Commutative Algebra

Timothy J. Ford

DEPARTMENT OF MATHEMATICS, FLORIDA ATLANTIC UNIVERSITY, BOCA RATON, FL 33431

Email address: ford@fau.edu

URL: http://math.fau.edu/ford

Contents

Preface

The purpose of this book is to provide a self-contained introduction to the theory of Commutative Algebra. This book contains more material than a typical one-semester course would cover. For those who intend to use parts of this book as a source for such a course, here is a rough approximation to the logical interdependence of the chapters:

$$
\begin{tikzcd}
 & \text{Chap. 1, 2, 3} \arrow[d] & \\
 & \text{Chap. 4} \arrow[dl] \arrow[dr] & \\
\text{Chap. 5} \arrow[d] & & \text{Chap. 6} \arrow[d] \\
\text{Chap. 8} \arrow[ddr] & & \text{Chap. 7} \arrow[d] \\
 & & \text{Chap. 9} \arrow[dl] \\
 & \text{Chap. 10} \arrow[d] & \\
 & \text{Chap. 11} \arrow[d] & \\
 & \text{Chap. 12} &
\end{tikzcd}
$$

The Chapter 1 establishes most of our conventions, notation and terminology. It contains an outline of the material generally covered in a first course on Abstract Algebra. This includes background material on the subjects of group theory, ring theory, linear algebra, fields, and modules. Proofs are frequently omitted. Chapter 2 contains a deeper study of modules. Generally, the ground ring is not assumed to be commutative. Chapter 3 emphasizes modules over commutative rings. Chapters 4 and 5 provide a deeper study of ring theory. Chapter 4 begins with a basic introduction to artinian and noetherian rings and modules. The Jacobson radical is defined and the fundamental properties of semisimple rings are studied. This leads into the proof of the Wedderburn-Artin Theorem on the structure of a simple ring. The proof we give is an application of Morita Theory. Chapters 1, 2, 3 and 4 are fundamental. All of the subsequent chapters depend on these four.

Chapter 5 is an introduction to separable algebras. The results from this chapter are used in Chapters 8, 10, 11 and 12. Chapters 6, 7 and 9 are mostly about commutative algebra. These three chapters do not depend on Chapters 5 or 8.

Chapter 8 is a self-contained introduction to homological algebra. First we derive the fundamental properties of the left derived and right derived groups of a covariant or contravariant additive functor from the category of modules to the category of abelian groups. This includes an introduction to the Tor and Ext groups. The projective dimension and injective dimension of a module are defined and applied to define the cohomological dimension of a commutative ring. There is an entire section on group cohomology. The Amitsur complex of a faithfully flat extension of commutative rings is defined and applied to the theory of faithfully flat descent. Hochschild cohomology groups are defined. Amitsur cohomology groups are defined and the connection with twisted forms is studied. This chapter does not depend on Chapters 6, 7 or 9.

Chapters 10, 11 and 12 are mostly about commutative algebra. These three chapters depend on all of the previous chapters.

The material contained in this book has been assembled from various sources. Rather than placing a citation on each individual definition, example, or theorem, each section begins with a short list of the main sources of general reference for that particular section.

CHAPTER 1

Preliminaries and Prerequisites

This chapter contains material of a background nature that many readers will already be familiar with. Most of our notation and conventions are established here. Proofs are frequently omitted. Most of the material appearing in this chapter will have significant applications in the chapters that follow. Such results are listed here to simplify the process of making citations and references in the presentation that follows. To avoid listing many special cases, a theorem is frequently stated in a form that is more general than any given application may require. For all other unexplained notation and terminology, the reader is referred to [**19**].

1. Rings and Modules

1.1. Groups. This book is devoted mostly to the subjects of rings and modules. We list in this short section a few necessary references to groups. A *group* is a nonempty set G together with an associative binary operation such that an identity element exists in G, and every element of G is invertible. A commutative group is called an *abelian group*.

