_p m \in \bigoplus_{n \geq n_2} N''_n \subset N$. So $m \in N'$. Thus $N'' \subset N'$. □

Exercise **(20.25)**. — 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 $x = \sum_{i \geq r}^{r+n} x_i \in R$ 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 **(3.31)**. 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 $0 = xm = \sum x_i m$. If m is homogeneous, then $x_i m = 0$ 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 **(13.28)**. □

Exercise **(20.26)**. — 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 **(20.24)**. □

Exercise **(20.30)**. — 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 $f x_i \in R$ 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 **(12.20)**. So $\deg h(\overline{R}/R, n) < \deg h(\overline{R}, n)$ by **(20.10)** and (1). But

$$h(\overline{R}, n) = h(R, n) + h(\overline{R}/R, n)$$

by **(19.9)** and **(20.8)**. Thus (2) holds. □

21. Dimension

Exercise **(21.6)**. — Let A be a Noetherian local ring, N a finitely generated module, $y_1, \dots, y_r$ a sop for N. Set $N_i := N/\langle y_1, \dots, y_i \rangle N$. Show $\dim(N_i) = r - i$.

Solution: First, $\dim(N) = r$ by **(21.4)**. Then $\dim(N_i) \geq \dim(N_{i-1}) - 1$ for all i by **(21.5)**, and $\dim(N_r) = 0$ by **(19.18)**. So $\dim(N_i) = r - i$ for all i. □

Exercise **(21.9)**. — 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 **(1.9)** and **(2.7)**. So $\operatorname{ht}(\mathfrak{p}') \leq r - r'$ by **(21.8)**.

On the other hand, $R'_{\mathfrak{p}'} = R'_{\mathfrak{p}}$ by **(11.23)**, and $R'_{\mathfrak{p}} = R_{\mathfrak{p}}/\langle x_1/1, \dots, x_{r'}/1 \rangle$ by **(12.22)** Hence $\dim(R'_{\mathfrak{p}'}) \geq \dim(R_{\mathfrak{p}}) - r'$ by repeated application of **(21.5)** with $R_{\mathfrak{p}}$ for both R and M. So $\operatorname{ht}(\mathfrak{p}') \geq r - r'$ by **(21.7.1)**, as required. □

Exercise **(21.11)**. — Let R be a Noetherian ring, $\mathfrak{p}$ a prime of height at least 2. Prove that $\mathfrak{p}$ is the union of height-1 primes, but not of finitely many.

Solution: If $\mathfrak{p}$ were the union of finitely many height-1 primes, then by Prime Avoidance **(3.19)**, one would be equal to $\mathfrak{p}$, a contradiction.

To prove $\mathfrak{p}$ is the union of height-1 primes, we may replace R by $R/\mathfrak{q}$ where $\mathfrak{q} \subset \mathfrak{p}$ is a minimal prime, as preimage commutes with union. Thus we may assume R is a domain. Given a nonzero $x \in \mathfrak{p}$, let $\mathfrak{q}_x \subset \mathfrak{p}$ be a minimal prime of $\langle x \rangle$. Then $\operatorname{ht}(\mathfrak{q}_x) = 1$ by the Krull Principal Theorem **(21.10)**. Plainly $\bigcup \mathfrak{q}_x = \mathfrak{p}$. □

Exercise **(21.12)**. — Let R be a Noetherian ring. Prove the following equivalent:

(1) R has only finitely many primes.
(2) R has only finitely many height-1 primes.
(3) R is semilocal of dimension 1.

Solution: Trivially, (1) implies (2).

Assume (2). By **(21.11)**, there's no prime of height at least 2. Thus $\dim(R) \leq 1$. So every prime is either of height 1 or of height 0. But the height-0 primes are minimal, so finite in number by **(17.22)**. Hence R is semilocal. Thus (3) holds.

Finally, assume (3). Again, every prime is either of height 1 or of height 0, and the the height-0 primes are finite in number. But the height-1 primes are maximal, so finite in number. Thus (1) holds. □

Exercise **(21.13)** (*Artin–Tate* [**1**, Thm. 4]). — Let R be a Noetherian domain, and set $K := \operatorname{Frac}(R)$. Prove the following equivalent:

(1) $K = R_f$ for some nonzero $f \in R$.
(2) K is algebra finite over R.
(3) Some nonzero $f \in R$ lies in every nonzero prime.
(4) R has only finitely many height-1 primes.
(5) R is semilocal of dimension 1.

Solution: By **(11.13)**, (1) implies (2).

Assume (2), and say $K = R[x_1, \dots, x_n]$. Let f be a common denominator of the x_i. Then given any $y \in K$, clearly $f^m y \in R$ for some $m \geq 1$.

Let $\mathfrak{p} \subset R$ be a nonzero prime. Take a nonzero $z \in \mathfrak{p}$. By the above, $f^m(1/z) \in R$ for some $m \geq 1$. So $f^m(1/z)z \in \mathfrak{p}$. So $f \in \mathfrak{p}$. Thus (2) implies (3).

Assume (3). Given $0 \neq y \in R$, the Scheinnullstellensatz **(3.29)** yields $f \in \sqrt{\langle y \rangle}$. So $f^n = xy$ for some $n \geq 1$ and $x \in R$. So $1/y = x/f^n$. Thus (3) implies (1).

Again assume (3). Let $\mathfrak{p}$ be a height-1 prime. Then $f \in \mathfrak{p}$. So $\mathfrak{p}$ is minimal containing $\langle f \rangle$. So $\mathfrak{p}$ is one of finitely many primes by **(17.22)**. Thus (4) holds.

Conversely, assume (4). Take a nonzero element in each height-1 prime, and let f be their product. Then f lies in every height-1 prime. But every nonzero prime contains a height-1 prime owing to the Dimension Theorem **(21.4)**. Thus (3) holds.

Finally, (4) and (5) are equivalent by **(21.12)**. □

Exercise **(21.14)**. — 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. Then $\langle p\rangle$ is a prime ideal as p is a prime element by **(2.6)**. But $\langle p\rangle \subset \mathfrak{p}$ and $\mathrm{ht}(\mathfrak{p}) = 1$. 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 [**2**, Ch. 11, Sec. 2, pp. 392–396]). Let $\mathfrak{p}$ be a prime minimal containing p. By Krull's Principal Ideal Theorem, $\mathrm{ht}(\mathfrak{p}) = 1$. 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 **(21.15)**. — (1) Let A be a Noetherian local ring with a principal prime $\mathfrak{p}$ of height at least 1. Prove A is a domain by showing any prime $\mathfrak{q} \subsetneqq \mathfrak{p}$ is $\langle 0\rangle$.

(2) Let k be a field, $P := k[[X]]$ the formal power series ring in one variable. Set $R := P \times P$. Prove that R is Noetherian and semilocal, and that R contains a principal prime $\mathfrak{p}$ of height 1, but that R is not a domain.

Solution: To prove (1), say $\mathfrak{p} = \langle x\rangle$. Take $y \in \mathfrak{q}$. Then $y = ax$ for some a. But $x \notin \mathfrak{q}$ since $\mathfrak{q} \subsetneqq \mathfrak{p}$. 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 **(10.11)** 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 $a = a_1x$ 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 stabilizes as A is Noetherian: there's a k such that $a_k \in \langle a_{k-1}\rangle$. Then $a_k = ba_{k-1} = ba_kx$ for some b. So $a_k(1-bx) = 0$. But $1 - bx$ is a unit by **(3.6)** as A is local. So $a_k = 0$. Thus $y = 0$, so A is a domain.

As to (2), every nonzero ideal of P is of the form $\langle X^n\rangle$ by **(3.11)**. Hence P is Noetherian. Thus R is Noetherian by **(16.17)**.

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 **(2.11)**. Further, $\mathfrak{m} := \langle X\rangle$ is the unique maximal ideal by **(3.10)**. 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 $\mathrm{ht}(\mathfrak{p}) = 1$.