A subgroup of a group G is a subset H that is itself a group under the binary operation on G. Associated to a subgroup H is an equivalence relation on G called left congruence modulo H. Specifically, if the group operation is written multiplicatively, two elements x and y of G are left congruent modulo H if there is an element z in H such that $y = xz$. The equivalence class of x is the set $xH = \{xz \mid z \in H\}$, which is called the left coset of x modulo H. The set of all left cosets of H in G is denoted G/H and there is a natural map $\eta : G \to G/H$. All left cosets of H have the same cardinality. The number of left cosets of H in G is called the *index of H in G* and is denoted $[G : H]$.

THEOREM 1.1.1. *(Lagrange's Theorem) If G is a group and $K \subseteq H \subseteq G$ is a chain of subgroups, then $[G : K] = [G : H][H : K]$. If two of the three indices are finite, then so is the third.*

1.2. Rings. A *ring* is a nonempty set R with two binary operations, addition written $+$, and multiplication written $\cdot$ or by juxtaposition. Under addition $(R,+)$ is an abelian group with identity element 0. Under multiplication $(R,\cdot)$ is associative and contains an identity element, denoted by 1. Multiplication distributes over addition from both the left and the right. If $(R,\cdot)$ is commutative, then we say R is a *commutative ring*. The *trivial ring* is $\{0\}$, in which $0 = 1$. Otherwise $0 \neq 1$. We say $a \in R$ is a *left zero divisor* if $a \neq 0$ and there exists $b \neq 0$ such that $ab = 0$. We say a is *left invertible* in case there is $b \in R$ such that $ba = 1$. The reader should define the terms *right zero divisor* and *right invertible*. If a is both a left zero divisor and right zero divisor, then we say a is a *zero divisor*. If a is both left invertible and right invertible, then we say a is *invertible*. In this case, the left inverse and right inverse of a are equal and unique. An invertible element in a ring R is also called a *unit* of R. If $R \neq \{0\}$ and R has no zero divisors, then we say R is a *domain*. A commutative domain is called an *integral domain*. A domain in which every nonzero element is invertible is called a *division ring*. A commutative division ring is called a *field*. The set of all invertible elements in a ring R is a group which is denoted $\operatorname{Units}(R)$ or R^* and is called *the group of units in* R. If A is a subset of R, then we say A is a *subring* of R if A contains both 0 and 1 and A is a ring under the addition and multiplication rules of R. The *center* of R is the set $Z(R) = \{x \in R \mid xy = yx\,(\forall y \in R)\}$. The center of R is a commutative ring and a subring of R. If $x \in Z(R)$, then we say x is *central*.

Let R be a ring. A *left ideal* of R is a nonempty subset $I \subseteq R$ such that $(I,+)$ is a subgroup of $(R,+)$ and $ax \in I$ for all $a \in R$ and all $x \in I$. The reader should define the term *right ideal*. If I is both a left ideal and right ideal, we say I is an *ideal*. If S is a ring, a *homomorphism* from R to S is a function $f\colon R \to S$ satisfying

(1) $f(x+y) = f(x)+f(y)$ for all $x,y \in R$,
(2) $f(xy) = f(x)f(y)$ for all $x,y \in R$, and
(3) $f(1) = 1$.

The *kernel* of f is $\ker(f) = \{x \in R \mid f(x) = 0\}$, which is an ideal in R. The *image* of f is $\operatorname{im}(f) = \{f(x) \in S \mid x \in R\}$, which is a subring of S.

PROPOSITION 1.1.2. *If I is a left ideal in R, then I is both a left and right ideal if and only if the set $R/I = \{a+I \mid a \in R\}$ of all left cosets of I in R is a ring where addition and multiplication of cosets is defined by the rules*

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)(b+I) = ab+I.$$

The additive identity is the coset $0+I$, the multiplicative identity is $1+I$. The natural map $R \to R/I$ is a homomorphism of rings. The ring R/I is called the residue class ring*, or* factor ring*, or* quotient ring *of R modulo I.*

THEOREM 1.1.3. *Let $\theta\colon R \to S$ be a homomorphism of rings.*

(1) If I is an ideal of R contained in $\ker\theta$ and $\eta : R \to R/I$ is the natural map, then there exists a unique homomorphism $\varphi\colon R/I \to S$ such that the diagram

$$\begin{tikzcd} R \arrow[rr, "\theta"] \arrow[dr, "\eta"'] & & S \\ & R/I \arrow[ur, "\varphi"'] & \end{tikzcd}$$

commutes. That is, $\varphi(x+I) = \theta(x)$.

(2) There is a unique monomorphism of rings $\bar\theta : R/\ker\theta \to S$ such that $\theta = \bar\theta\eta$. The homomorphism θ factors into an epimorphism η followed by a monomorphism $\bar\theta$. There is an isomorphism of rings $\varphi : R/\ker\theta \to \operatorname{im}\theta$.

(3) If $I \subseteq J \subseteq R$ is a chain of ideals in R, then J/I is an ideal in R/I and the natural map

$$\frac{R/I}{J/I} \to R/J$$

sending the coset containing $x+I$ to the coset $x+J$ is an isomorphism of rings.

EXAMPLE 1.1.4. Let R be a commutative ring and G a group with identity element denoted e. The *group ring* is the set of all finite formal sums

$$R(G) = \left\{ \sum_{\sigma\in G} r_\sigma\sigma \mid r_\sigma \in R \text{ and } r_\sigma = 0 \text{ for all but finitely many } \sigma \right\}$$

with addition and multiplication rules defined by

$$\sum_{\sigma\in G} r_\sigma\sigma + \sum_{\sigma\in G} s_\sigma\sigma = \sum_{\sigma\in G}(r_\sigma + s_\sigma)\sigma$$

$$\left(\sum_{\sigma\in G} r_\sigma\sigma\right)\left(\sum_{\tau\in G} s_\tau\tau\right) = \sum_{\sigma\in G}\sum_{\tau\in G}(r_\sigma s_\tau)(\sigma\tau).$$

The additive identity is $0 = \sum_{\sigma\in G} 0\sigma$, the multiplicative identity is $1 = 1e$. Suppose H is a group and $\theta\colon H \to G$ is a homomorphism of groups. The action $rh \mapsto r\theta(h)$ induces a homomorphism of group rings $R(H) \to R(G)$.

(1) The homomorphism $\langle e\rangle \to G$ induces a homomorphism $\theta : R \to R(G)$. Notice that θ is one-to-one and the image of θ is contained in the center of $R(G)$.
(2) The homomorphism $G \to \langle e\rangle$ induces $\varepsilon : R(G) \to R$. Notice that ε is onto, and the kernel of ε contains the set of elements $D = \{1-\sigma \mid \sigma \in G\}$. The kernel of ε is the ideal generated by D in $R(G)$. Sometimes ε is called the *augmentation map*.

EXAMPLE 1.1.5. If $R_1,\dots,R_n$ are rings, then the direct product $R_1\times\cdots\times R_n$ is a ring, with coordinate-wise addition and multiplication. That is, if $x = (x_1,\dots,x_n)$ and $y = (y_1,\dots,y_n)$, then $x+y = (x_1+y_1,\dots,x_n+y_n)$ and $xy = (x_1y_1,\dots,x_ny_n)$. The additive identity is $0 = (0,\dots,0)$ and the multiplicative identity is $1 = (1,\dots,1)$. The projection map $\pi_k : R_1\times\cdots\times R_n \to R_k$ onto coordinate k, defined by $\pi_k(x_1,\dots,x_n) = x_k$, is an onto homomorphism of rings. The canonical injection map $\iota_k : R_k \to R_1\times\cdots\times R_n$ maps $x \in R_k$ to the n-tuple which is x in coordinate k and 0 elsewhere. Then ι_k is additive and multiplicative. If $n \geq 2$, then $\iota_k(1) \neq 1$, hence ι_k is not a homomorphism of rings.

EXAMPLE 1.1.6. Standard examples of homomorphisms are listed here.