Finally, R is not a domain as $(1, 0) \cdot (0, 1) = 0$. □

Exercise **(21.16)**. — 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, **(21.9)**, yields $\mathrm{ht}\,\mathfrak{p}_1 = 1$. 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 **(15.9)**. □

Exercise **(21.18)**. — Let R be a Noetherian ring. Show that

$$\dim(R[X]) = \dim(R) + 1.$$

Solution: Let $\mathfrak{P}$ be a prime ideal of $R[X]$, and $\mathfrak{p}$ its contraction in R. Then $R_{\mathfrak{p}} \to R[X]_{\mathfrak{P}}$ is a flat local homomorphism by **(13.47)**. Hence **(21.17)** yields

$$\dim(R[X]_{\mathfrak{P}}) = \dim(R_{\mathfrak{p}}) + \dim\bigl(R[X]_{\mathfrak{P}}/\mathfrak{p}R[X]_{\mathfrak{P}}\bigr). \qquad \textbf{(21.18.1)}$$

Set $k := \mathrm{Frac}(R/\mathfrak{p})$. Then $R[X]_{\mathfrak{P}}/\mathfrak{p}R[X]_{\mathfrak{P}} = k[X]_{\mathfrak{P}}$ owing to **(1.7)** and **(11.27)** and **(11.30)**. But $k[X]$ is a PID, so $\dim(k[X]_{\mathfrak{P}}) \leq 1$. Plainly, $\dim(R_{\mathfrak{p}}) \leq \dim(R)$. So **(21.18.1)** yields $\dim(R[X]_{\mathfrak{P}}) \leq \dim(R) + 1$. Thus $\dim(R[X]) \leq \dim(R) + 1$. Finally, the opposite inequality holds by **(15.19)**. □

Exercise **(21.19)**. — 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 **(10.13)**(2). The assertion follows. □

Exercise **(21.23)**. — 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 $x_1, \ldots, x_r$ generate the maximal ideal $\mathfrak{m}$ of A. So the residues of $x_{s+1}, \ldots, x_r$ generate that $\mathfrak{n}$ of B. Hence $\dim(B) \leq r - s$ by **(21.19)**. 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 $x_{s+1}, \ldots, x_r \in A$. Hence $\mathfrak{m}$ is generated by $x_1, \ldots, x_r$. 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 that the following three conditions are equivalent:

$$(1)\ \kappa\colon M \to \widehat{M} \text{ is injective;} \quad (2)\ \bigcap \mathfrak{a}^n M = \langle 0\rangle; \quad (3)\ M \text{ is separated.}$$

Assume R is Noetherian and M finitely generated. Assume either (a) $\mathfrak{a} \subset \mathrm{rad}(R)$ or (b) R is a domain, $\mathfrak{a}$ is proper, and M is torsionfree. Conclude $M \subset \widehat{M}$.

Solution: A constant ssequence (m) has 0 as a limit if and only if $m \in \mathfrak{a}^n M$ for every n. So $\mathrm{Ker}(\kappa) = \bigcap \mathfrak{a}^n M$. Thus (1) and (2) are equivalent. Moreover, (2) and (3) were proved equivalent in **(22.1)**.

Set $N := \bigcap \mathfrak{a}^n M$. Assume R is Noetherian and M finitely generated. By the Krull Intersection Theorem, **(18.29)** or **(20.19)**, there's $x \in \mathfrak{a}$ with $(1+x)N = \langle 0\rangle$.

Assume (a). Then $1 + x$ is a unit by **(3.2)**. Thus (2) holds and (1) follows.

Finally, assume (b). Then $1 + x \neq 0$ as $\mathfrak{a}$ is proper. Let $m \in M$. If $(1 + x)m = 0$, then $m = 0$ as M is torsionfree. Thus again (2) holds and (1) follows. □

Exercise **(22.6)**. — Let R be a ring. Given R-modules Q_n equipped with linear maps $\alpha_n^{n+1}\colon Q_{n+1} \to Q_n$ for $n \ge 0$, set $\alpha_n^m := \alpha_n^{n+1} \cdots \alpha_{m-1}^m$ for $m > n$. We say the Q_n satisfy the **Mittag-Leffler Condition** if the descending chain

$$Q_n \supset \alpha_n^{n+1} Q_{n+1} \supset \alpha_n^{n+2} Q_{n+2} \supset \cdots \supset \alpha_n^m Q_m \supset \cdots$$

stabilizes; that is, $\alpha_n^m Q_m = \alpha_n^{m+k} Q_{m+k}$ for all $k > 0$.

(1) Assume for each n, there is $m > n$ with $\alpha_n^m = 0$. Show $\varprojlim^1 Q_n = 0$.

(2) Assume α_n^{n+1} is surjective for all n. Show $\varprojlim^1 Q_n = 0$.

(3) Assume the Q_n satisfy the Mittag-Leffler Condition. Set $P_n := \bigcap_{m \ge n} \alpha_n^m Q_m$, which is the stable submodule. Show $\alpha_n^{n+1} P_{n+1} = P_n$.

(4) Assume the Q_n satisfy the Mittag-Leffler Condition. Show $\varprojlim^1 Q_n = 0$.

Solution: For (1), given $(q_n) \in \prod Q_n$, for each $k \ge n$, set $q_k' := \alpha_n^k q_k$ and $p_n := q_n + q_{n+1}' + \cdots + q_m'$. Then $\theta_n p_n = p_n - \alpha_n^{n+1} p_{n+1} = q_n$ as $\alpha_n^{m+k} = 0$ for all $k \ge 0$ owing to the hypothesis. So θ is surjective. Thus (1) holds.

For (2), given $(q_n) \in \prod Q_n$, solve the equations $p_n - \alpha_n^{n+1}(p_{n+1}) = q_n$ recursively, starting with $p_0 = 0$, to get $(p_n) \in \prod Q_n$ with $\theta(p_n) = q_n$. Thus (2) holds.

For (3), there is $m > n+1$ such that $P_n = \alpha_n^m Q_m$ and $P_{n+1} = \alpha_{n+1}^m Q_m$. But $\alpha_n^m Q_m = \alpha_n^{n+1} \alpha_{n+1}^m Q_m$ by definition of α_n^m. Thus (3) holds.

For (4), form the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \to & \prod P_n & \to & \prod Q_n & \to & \prod (Q_n/P_n) & \to & 0 \\
 & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} & & \\
0 & \to & \prod P_n & \to & \prod Q_n & \to & \prod (Q_n/P_n) & \to & 0
\end{array}$$

Apply the Snake Lemma **(5.13)**. It yields the following exact sequence of cokernels:

$$\varprojlim^1 P_n \to \varprojlim^1 Q_n \to \varprojlim^1 (Q_n/P_n).$$

For each n, the restriction $\alpha_n^{n+1}\big|P_n$ is surjective by (3). So $\varprojlim^1 P_n = 0$ by (1). Further, for each n, there is $m > n$ such that $\alpha_n^m Q_m = P_n$. So the induced map $(Q_m/P_m) \to (Q_n/P_n)$ is 0. So $\varprojlim^1 (Q_n/P_n) = 0$ by (1). Thus (4) holds. □

Exercise **(22.10)**. — Let A be a ring, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ be maximal ideals. Set $\mathfrak{m} := \bigcap \mathfrak{m}_i$, and give A the $\mathfrak{m}$-adic topology. Prove that $\widehat{A} = \prod \widehat{A}_{\mathfrak{m}_i}$.

Solution: For each $n > 0$, the $\mathfrak{m}_i^n$ are pairwise comaximal by **(1.14)**(3). Hence $\mathfrak{m}^n = \prod_{i=1}^m \mathfrak{m}_i^n$ by **(1.14)**(4b), and so $A/\mathfrak{m}^n = \prod_{i=1}^n A/\mathfrak{m}_i^n$ by **(1.14)**(4c). But $A/\mathfrak{m}_i^n$ is local with maximal ideal $\mathfrak{m}_i/\mathfrak{m}_i^n$. So $(A/\mathfrak{m}_i^n)_{\mathfrak{m}_i} = A/\mathfrak{m}_i^n$ by **(11.23.1)**. Further, $(A/\mathfrak{m}_i^n)_{\mathfrak{m}_i} = A_{\mathfrak{m}_i}/\mathfrak{m}_i^n A_{\mathfrak{m}_i}$ by **(12.22)**. So $A/\mathfrak{m}^n = \prod_{i=1}^m (A_{\mathfrak{m}_i}/\mathfrak{m}_i^n A_{\mathfrak{m}_i})$. Taking inverse limits, we obtain the assertion by **(22.8)**, because inverse limit commutes with finite product by the construction of the limit. □

Exercise **(22.11)**. — Let R be a ring, M a module, $F^\bullet M$ a filtration, and $N \subset M$ a submodule. Give N and M/N the induced filtrations:

$$F^n N := N \cap F^n M \quad \text{and} \quad F^n(M/N) := F^n M / F^n N.$$

(1) Prove $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = (M/N)\,\widehat{}\,$.

(2) Also assume $N \supset F^n M$ for $n \gg 0$. Prove $\widehat{M}/\widehat{N} = M/N$ and $G^\bullet \widehat{M} = G^\bullet M$.

Solution: For (1), set $P := M/N$. Form the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \to & N/F^{n+1}N & \to & M/F^{n+1}M & \to & P/F^{n+1}P & \to & 0 \\
 & & {\scriptstyle\kappa_n}\downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N/F^n N & \longrightarrow & M/F^n M & \longrightarrow & P/F^n P & \longrightarrow & 0
\end{array}$$

Its rows are exact, and κ_n is surjective. So the induced sequence

$$0 \to \widehat{N} \to \widehat{M} \to \widehat{P} \to 0$$

is exact by **(22.7)** and **(22.8)**. Thus (1) holds.

For (2), notice $F^n P = 0$ for $n \gg 0$. So plainly $P = \widehat{P}$. Thus $\widehat{M}/\widehat{N} = M/N$.

In particular, fix n and take $N := F^n M$. Then $\widehat{M}/F^n\widehat{M} = M/F^n M$. But n is arbitrary. Hence $F^n\widehat{M}/F^{n+1}\widehat{M} = F^n M/F^{n+1} M$. Thus $G^\bullet \widehat{M} = G^\bullet M$. □

Exercise **(22.12)**. — (1) Let R be a ring, $\mathfrak{a}$ an ideal. If $G^\bullet R$ is a domain, show $\widehat{R}$ is an domain. If also $\bigcap_{n \ge 0} \mathfrak{a}^n = 0$, 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 $x' \in G^r \widehat{R}$ and $y' \in G^s \widehat{R}$ denote the images of x and y. Then $x' \ne 0$ and $y' \ne 0$. Now, $G^\bullet \widehat{R} = G^\bullet R$ by **(22.11)**. Assume $G^\bullet R$ is a domain. Then $x'y' \ne 0$. Hence $x'y' \in G^{r+s}\widehat{R}$ is the image of $xy \in \widehat{\mathfrak{a}}^{\,r+s}$. Hence $xy \ne 0$. Thus $\widehat{R}$ is a domain.

If $\bigcap_{n \ge 0} \mathfrak{a}^n = 0$, 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 $\bigcap_{n \ge 0} \mathfrak{m}^n = 0$ by the Krull Intersection Theorem **(18.29)**, and $G^\bullet A$ is a polynomial ring by **(21.22)**, so a domain. Hence A is a domain, by (1). Thus (2) holds. □

Exercise **(22.14)**. — Let A be a Noetherian local ring, $\mathfrak{m}$ the maximal ideal, M a finitely generated module. Prove (1) that $\widehat{A}$ is a Noetherian local ring with $\widehat{\mathfrak{m}}$ as maximal ideal, (2) that $\dim(M) = \dim(\widehat{M})$, and (3) that A is regular if and only if $\widehat{A}$ is regular.

Solution: First, $\widehat{A}$ is Noetherian by **(22.30)**, and it's local with $\widehat{\mathfrak{m}}$ as maximal ideal by **(22.13)**. Thus (1) holds.

Second, $M/\mathfrak{m}^n M = \widehat{M}/\widehat{\mathfrak{m}}^n \widehat{M}$ by **(22.11)** and **(22.22)**. So $d(M) = d(\widehat{M})$ by **(20.13)**. Thus (2) holds by **(21.4)**.

Third, $\mathfrak{m}/\mathfrak{m}^2 = \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2$ by **(22.11)**. Hence $\mathfrak{m}$ and $\widehat{\mathfrak{m}}$ have generating sets with the same number of elements by **(10.16)**. Thus (3) holds. □

Exercise **(22.15)**. — Let A be a ring, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ maximal ideals. Set $\mathfrak{m} := \bigcap \mathfrak{m}_i$ and give A the $\mathfrak{m}$-adic topology. Prove that $\widehat{A}$ is a semilocal ring, that $\widehat{\mathfrak{m}}_1, \ldots, \widehat{\mathfrak{m}}_m$ are all its maximal ideals, and that $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{A})$.

Solution: First, **(22.11)** 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 $\widehat{\mathfrak{m}}_1, \ldots, \widehat{\mathfrak{m}}_m$ are all the maximal ideals of $\widehat{A}$, and so $\widehat{A}$ is semilocal. □

Exercise **(22.18)**. — Let A be a Noetherian semilocal ring. Prove that an element $x \in A$ is a nonzerodivisor on A if and only if its image $\widehat{x} \in \widehat{A}$ is one on $\widehat{A}$.

Solution: Assume x is a nonzerodivisor. Then the multiplication map μ_x is injective on A. So by Exactness of Completion **(22.17)**, 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 by **(22.4)**, as the completion is taken with respect to the Jacobson radical; further, $\widehat{\mu}_x$ induces μ_x. Thus x is a nonzerodivisor. □

Exercise **(22.19)**. — Let $p \in \mathbb{Z}$ be prime. For $n > 0$, define a $\mathbb{Z}$-linear map

$$\alpha_n \colon \mathbb{Z}/\langle p\rangle \to \mathbb{Z}/\langle p^n\rangle \quad \text{by} \quad \alpha_n(1) = p^{n-1}.$$

Set $A := \bigoplus_{n\ge1} \mathbb{Z}/\langle p\rangle$ and $B := \bigoplus_{n\ge1} \mathbb{Z}/\langle p^n\rangle$. Set $\alpha := \bigoplus \alpha_n$; so $\alpha\colon A \to B$.

(1) Show that the p-adic completion $\widehat{A}$ is just A.

(2) Show that, in the topology on A induced by the p-adic topology on B, the completion $\overline{A}$ is equal to $\prod_{n=1}^{\infty} \mathbb{Z}/\langle p\rangle$.

(3) Show that the natural sequence of p-adic completions

$$\widehat{A} \xrightarrow{\widehat{\alpha}} \widehat{B} \xrightarrow{\widehat{\kappa}} (B/A)\widehat{\ }$$

is not exact at $\widehat{B}$. (Thus p-adic completion is *neither* left exact *nor* right exact.)

Solution: For (1), note $pA = 0$. So every Cauchy sequence is constant. Hence $\widehat{A} = A$. Thus (1) holds.

For (2), set $A_k := \alpha^{-1}(p^k B)$. These A_k are the fundamental open neighborhoods of 0 in the topology induced from the p-adic topology of B. So

$$A_k = \alpha^{-1}\big(0 \oplus \cdots \oplus 0 \oplus \textstyle\bigoplus_{n>k} \langle p^k\rangle/\langle p^n\rangle\big) = \big(0 \oplus \cdots \oplus 0 \oplus \textstyle\bigoplus_{n>k} \mathbb{Z}/\langle p\rangle\big).$$

Hence $A/A_k = \bigoplus_{i=1}^{k} \mathbb{Z}/\langle p\rangle = \prod_{n=1}^{k} \mathbb{Z}/\langle p\rangle$. But by **(22.8)**, in the induced topology, the completion $\overline{A}$ is equal to $\varprojlim_{k\ge1} A/A_k$. Thus

$$\overline{A} = \varprojlim_{k\ge1} \textstyle\prod_{n=1}^{k} \mathbb{Z}/\langle p\rangle.$$

Given any sequence of modules $M_1, M_2, \ldots$, let $\pi_k^{k+1}\colon \prod_{n=1}^{k+1} M_n \to \prod_{n=1}^{k} M_n$ be the projections. Then **(22.5)** yields $\varprojlim_{k\ge1} \prod_{n=1}^{k} M_n = \prod_{n=1}^{\infty} M_n$. Thus (2) holds.