(1) If u is an invertible element of R, the *inner automorphism* of R defined by u is $\sigma_u\colon R \to R$ where $\sigma_u(x) = uxu^{-1}$.
(2) If R is a ring, then the zero mapping $R \to (0)$ is a homomorphism of rings. In the category of rings, (0) is a terminal object.
(3) If R is a ring, there is a unique homomorphism $\chi\colon \mathbb{Z} \to R$. In fact, by definition $\chi(1) = 1$ so $\chi(n) = n\chi(1) = n1$ for an arbitrary integer n. In the category of rings, $\mathbb{Z}$ is an initial object. The image of χ is the smallest subring of R. The kernel of χ is a subgroup of $\mathbb{Z}$, hence is equal to (n) for some nonnegative integer n. We call n the *characteristic* of R and write $n = \operatorname{char}(R)$.

If R is a ring and $X \subseteq R$, then the *left ideal generated by* X, denoted (X), is the intersection of the left ideals of R that contain X. If A and B are left ideals of R, then $A+B$ is a left ideal. The left ideal generated by the set $\{ab \mid a\in A, b\in B\}$ is denoted AB. If R is a ring and I and J are ideals in R, then we say I and J are *comaximal* if $I+J = R$.

THEOREM 1.1.7. *Let R be any ring. If $I_1,\dots,I_n$ are ideals in R and*

$$\phi : R \to R/I_1 \times R/I_2 \times\cdots\times R/I_n$$

is the natural map given by $x \mapsto (x+I_1,\dots,x+I_n)$, then the following are true.

(1) ϕ is a homomorphism of rings.
(2) The kernel of ϕ is equal to $I_1\cap I_2\cap\cdots\cap I_n$.
(3) ϕ is onto if and only if $n = 1$ or the ideals are pairwise comaximal.

Let $\{I_1,\dots,I_n\}$ be a set of ideals in a ring R. For $n \geq 2$, $I_1+I_2+\cdots+I_n$ is defined recursively to be $(I_1+\cdots+I_{n-1})+I_n$ and is called the *sum* of the ideals. The sum of the ideals is equal to the ideal of R generated by the set $I_1\cup I_2\cup\cdots\cup I_n$. We say that R is the *internal direct sum* of the ideals in case

(1) $R = I_1 + I_2 + \cdots + I_n$, and
(2) for each $x \in R$, x has a unique representation as a sum $x = x_1 + x_2 + \cdots + x_n$ where $x_i \in I_i$.

We denote the internal direct sum by $R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$.

Let R be a ring. An *idempotent* of R is an element $e \in R$ that satisfies the equation $e^2 = e$. The elements 0 and 1 are called the trivial idempotents. A set $\{e_i \mid i \in I\}$ of idempotents in R is said to be *orthogonal* if $e_i e_j = 0$ for all $i \neq j$.

In the direct product $R_1 \times \cdots \times R_n$, let e_k be the image of $\iota_k(1)$. Then e_k is the n-tuple with 1 in coordinate k and 0 elsewhere. The set $\{e_1, \ldots, e_n\}$ is a set of orthogonal idempotents contained in the center of $R_1 \times \cdots \times R_n$.

THEOREM 1.1.8. *If $A_1, \ldots, A_n$ are ideals in the ring R and $R = A_1 \oplus \cdots \oplus A_n$, then the following are true.*

(1) For each k, $A_k \cap \left(\sum_{j \neq k} A_j\right) = (0)$.
(2) If $x \in A_i$, $y \in A_j$ and $i \neq j$, then $xy = yx = 0$.
(3) For each i, A_i is a ring. If the identity element of A_i is denoted e_i, then $\{e_1, \ldots, e_n\}$ is a set of orthogonal idempotents in R. Moreover, each e_i is in the center of R and $A_i = Re_i$ is a principal ideal in R.
(4) R is isomorphic to the (external) direct product $A_1 \times \cdots \times A_n$.
(5) Suppose for each k that I_k is a left ideal in the ring A_k. Then $I = I_1 + I_2 + \cdots + I_n$ is a left ideal in R, where the sum is a direct sum.
(6) If I is a left ideal of R, then $I = I_1 \oplus I_2 \oplus \cdots \oplus I_n$ where each I_k is a left ideal in the ring A_k.