For (3), note that, by (2) and **(22.7.1)**, the following sequence is exact:

$$0 \to \overline{A} \to \widehat{B} \xrightarrow{\widehat{\kappa}} (B/A)\widehat{\ }.$$

But $\widehat{A} = A$ by (1), and $A \ne \overline{A}$ as A is countable yet $\overline{A}$ is not. Thus $\operatorname{Im}(\widehat{\alpha}) \ne \operatorname{Ker}(\widehat{\kappa})$; that is, (3) holds. □

Exercise **(22.21)**. — 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 **(22.17)** shows that $M \mapsto \widehat{M}$ preserves surjections. So **(8.19)** yields the desired surjectivity. □

Exercise **(22.24)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Prove that $\widehat{R}$ is faithfully flat if and only if $\mathfrak{a} \subset \operatorname{rad}(R)$.

Solution: First, $\widehat{R}$ is flat over R by **(22.23)**. Next, let $\mathfrak{m}$ be a maximal ideal of R. Then $\widehat{R} \otimes_R (R/\mathfrak{m}) = (R/\mathfrak{m})\widehat{\ }$ by **(22.20)**. But $(R/\mathfrak{m})\widehat{\ } = \varprojlim (R/\mathfrak{m})/\mathfrak{a}^r(R/\mathfrak{m})$ by **(22.8)**. Plainly $(R/\mathfrak{m})/\mathfrak{a}^r(R/\mathfrak{m}) = R/(\mathfrak{a}^r + \mathfrak{m})$. Hence $\widehat{R} \otimes_R (R/\mathfrak{m}) \ne 0$ if and only if $\mathfrak{a} \subset \mathfrak{m}$. Thus, the assertion follows from **(9.4)**. □

Exercise **(22.25)**. — 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 a cyclic R-module by **(10.13)**(2). But $\mathfrak{b}/\mathfrak{a}\mathfrak{b}\widehat{\mathfrak{b}}/(\mathfrak{a}\mathfrak{b})\widehat{\ }$ by **(22.11)**, and $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$ by **(22.22)**(2).

Assume $\mathfrak{b}\widehat{R} = \widehat{R}b$. Then $\widehat{\mathfrak{b}}/(\mathfrak{a}\mathfrak{b})\widehat{\ } = \widehat{R}b'$ where b' is the residue of b. But, given $x \in \widehat{R}$, there's $y \in R$ with $x - \kappa y \in \widehat{\mathfrak{a}}$, as x is the limit of a Cauchy sequence (κy_n) with $y_n \in R$. Then $xb' = yb'$. Thus $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ is also a cyclic R-module, as desired. □

Exercise **(22.28)** (*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 $m_1, \ldots, m_n \in M$ generate assuming their images $m_1', \ldots, m_n'$ in $M/\mathfrak{a}M$ generate.

Solution: Note that $m_1', \ldots, m_n'$ generate $G^\bullet M$ over $G^\bullet R$. Thus $m_1, \ldots, m_n$ generate M over R by the proof of **(22.27)**.

Alternatively, M is finitely generated over R and complete by the statement of **(22.27)**. As M is also separated, $M = \widehat{M}$. Hence M is also an $\widehat{R}$-module. As 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 **(10.13)**(2), the m_i generate M over $\widehat{R}$, so also over R as κ_R is surjective. □

23. Discrete Valuation Rings

Exercise **(23.6)**. — Let R be a ring, M a module, and $x, y \in R$.

(1) Assume that x, y form an M-sequence. Prove that, given any $m, n \in M$ with $xm = yn$, there exists $p \in M$ with $m = yp$ and $n = xp$.

(2) Assume that x, y form an M-sequence and that $y \notin \operatorname{z.div}(M)$. Prove that y, x form an M-sequence too.

(3) Assume that R is local, that x, y lie in its maximal ideal $\mathfrak{m}$, and that M is nonzero and Noetherian. Assume that, given any $m, n \in M$ with $xm = yn$, there exists $p \in M$ with $m = yp$ and $n = xp$. Prove that x, y and y, x form M-sequences.

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 $p \in M$ with $n = xp$. So $x(m - yp) = 0$. But $x \notin \operatorname{z.div}(M)$. Thus $m = yp$.

Consider (2). First, $M/\langle y, x\rangle M \ne 0$ as x, y form an M-sequence. Next, set $M_1 := M/yM$. We must prove $x \notin \operatorname{z.div}(M_1)$. Given $m_1 \in M_1$ with $xm_1 = 0$, lift m_1 to $m \in M$. Then $xm = yn$ for some $n \in M$. By (1), there is $p \in M$ with $m = yp$. Thus $m_1 = 0$, as desired.

Consider (3). The statement is symmetric in x and y. So let's prove x, y form an M-sequence. First, $M/\langle x, y\rangle M \ne 0$ by Nakayama's Lemma.

Next, we must prove $x \notin \operatorname{z.div}(M)$. Given $m \in M$ with $xm = 0$, set $n := 0$.

Then $xm = yn$; so there exists $p \in M$ with $m = yp$ 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 $m = 0$, as desired. Thus $x \notin \mathrm{z.div}(M)$.

Finally, set $M_1 := M/xM$. We must prove $y \notin \mathrm{z.div}(M_1)$. Given $n_1 \in M_1$ with $yn_1 = 0$, lift n_1 to $n \in M$. Then $yn = xm$ for some $m \in M$. So there exists $p \in M$ with $n = xp$. Thus $n_1 = 0$, as desired. Thus x, y form an M-sequence. □

Exercise **(23.8)**. — Let R be a local ring, $\mathfrak{m}$ its maximal ideal, M a Noetherian module, $x_1, \ldots, x_n \in \mathfrak{m}$, and σ a permutation of $1, \ldots, n$. Assume $x_1, \ldots, x_n$ form an M-sequence, and prove $x_{\sigma 1}, \ldots, x_{\sigma n}$ do too; first, say σ transposes i and $i+1$.

Solution: Say σ transposes i and $i+1$. Set $M_j := M/\langle x_1, \ldots, x_j\rangle$. Then x_i, x_{i+1} form an M_{i-1}-sequence; so x_{i+1}, x_i do too owing to **(23.6)**. So

$$x_1, \ldots, x_{i-1}, x_{i+1}, x_i$$

form an M-sequence. But $M/\langle x_1, \ldots, x_{i-1}, x_{i+1}, x_i\rangle M_{i+1}$. Hence $x_{\sigma 1}, \ldots, x_{\sigma n}$ form an M-sequence. In general, σ is a composition of transpositions of successive integers; hence, the general assertion follows. □

Exercise **(23.7)**. — Let A be a Noetherian local ring, M and N nonzero finitely generated modules, $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ a left-exact functor that preserves the finitely generated modules (such as $F(\bullet) := \mathrm{Hom}(M, \bullet)$ by **(16.20)**). Show that, if N has depth at least 2, then so does $F(N)$.

Solution: An N-sequence x, y yields a commutative diagram with exact rows:

$$\begin{array}{ccccc} 0 \to & N & \xrightarrow{\mu_x} & N & \to N/xN \\ & \downarrow{\scriptstyle \mu_y} & & \downarrow{\scriptstyle \mu_y} & \quad\downarrow{\scriptstyle \mu_y} \\ 0 \to & N & \xrightarrow{\mu_x} & N & \to N/xN \end{array}$$

Applying the left-exact functor F yields this commutative diagram with exact rows:

$$\begin{array}{ccccc} 0 \to & F(N) & \xrightarrow{\mu_x} & F(N) & \to F(N/xN) \\ & \downarrow{\scriptstyle \mu_y} & & \downarrow{\scriptstyle \mu_y} & \quad\downarrow{\scriptstyle \mu_y} \\ 0 \to & F(N) & \xrightarrow{\mu_x} & F(N) & \to F(N/xN) \end{array}$$

Thus x is a nonzerodivisor on $F(N)$. Further $F(N)/xF(N) \hookrightarrow F(N/xN)$.

As $N/xN \xrightarrow{\mu_y} N/xN$ is injective and F is left exact, the right-hand vertical map μ_y is injective. So its restriction

$$F(N)/xF(N) \xrightarrow{\mu_y} F(N)/xF(N)$$

is also injective. Thus x, y is an $F(N)$-sequence. □

Exercise **(23.9)**. — 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. Prove that, if A is regular, then A is Cohen–Macaulay.