PROPOSITION 1.1.9. *Suppose $A_1, \ldots, A_n$ are ideals in the ring R satisfying*

(1) $R = A_1 + A_2 + \cdots + A_n$ and
(2) for $k = 1, \ldots, n-1$, we have $A_k \cap (A_{k+1} + \cdots + A_n) = (0)$.

Then $R = A_1 \oplus A_2 \oplus \cdots \oplus A_n$.

1.3. Modules and Algebras. If R is a ring, an *R-module* is an abelian group M written additively together with a left multiplication action by R such that for all $r, s \in R$ and $x, y \in M$ the rules

(1) $r(x+y) = rx + ry$
(2) $r(sx) = (rs)x$
(3) $(r+s)x = rx + sx$
(4) $1x = x$

are satisfied. If R is a division ring, then M is called a *vector space*. By default, an R-module is assumed to be a left R-module. There will be times when for sake of convenience we will utilize right R-modules. The statement of the definition for a right R-module is left to the reader. If M is an abelian group, then the set of all endomorphisms of M, $\operatorname{Hom}(M, M)$, is a ring. Endomorphisms are added point-wise and multiplication is composition of functions.

LEMMA 1.1.10. *Let R be a ring.*

(1) If M is an R-module, then there is a homomorphism of rings $\lambda : R \to \operatorname{Hom}(M, M)$ defined by $\lambda(r) = \lambda_r$, where $\lambda_r : M \to M$ is the "left multiplication by r" function defined by $\lambda_r(x) = rx$.
(2) If M is an abelian group and $\lambda : R \to \operatorname{Hom}(M, M)$ is a homomorphism of rings, then the product $r * x = \lambda(r)(x)$ makes M into an R-module.

In Lemma 1.1.10, the kernel of $\lambda : R \to \operatorname{Hom}(M,M)$ is denoted $\operatorname{annih}_R(M)$ and is called the *annihilator of M in R*. Then $\operatorname{annih}_R(M)$ is equal to $\{r \in R \mid rx = 0 \text{ for all } x \in M\}$. Since λ is a homomorphism of rings, $\operatorname{annih}_R(M)$ is a two-sided ideal in R. If λ is one-to-one, then we say M is a *faithful R-module*.

EXAMPLE 1.1.11. Standard examples of modules are listed here.

(1) Let M be any additive abelian group. By Example 1.1.6 (3), there is a unique homomorphism of rings $\chi : \mathbb{Z} \to \operatorname{Hom}(M,M)$. Therefore, M is a $\mathbb{Z}$-module in a unique way.
(2) If R is a ring and I is a left ideal in R, then I is an R-module, by the usual addition and multiplication in R. As a special case, taking $I = R$ implies R is a left R-module.
(3) Let $\phi : R \to S$ be a homomorphism of rings. If M is an S-module with associated homomorphism $\theta : S \to \operatorname{Hom}(M,M)$, then M is an R-module by the composition homomorphism $\theta\phi : R \to \operatorname{Hom}(M,M)$.
(4) Let M be an R-module with associated homomorphism $\theta : R \to \operatorname{Hom}(M,M)$. If I is a two-sided ideal of R contained in $\operatorname{annih}_R(M)$, then θ factors through R/I. The homomorphism $R/I \to \operatorname{Hom}(M,M)$ makes M into an R/I-module. See Exercise 1.1.1 for a continuation of this example.

If R is a commutative ring, then an *R-algebra* is a ring A together with a homomorphism of rings $\theta : R \to Z(A)$ mapping R into the center of A. We call θ the *structure homomorphism* of A. We write $R \cdot 1$ for the image of θ. If B is a subring of A containing $R \cdot 1$, then we say B is an *R-subalgebra* of A. We say A is a *finitely generated* R-algebra in case there exists a finite subset $X = \{x_1, \dots, x_n\}$ of A and A is the smallest subalgebra of A containing X and $R \cdot 1$. In the milieu of R-algebras, the definitions for the terms *center*, *left ideal*, *ideal* are the same as for rings.

A homomorphism from the R-algebra A to the R-algebra B is a homomorphism of rings $\theta : A \to B$ such that for each $r \in R$ and $x \in A$, $\theta(rx) = r\theta(x)$. An *R-algebra automorphism* of A is a homomorphism from A to A that is one-to-one and onto. The set of all R-algebra automorphisms is a group and is denoted $\operatorname{Aut}_R(A)$.

If M is an R-module, then a *submodule* of M is a nonempty subset $N \subseteq M$ such that N is an R-module under the operation by R on M. If $X \subseteq M$, the *submodule of M generated by X* is the intersection of the submodules of M containing X. A submodule is *principal*, or *cyclic*, if it is generated by a single element. The submodule generated by X is denoted (X). If $X = \{x_1, x_2, \dots, x_n\}$ is finite, we sometimes write $(X) = Rx_1 + Rx_2 + \cdots + Rx_n$. We say M is *finitely generated* if there exists a finite set $X = \{x_1, x_2, \dots, x_n\} \subseteq M$ such that $M = (X)$. If I is a left ideal of R, the submodule of M generated by the set $\{rx \mid r \in I, x \in M\}$ is denoted IM.

If M and N are R-modules, a *homomorphism* from M to N is a function $f : M \to N$ satisfying

(1) $f(x+y) = f(x) + f(y)$ and
(2) $f(rx) = rf(x)$

for all $x, y \in M$ and $r \in R$. Since f is a homomorphism of abelian groups $f : (M,+) \to (N,+)$, the *kernel* of f is $\ker(f) = \{x \in M \mid f(x) = 0\}$ and the *image* is $\operatorname{im}(f) = \{f(x) \in N \mid x \in M\}$. The *cokernel* of f is the quotient module $N/\operatorname{im}(f)$. The set of all R-module homomorphisms from M to N is denoted $\operatorname{Hom}_R(M,N)$. An *epimorphism* is a homomorphism that is onto. A *monomorphism* is a homomorphism that is one-to-one. An *isomorphism* is a homomorphism $f : M \to N$ that is one-to-one and onto. In this case we say M and

N are *isomorphic*. An *endomorphism* of M is a homomorphism from M to M. The ring $\operatorname{Hom}_R(M,M)$ is called the *ring of endomorphisms* of M.

If M is an R-module, then M is said to be *simple* if $M \neq (0)$ and the only submodules of M are (0) and M. If A is a submodule of M, then we say A is a *maximal submodule of* M in case A is a maximal member of the set $\{S \subseteq M \mid S \text{ is a submodule of } M \text{ and } S \neq M\}$, ordered by set inclusion.

THEOREM 1.1.12. *Let $\theta : M \to N$ be a homomorphism of R-modules.*

(1) If S is a submodule of M contained in $\ker\theta$ and $\eta : M \to M/S$ is the natural map, then there exists a unique homomorphism $\varphi : M/S \to N$ such that the diagram

$$\begin{tikzcd} M \arrow[rr, "\theta"] \arrow[dr, "\eta"'] & & N \\ & M/S \arrow[ur, "\varphi"'] & \end{tikzcd}$$

commutes. The natural map $\varphi : M/\ker\theta \to \operatorname{im}\theta$ defined by sending the coset $x+\ker\theta$ to $\theta(x)$ is an isomorphism of modules.

(2) If A and B are submodules of M, then the natural map

$$\frac{A}{A\cap B} \to \frac{A+B}{B}$$

defined by sending the coset $x+A\cap B$ to the coset $x+B$ is an isomorphism. If $A \subseteq B$, then the natural map

$$\frac{M/A}{B/A} \to M/B$$

defined by sending the coset containing $x+A$ to the coset $x+B$ is an isomorphism.

(3) If A is a submodule of M, then there is a one-to-one order-preserving correspondence between the submodules B such that $A \subseteq B \subseteq M$ and the submodules of M/A given by $B \mapsto B/A$. The submodule A is maximal if and only if M/A is a simple R-module.