Solution: Assume A is regular. Given a regular sop $x_1, \ldots, x_r$, 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 **(21.23)**. So $x_1 \neq 0$. But A is a domain by **(21.24)**. So $x_1 \notin \mathrm{z.div}(A)$. Further, if $r \geq 2$, then the residues of $x_2, \ldots, x_r$ form a regular sop of A_1; so we may assume they form an A_1-sequence by induction on r. Thus $x_1, \ldots, x_r$ is an A-sequence.

Conversely, if $\mathfrak{m}$ is generated by an A-sequence $x_1, \ldots, x_n$, then $n \leq \mathrm{depth}(A) \leq r$ by **(23.4)** and **(23.5)**(3), and $n \geq r$ by **(21.19)**. Thus then $n = \mathrm{depth}(A) = r$, and so A is regular and Cohen–Macaulay. □

Exercise **(23.11)**. — 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 **(23.10)**. □

Exercise **(23.12)**. — 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 **(12.22)** 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, **(10.11)**. Therefore, $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional over k; hence, $\mathfrak{m}$ is principal by **(10.13)**(2). Now, since f is irreducible, A is a domain. Hence, A is a DVR by **(23.10)**.

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 **(23.11)**. □

Exercise **(23.13)**. — 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 **(23.3)** implies A is a DVR. □

Exercise **(23.14)**. — 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 $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{q})$.

(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 $0 \le i \le r$, 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 $\operatorname{ht}\mathfrak{p} \le \operatorname{ht}\mathfrak{q}$. 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 $\mathfrak{p}_i \ne \mathfrak{p}_{i+1}$ by Incomparability, **(14.3)**; whence, $\operatorname{ht}\mathfrak{p} \ge \operatorname{ht}\mathfrak{q}$. Hence $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{q}$. Thus (1) holds.

Alternatively, by **(15.14)**, $\operatorname{ht}(\mathfrak{p}) + \dim(P/\mathfrak{p}) = n$ 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 **(15.13)**, $\dim P/\mathfrak{p} = \operatorname{tr.deg}_K \operatorname{Frac}(P/\mathfrak{p})$ 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 **(23.10)**. 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 **(23.16)**. — Let R be a Noetherian domain, M a finitely generated module. Show that M is torsionfree if and only if it satisfies (S_1).

Solution: Assume M satisfies (S_1). By **(23.15)**, the only prime in $\operatorname{Ass}(M)$ is $\langle 0\rangle$. Hence $\operatorname{z.div}(M) = \{0\}$ by **(17.15)**. Thus M is torsionfree.

Conversely, assume M is torsionfree. Suppose $\mathfrak{p} \in \operatorname{Ass}(M)$. Then $\mathfrak{p} = \operatorname{Ann}(m)$ for some $m \in M$. But $\operatorname{Ann}(m) = \langle 0\rangle$ for all $m \in M$. So $\mathfrak{p} = \langle 0\rangle$ is the only associated prime. Thus M satisfies (S_1) by **(23.15)**. □

Exercise **(23.17)**. — 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 any irredundant primary decomposition $\langle 0\rangle = \bigcap \mathfrak{q}_i$. Set $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$. Then $\mathfrak{p}_i \in \operatorname{Ass}(R)$ by **(18.5)** and **(18.20)**. So $\mathfrak{p}_i$ is minimal by (S_1). Hence the localization $R_{\mathfrak{p}_i}$ is a field by (R_0). So $\mathfrak{p}_i R_{\mathfrak{p}_i} = 0$. But $\mathfrak{p}_i R_{\mathfrak{p}_i} \supset \mathfrak{q}_i R_{\mathfrak{p}_i}$. Hence $\mathfrak{p}_i R_{\mathfrak{p}_i} = \mathfrak{q}_i R_{\mathfrak{p}_i}$. Therefore, $\mathfrak{p}_i = \mathfrak{q}_i$ by **(18.23)**. 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 **(13.41)**. 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 **(18.20)**. Thus R satisfies (S_1). □

Exercise **(23.22)**. — 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 **(17.10)**. So $\operatorname{depth}(R_\mathfrak{p}) = 1$ by **(23.5)**(2). But $R_\mathfrak{p}$ is normal by **(11.32)**. Hence $\mathfrak{p}R_\mathfrak{p}$ is principal by **(23.10)**.

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 **(17.18)**. So, by hypothesis, $\mathfrak{p}R_\mathfrak{p}$ is principal. So $R_\mathfrak{p}$ is a DVR by **(23.10)**. 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 $x \ne 0$ by **(23.5)**(2). Then $\langle x/s\rangle = \langle x/1\rangle \subset R_\mathfrak{p}$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ by **(17.10)**. So, by hypothesis, $\mathfrak{p}R_\mathfrak{p}$ is principal. So $\dim(R_\mathfrak{p}) = 1$ by **(23.10)**. Thus R also satisfies (S_2). So R is normal by Serre's Criterion, **(23.20)**. □

Exercise **(23.23)**. — 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 for 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:

$$R \to K \to \textstyle\prod_{\mathfrak{p}\in\Sigma} K_\mathfrak{p}/R_\mathfrak{p}. \tag{23.23.1}$$

Solution: Assume (S_1) holds. Then, given $\mathfrak{p} \in \Phi$, there exists a nonzerodivisor $x \in \mathfrak{p}$ owing to **(17.15)** and **(23.15)**. Clearly, $\mathfrak{p}$ is minimal containing $\langle x\rangle$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ by **(17.18)**. Hence $\operatorname{depth}(R_\mathfrak{p}) = 1$ by **(23.5)**(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 **(23.23.1)**. 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 **(23.5)**(2). Therefore, $a \in bR$ by **(18.26)**. Thus $x \in R$. Thus **(23.23.1)** is exact. □

Exercise **(23.24)**. — 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 **(14.17)**. So **(23.17)** yields (R_0) and (S_1). But $R_\mathfrak{p}$ is normal for any prime $\mathfrak{p}$ by **(14.16)**. Thus (2) holds by **(23.10)**.

Assume (2). Then (R_1) and (S_1) hold trivially. Thus **(23.23)** 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 **(23.17)**. Thus **(14.17)** yields (1). □

23. Appendix: Cohen–Macaulayness

Exercise **(23.25)**. — Let $R \to R'$ be a flat map of Noetherian rings, $\mathfrak{a} \subset R$ an ideal, M a finitely generated R-module, and $x_1, \ldots, x_r$ an M-sequence in $\mathfrak{a}$. Set $M' := M \otimes_R R'$. Assume $M'/\mathfrak{a}M' \ne 0$. Show $x_1, \ldots, x_r$ is an M'-sequence in $\mathfrak{a}R'$.

Solution: For all i, set $M_i := M/\langle x_1, \ldots, x_i\rangle M$ and $M'_i := M'/\langle x_1, \ldots, x_i\rangle M'$. Then $M'_i = M_i \otimes_R R'$ by right exactness of tensor product **(8.13)**. Moreover, by hypothesis, x_{i+1} is a nonzerodivisor on M_i. Thus the multiplication map $\mu_{x_{i+1}}\colon M_i \to M_i$ is injective. Hence $\mu_{x_{i+1}}\colon M'_i \to M'_i$ is injective by flatness. Finally $\langle x_1, \ldots, x_r\rangle \subset \mathfrak{a}$, so $M'_r \ne 0$. Thus the assertion holds. □

EXERCISE **(23.26)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module with $M/\mathfrak{a}M \neq 0$. Let $x_1, \ldots, x_r$ be an M-sequence in $\mathfrak{a}$ and $\mathfrak{p} \in \operatorname{Supp}(M/\mathfrak{a}M)$. Prove the following statements:

(1) $x_1/1, \ldots, x_r/1$ is an $M_\mathfrak{p}$-sequence in $\mathfrak{a}_\mathfrak{p}$, and

(2) $\operatorname{depth}(\mathfrak{a}, M) \le \operatorname{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p})$.

SOLUTION: First, **(13.31)** yields $\mathfrak{p} \in \operatorname{Supp}(M) \cap \mathbf{V}(\mathfrak{a})$. So $M_\mathfrak{p} \neq 0$ and $\mathfrak{p} \in \mathbf{V}(\mathfrak{a})$. Hence $M_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}M_\mathfrak{p} \neq 0$ by Nakayama's Lemma **(10.11)**. But $R_\mathfrak{p}$ is R-flat by **(12.21)**. Thus **(23.25)** yields (1). Hence $r \le \operatorname{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p})$. Thus **(23.4)** yields (2). □

EXERCISE **(23.29)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module with $M/\mathfrak{a}M \neq 0$. Let $x \in \mathfrak{a}$ be a nonzerodivisor on M. Show

$$\operatorname{depth}(\mathfrak{a}, M/xM) = \operatorname{depth}(\mathfrak{a}, M) - 1. \qquad \textbf{(23.29.1)}$$

SOLUTION: There's a finished M/xM-sequence $x_2, \ldots, x_r$ in $\mathfrak{a}$ by **(23.27)**. Then $x, x_2, \ldots, x_r$ is a finished M-sequence in $\mathfrak{a}$. Thus **(23.28)** yields **(23.29.1)**. □

EXERCISE **(23.30)**. — Let A be a Noetherian local ring, M a finitely generated module, $x \notin \operatorname{z.div}(M)$. Show M is Cohen–Macaulay if and only if M/xM is so.

SOLUTION: First **(23.29)** yields $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$. Also **(21.5)** yields $\dim(M/xM) = \dim(M) - 1$. The assertion follows. □

EXERCISE **(23.32)**. — Let A be a Noetherian local ring, and M a nonzero finitely generated module. Prove the following statements:

(1) $\operatorname{depth}(M) = \operatorname{depth}(\widehat{M})$.

(2) M is Cohen–Macaulay if and only if $\widehat{M}$ is Cohen–Macaulay.

SOLUTION: The completion $\widehat{A}$ is faithfully flat by **(22.24)**, and the maximal ideal of A extends to the maximal ideal of $\widehat{A}$ by **(22.14)**(1) and **(22.22)**(2). So **(23.31)** yields (1). Further, $\dim(M) = \dim(\widehat{M})$ by **(22.14)**(2); so (1) implies (2). □

EXERCISE **(23.33)**. — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module with $M/\mathfrak{a}M \neq 0$. Show that there is $\mathfrak{p} \in \operatorname{Supp}(M/\mathfrak{a}M)$ with

$$\operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p}). \qquad \textbf{(23.33.1)}$$

SOLUTION: There exists a finished M-sequence $x_1, \ldots, x_r$ in $\mathfrak{a}$ by **(23.27)**, and **(23.26)**(1) implies $x_1/1, \ldots, x_r/1$ is an $M_\mathfrak{p}$-sequence. Set $M_r := M/\langle x_1, \ldots, x_r\rangle M$. Then $\mathfrak{a} \subset \operatorname{z.div}(M_r)$ by finishedness. So $\mathfrak{a} \subset \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M_r)$ by **(17.26)**. So $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(M_r)_\mathfrak{p}$ by **(17.10)**. So $\mathfrak{p}R_\mathfrak{p} \subset \operatorname{z.div}(M_r)_\mathfrak{p}$. Hence $x_1/1, \ldots, x_r/1$ is finished in $\mathfrak{p}R_\mathfrak{p}$. So **(23.28)** yields **(23.33.1)**. □

EXERCISE **(23.37)**. — Prove that a Cohen–Macaulay local ring A is catenary.

SOLUTION: Take primes $\mathfrak{q} \subsetneqq \mathfrak{p}$ in A. Fix a maximal chain from $\mathfrak{p}$ up to the maximal ideal and a maximal chain from $\mathfrak{q}$ down to a minimal prime. Now, all maximal chains of primes in A have length $\dim(A)$ by **(23.36)**. Hence all maximal chains of primes from $\mathfrak{q}$ to $\mathfrak{p}$ have the same length. Thus A is catenary. □

24. Dedekind Domains

EXERCISE **(24.5)**. — Let R be a domain, S a multiplicative subset.

(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 $\dim(R) \ge 1$. 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 **(11.20)**(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 **(11.20)**(2); so $\dim(S^{-1}R) \ge 1$. 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 **(11.20)**(2). So $r \le 1$ 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 $\mathfrak{p}'_i := \mathfrak{p}_i R_{\mathfrak{p}_r}$. Then $0 = \mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ is a chain of primes by **(11.20)**(2). So if $\dim(R_{\mathfrak{p}_r}) = 1$, then $r \le 1$. Thus, if $\dim(R_\mathfrak{p}) = 1$ for every nonzero $\mathfrak{p}$, then $\dim(R) \le 1$. □

EXERCISE **(24.6)**. — Let R be a Dedekind domain, S a multiplicative subset. 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 **(11.32)**. 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 **(13.37)**, it suffices to establish the two equations after localizing at each maximal ideal $\mathfrak{p}$. But localization commutes with sum and intersection by **(12.17)**(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 replacing R by $R_\mathfrak{p}$, we may assume R is a DVR.

Referring to **(23.1)**, take a uniformizing parameter t. 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:

$$\max\{i, \min\{j,k\}\} = \min\{\max\{i,j\}, \max\{i,k\}\},$$
$$\min\{i, \max\{j,k\}\} = \max\{\min\{i,j\}, \min\{i,k\}\}.$$

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 **(10.11)**, $\mathfrak{p}_1 A_{\mathfrak{p}_1} \neq \mathfrak{p}_1^2 A_{\mathfrak{p}_1}$; 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, **(1.14)**, there is an $x \in A$ with $x \equiv y \bmod \mathfrak{p}_1^2$ and $x \equiv 1 \bmod \mathfrak{p}_i$ for $i \ge 2$.

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 $n_i \ge 0$. But $x \notin \mathfrak{p}_i$ for $i \ge 2$; so $n_i = 0$ for $i \ge 2$. 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 $\mathfrak{a} = \langle \prod x_i^{m_i}\rangle$, 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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ 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 **(11.20)**. 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, **(1.14)**, 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 $\mathfrak{p}_1R', \ldots, \mathfrak{p}_rR'$ 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 **(12.22)**, $R'/\mathfrak{a}R' = S^{-1}(R/\mathfrak{a})$. Finally, $S^{-1}(R/\mathfrak{a}) = R/\mathfrak{a}$ by **(11.6)**, as 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, **(1.14)**, 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. But $R/\mathfrak{p}_i^{n_i} = S^{-1}(R/\mathfrak{p}_i^{n_i})$ by **(11.6)**, as 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 $R_1, \ldots, R_k$, 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 **(1.16)**. Say $\mathfrak{b}_i = \langle a_i\rangle$. Then $\mathfrak{b} = \big\langle (a_1, \ldots, a_k)\big\rangle$. 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:

$$\pi\colon M \otimes N \twoheadrightarrow MN \quad\text{and}\quad \varphi\colon (M : N) \xrightarrow{\sim} \mathrm{Hom}(N, M).$$

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 $M \subset \mathrm{Frac}(R)$.

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 $\theta(y) = yz$. Therefore, $z \in (M : N)$ as $y \in N$ is arbitrary and $\theta(y) \in M$; further, $\theta = \varphi(z)$. 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 **(13.43)**, 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 **(12.14)**, 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 **(8.6)**(2). Thus $\pi_{\mathfrak{m}} \simeq 1_{N_{\mathfrak{m}}}$. □

Exercise **(25.9)**. — Let R be a domain, M and N fractional ideals.

(1) Assume N is invertible, and show that $(M : N) = M \cdot N^{-1}$.

(2) Show that both M and N are invertible if and only if their product MN is, and that if so, then $(MN)^{-1} = N^{-1}M^{-1}$.

Solution: For (1), note that $N^{-1} = (R : N)$ by **(25.8)**. So $M(R : N)N = M$. Thus $M(R : N) \subset (M : N)$. Conversely, note that $(M : N)N \subset M$. Hence $(M : N) = (M : N)N(R : N) \subset M(R : N)$. Thus (1) holds.

In (2), if M and N are invertible, then $(MN)N^{-1}M^{-1} = MM^{-1} = R$; thus MN is invertible, and $N^{-1}M^{-1}$ is its inverse. Conversely, if MN is invertible, then $R = (MN)(MN)^{-1} = M(N(MN)^{-1})$; thus, M is invertible. Similarly, N is invertible. Thus (2) holds. □

Exercise **(25.12)**. — 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

$$d' := \gcd\{n_i m'\} = \gcd\{n_i m a/b\} = a \gcd\{n_i m\}/b = ad/b.$$

So $m' = (a/b)m = (ad/b)x = d'x$. But $d' \in R$. Thus $M = Rx$. □

Exercise **(25.15)**. — 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 **(2.25)**.

Conversely, let R be a Dedekind UFD. Then every nonzero fractional ideal is invertible by **(25.3)** and **(25.14)**, so is principal by **(25.12)**. Thus R is a PID.

Alternatively and more directly, every nonzero prime is of height 1 as $\dim R = 1$, so is principle by **(21.14)**. But, by **(24.10)**, every nonzero ideal is a product of nonzero prime ideals. Thus again, R is a PID. □

Exercise **(25.17)**. — 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 $\beta(m)=\sum a_im_i$. 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 **(25.18)**. — 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 **(25.17)**. 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 **(25.17)**. Thus (2) holds.

Conditions (2) and (3) are equivalent by **(13.52)**.

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 **(13.51)**; so $\operatorname{Hom}_R(M,R)_\mathfrak{m}=\operatorname{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m},R_\mathfrak{m})$ by **(12.25)**.

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 **(13.43)**. 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 of K, and $V\subset W\subset K$ a subring. Prove that W is also a valuation ring of K, that its maximal ideal $\mathfrak{p}$ lies in V, that $V/\mathfrak{p}$ is a valuation ring of the field $W/\mathfrak{p}$, and that $W=V_\mathfrak{p}$.

SOLUTION: First, let $x\in K-W\subset K-V$. Then $1/x\in V\subset W$. Thus W is a valuation ring of K.

Second, let $y\in\mathfrak{p}$. Then **(26.2)** implies $1/y\in K-W\subset K-V$. So $y\in V$.

Third, $x\in W-V$ implies $1/x\in V$; whence, $V/\mathfrak{p}$ is a valuation ring of W/p.

Fourth, $V_\mathfrak{p}\subset W_\mathfrak{p}=W$. Conversely, let $x\in W-V$. Then $1/x\in V$. But $1/x\notin\mathfrak{p}$ as $\mathfrak{p}$ is the maximal ideal of W. So $x\in V_\mathfrak{p}$. Thus $W=V_\mathfrak{p}$. □

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 $x^n+a_1x^{n-1}+\cdots+a_n=0$ with $a_i\in V$. Then

$$1+a_1x^{-1}+\cdots+a_nx^{-n}=0. \qquad \textbf{(26.5.1)}$$

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 **(26.9)**. — Let K be a field, $\mathcal{S}$ the set of local subrings ordered by domination. Show that the valuation rings of K are the maximal elements of $\mathcal{S}$.

SOLUTION: Let V be a valuation ring of K. Then $V\in\mathcal{S}$ 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.

Conversely, let $V\in\mathcal{S}$ be maximal. By **(26.8)**, V is dominated by a valuation ring V' of K. By maximality, $V=V'$. □

EXERCISE **(26.14)**. — 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 **(26.15)**. — 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 $x_i\neq0$ for all i. Let v be the valuation. Suppose $v(x_1)\le v(x_i)$ 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 **(23.10)**. Conversely, assume V is a DVR. Then V is a PID by **(23.1)**, so Noetherian. Thus (2) holds. □

EXERCISE **(26.20)**. — Let R be a Noetherian domain, $K:=\operatorname{Frac}(R)$, and L a finite extension field (possibly $L=K$). Prove the integral closure $\overline{R}$ of R in L is the intersection of all DVRs V of L containing R by modifying the proof of **(26.10)**: show y is contained in a height-1 prime $\mathfrak{p}$ of $R[y]$ and apply **(26.18)** to $R[y]_\mathfrak{p}$.

SOLUTION: Every DVR V is normal by **(23.10)**. So if V is a DVR of L and $V\supset R$, then $V\supset\overline{R}$. Thus $\bigcap_{V\supset R}V\supset\overline{R}$.

To prove the opposite inclusion, take any $x\in K-\overline{R}$. To find a DVR V of L 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 $x\in\overline{R}$, a contradiction.

Thus y is a nonzero nonunit of $R[y]$. Also, $R[y]$ is Noetherian by the Hilbert Basis Theorem **(16.12)**. So y lies in a height-1 prime $\mathfrak{p}$ of $R[y]$ by the Krull Principal

Ideal Theorem **(21.10)**. Then $R[y]_{\mathfrak{p}}$ is Noetherian of dimension 1. But L/K is a finite field extension, so $L/\operatorname{Frac}(R[y])$ is one too. Hence the integral closure R' of $R[y]_{\mathfrak{p}}$ in L is a Dedekind domain by **(26.18)**. So by the Going-up Theorem **(14.3)**, there's a prime $\mathfrak{q}$ of R' lying over $\mathfrak{p}R[y]_{\mathfrak{p}}$. Then as R' is Dedekind, $R'_{\mathfrak{q}}$ is a DVR of L by **(24.7)**. Further, $y \in \mathfrak{q}R'_{\mathfrak{q}}$. Thus $x \notin R'_{\mathfrak{q}}$, as desired. $\square$

Bibliography

[1] Artin, E., and Tate, J. T., "A note on finite ring extensions," J. Math. Soc. Japan, **3.1** (1951), 74–77.
[2] Artin, M., "Algebra," Prentice-Hall, 1991.
[3] Atiyah, M., and Macdonald, I., "Introduction to Commutative Algebra," Addison-Wesley, 1969.
[4] Eisenbud, D., "Commutative Algebra with a View Toward Algebraic Geomertry," Springer-Verlag, 1999.
[5] Grothendieck, A., and Dieudonné, J., "Eléments de Géométrie Algébrique I," Grundlehren **166**, Springer-Verlag, 1971.
[6] Grothendieck, A., and Dieudonné, J., "Eléments de Géométrie Algébrique IV-1," Publ. Math. IHES, Vol. 20, 1964.
[7] Grothendieck, A., and Dieudonné, J., "Eléments de Géométrie Algébrique IV-2," Publ. Math. IHES, Vol. 24, 1965.
[8] Judson, T., "Abstract Algebra: theory and Applications," Open source, Electronic Book,
[9] Lang, S., "Undergraduate Analysis," Springer-Verlag, 1997.
[10] Lang, S., "Algebra" Graduate Texts in Mathematics **211**, Springer-Verlag, 2002.
[11] Reid, M., "Undergraduate Commutative Algebra," Cambridge University Press, 1995.
[12] Stark H., "An Introduction to Number Theory," MIT Press, 1978.

Disposition of the Exercises in [3]

Chapter 1, pp. 10–16

1.— Essentially **(3.2)**, 11, owing to **(3.22)**, 14.
2.— Essentially **(3.36)**, 171
3.— Essentially **(3.37)**, 172
4.— Essentially **(3.38)**, 170
5.— Essentially **(3.39)**, 172
6.— Part of **(3.24)**, 169
7.— Essentially **(2.20)**, 165
8.— Follows easily from **(3.14)**, 167
9.— Essentially **(3.29)**, 14
10.— Essentially **(3.30)**, 170
11.— Essentially **(2.19)**, 165, and **(1.17)**, 164
12.— Essentially **(3.7)**, 11
13.— Standard; see [**10**], Theorem 2.5, p. 231
14.— Follows easily from **(3.15)**, 13, and **(3.16)**, 167
15.— Part of **(13.1)**, 77
16.— Best done by hand
17.— Part of **(13.1)**, 77, and **(13.20)**, 79, and **(13.16)**, 204
18.— Part of **(13.1)**, 77, and **(13.2)**, 201
19.— Essentially **(13.18)**, 205
20.— Essentially **(13.19)**, 205
21.— Part of **(13.1)**, 77, and **(13.13)**, 204, and **(13.12)**, 203
22.— Essentially **(13.3)**, 201, and **(1.13)**, 5
23.— Essentially **(13.24)**, 207, and **(1.17)**(5), 6
24.— About lattices, which we don't treat
25.— Essentially **(13.25)**, 80
26.— Analysis; solution sketched in place
27.— Rudimentary Algebraic Geometry, sketched in place
28.— Rudimentary Algebraic Geometry, sketched in place

Chapter 2, pp. 31–35

1.— Essentially **(8.17)**, 187
2.— Essentially **(8.16)**(1), 51
3.— Essentially **(10.17)**, 193
4.— Part of **(9.6)**, 55
5.— Part of **(9.8)**, 188
6.— Essentially **(8.24)**, 187
7.— Part of **(2.18)**, 165
8.— i) Part of **(9.10)**, 189
ii) Part of **(9.12)**, 189
9.— Part of **(16.16)**, 98
10.— Essentially **(10.14)**, 192
11.— Mostly in **(10.5)**, 61, and **(10.6)**, 191, and **(5.32)**, 30
12.— Immediate from **(5.22)**, 27, and **(5.23)**, 27
13.— Essentially **(8.4)**, 185
14.— Part of **(7.7)**, 43
15.— Part of **(7.8)**, 43
16.— Essentially **(6.6)**, 38
17.— Essentially **(7.2)**, 42, and **(7.3)**, 182
18.— Essentially **(6.6)**, 38
19.— Essentially **(7.14)**, 45
20.— Essentially **(8.13)**, 51
21.— Part of **(7.7)**, 43, and **(7.9)**, 183
22.— Part of **(7.17)**, 184, and **(7.9)**, 183
23.— Essentially **(8.25)**, 187
24.— About Tor, which we don't need
25.— Essentially **(9.16)**(2), 56
26.— Essentially **(9.26)**, 59
27.— Essentially **(10.9)**, 192
28.— Essentially **(10.10)**, 192

Chapter 3, pp. 43–49

1.— Part of **(12.7)**, 199
2.— Essentially **(12.8)**, 199
3.— Essentially **(11.29)**, 198
4.— Part of **(11.23)**, 69
5.— Essentially **(13.41)**, 209
6.— Essentially **(3.18)**, 168
7.— i) Part of **(3.16)**, 167;
rest is **(3.17)**, 168
8.— Essentially **(11.9)**, 195
9.— Essentially **(11.11)**, 196
10.— Essentially **(13.48)**, 210
11.— Essentially **(13.23)**, 206
12.— Essentially **(12.19)**, 200
13.— Essentially **(13.36)**, 208
14.— Essentially **(13.38)**, 209
15.— Essentially **(10.5)**, 61
16.— Essentially **(9.15)**, 189
17.— Essentially **(9.13)**, 189
18.— Essentially **(13.15)**, 204
19.— i) Essentially **(13.35)**, 81;
ii), iii), iv), v) essentially **(13.27)**, 80;
vi) essentially **(13.30)**, 80;
vii) essentially **(13.31)**, 81;
vi) essentially **(13.32)**, 208
20.— Essentially **(13.4)**, 201,
21.— i) Essentially **(13.5)**, 202;
ii) **(13.6)**, 202;
iii) **(13.7)**, 202;
iv) **(13.8)**, 202
22.— Essentially **(13.9)**, 203
23.— Essentially **(13.17)**, 205
24.— Covered in **(13.22)**, 206 and [**5**] (1.3.7), p. 199
25.— Essentially **(13.10)**, 203

26.— Essentially **(13.11)**, 203
27.— Covered in [**5**] (7.2.3), p. 333, and (7.2.12), p. 337 , and (7.2.13), p. 338
28.— See **27**
29.— See **27**
30.— Follows easily from **27**, and **28**, and **29**

Chapter 4, pp. 55–58
1.— To be done
2.— To be done
3.— To be done
4.— To be done
5.— To be done
6.— Analysis, continuing Ex. 26, p. 3 in [**3**]
7.— To be done
8.— To be done
9.— To be done
10.— To be done
11.— To be done
12.— To be done
13.— Part of **(18.27)**, 223
14.— Essentially **(18.20)**, 109
15.— To be done
16.— Covered in **(18.24)**, 109
17.— Technical conditions for primary decomposition; solution sketched in place
18.— Technical conditions for primary decomposition; solution sketched in place
19.— To be done
20.— To be done
21.— Essentially **(18.4)**, 106, and **(18.12)**, 107
22.— Essentially **(18.20)**, 109
23.— Essentially **(17.18)**, 103, and **(17.15)**, 103, and **(18.23)**, 109, and **(18.24)**, 109, and **(18.25)**, 110

Chapter 5, pp. 67–73
1.— To be done
2.— To be done
3.— To be done
4.— To be done
5.— To be done
6.— Part of **(10.31)**, 194
7.— To be done
8.— Part of **(14.7)**, 85
9.— To be done
10.— To be done
11.— Essentially **(14.11)**, 86
12.— To be done
13.— To be done
14.— To be done
15.— To be done
16.— Essentially **(15.1)**, 88
17.— Part of **(15.5)**, 90
18.— Essentially **(15.4)**, 90
19.— Part of **(15.5)**, 90
20.— To be done
21.— To be done
22.— To be done
23.— To be done
24.— Essentially **(15.26)**, 94, and **(15.29)**, 217
25.— To be done
26.— Essentially **(15.23)**, 216, and **(15.24)**, 216
27.— Essentially **(26.9)**, 246
28.— Essentially **(26.3)**, 245, and part of **(26.4)**, 245
29.— Part of **(26.4)**, 245
30.— Part of **(26.11)**, 158
31.— Part of **(26.11)**, 158
32.— To be done
33.— Essentially **(26.12)**, 159
34.— To be done
35.— To be done

Chapter 6, pp. 78–79
1.— Essentially **(10.4)**, 61, and to be done
2.— Part of **(16.13)**, 98
3.— To be done
4.— To be done
5.— To be done
6.— To be done
7.— To be done
8.— To be done
9.— To be done
10.— To be done
11.— To be done
12.— To be done

Chapter 7, pp. 84–88
1.— Essentially **(16.10)**, 97
2.— To be done
3.— To be done
4.— To be done
5.— Essentially **(16.22)**, 99
6.— To be done
7.— Follows easily from **(16.12)**, 98
8.— Essentially **(16.8)**, 218
9.— To be done
10.— To be done
11.— To be done
12.— To be done
13.— To be done
14.— Essentially **(15.8)**, 215
15.— Essentially **(10.20)**, 62, and **(9.26)**, 59
16.— Essentially **(13.51)**, 83
17.— To be done
18.— Essentially **(18.20)**, 109, and **(17.2)**,

101, and **(17.20)**, 103
19.— Follows easily from **(18.20)**, 109
20.— Essentially [**5**] (0,2.3.3), p. 56, and [**5**] (0,2.4.2), pp. 58
21.— Essentially [**5**] (0,2.4.3), p. 59
22.— Essentially [**5**] (0,2.4.6), p. 60
23.— Essentially **EGA**, IV1$_($,1.8.5), p. 239
24.— Essentially **EGA**, IV1$_($,1.10.4), p. 250
25.— Essentially **EGA**, IV2$_($,2.4.6), p. 20
26.— Trivial K-theory
27.— Trivial K-theory

Chapter 8, pp. 91–92
1.— Essentially **(18.27)**, 223, and **(18.28)**, 223
2.— Essentially **(19.12)**, 225
3.— Essentially **(19.8)**, 225
4.— To be done
5.— To be done
6.— Essentially **(19.5)**, 225

Chapter 9, p. 99
1.— To be done
2.— To be done
3.— Part of **(26.15)**, 246
4.— Essentially **(23.3)**, 139
5.— Part of **(25.21)**, 155
6.— To be done
7.— Essentially **(24.13)**, 243
8.— Essentially **(24.8)**, 242
9.— To be done

Chapter 10, pp. 113–115
1.— Essentially **(22.19)**, 235
2.— Essentially **(22.9)**, 133
3.— To be done
4.— To be done
5.— To be done
6.— To be done
7.— Essentially **(22.24)**, 135
8.— To be done
9.— To be done
10.— To be done
11.— To be done
12.— To be done

Chapter 11, pp. 125–126
1.— To be done
2.— To be done
3.— Essentially **(15.13)**, 92
4.— To be done
5.— Trivial K-theory
6.— Essentially **(15.19)**, 215
7.— Essentially **(21.18)**, 231

Index