EXAMPLE 1.1.13. Let R be a commutative ring and A an R-algebra. Let M be a left A-module. By virtue of the structure homomorphism $\theta : R \to A$, we view M as a left R-module. Then A acts on M as a ring of R-module endomorphisms. That is, if $a \in A$, $r \in R$, and $x \in M$, then $\lambda_a(rx) = arx = rax = r\lambda_a(x)$. The mapping $a \mapsto \lambda_a$ defines an R-algebra homomorphism $\lambda_A : A \to \operatorname{Hom}_R(M,M)$ which is called the *left regular representation* of A in $\operatorname{Hom}_R(M,M)$. In the special case where $M = A$, the map $\lambda_A : A \to \operatorname{Hom}_R(A,A)$ is one-to-one, because $\lambda_\alpha(1) = \alpha$.

EXAMPLE 1.1.14. Let R be a commutative ring, A an R-algebra, and M a left A-module. By Exercise 1.1.4, there are two monomorphisms of rings

$$\operatorname{Hom}_A(M,M) \xrightarrow{H_\theta} \operatorname{Hom}_R(M,M) \xrightarrow{H_\chi} \operatorname{Hom}_{\mathbb{Z}}(M,M)$$

where H_θ is induced by θ and H_χ is induced by the natural map $\chi : \mathbb{Z} \to R$. By Lemma 1.1.10, the homomorphism H_χ makes M into a module over the ring $\operatorname{Hom}_R(M,M)$. The composite homomorphism $H_\chi H_\theta$ makes M into a module over the ring $\operatorname{Hom}_A(M,M)$.

DEFINITION 1.1.15. Let R be a ring and $\{M_i \mid i = 1,2,\dots\}$ a sequence of R-modules. Suppose we have a sequence of R-module homomorphisms

$$M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \xrightarrow{\phi_3} \cdots. \tag{1.1}$$

Then (1.1) is a *complex* if for all $i \geq 1$, $\phi_{i+1}\phi_i = 0$, or equivalently, if $\operatorname{im}\phi_i \subseteq \ker\phi_{i+1}$. We say (1.1) is an *exact sequence* if for all $i \geq 1$, $\operatorname{im}\phi_i = \ker\phi_{i+1}$. A *short exact sequence* is an exact sequence with exactly five modules and four maps

$$0 \to M_2 \xrightarrow{\phi_2} M_3 \xrightarrow{\phi_3} M_4 \to 0 \tag{1.2}$$

where $M_1 = 0 = M_5$ and $\phi_1 = 0 = \phi_4$. The short exact sequence (1.2) is *split exact* if there exists an R-module homomorphism $\psi_3 : M_4 \to M_3$ such that $\phi_3\psi_3 = 1$. By Exercise 1.6.4, (1.2) is split exact if and only if there exists an R-module homomorphism $\psi_2 : M_3 \to M_2$ such that $\psi_2\phi_2 = 1$.

EXAMPLE 1.1.16. Let R be a ring and $f : M \to N$ a homomorphism of R-modules. There is an exact sequence

$$0 \to \ker(f) \to M \xrightarrow{f} N \to \operatorname{coker}(f) \to 0$$

of R-modules.

1.4. Exercises.

EXERCISE 1.1.1. Let R be a ring, I a two-sided ideal of R, and M a left R-module. Prove:

(1) If I is contained in $\operatorname{annih}_R(M)$, then M is an R/I-module under the multiplication rule $(r+I)x = rx$.
(2) M/IM is an R/I-module under the action $(r+I)(x+IM) = rx+IM$.
(3) An R-submodule of M/IM is an R/I-submodule, and conversely.

EXERCISE 1.1.2. Let R be any ring and I a left ideal of R. Prove:

(1) $\operatorname{annih}_R(R/I)$ is a two-sided ideal of R.
(2) $\operatorname{annih}_R(R/I) \subseteq I$.
(3) I is a two-sided ideal of R if and only if $\operatorname{annih}_R(R/I) = I$.

EXERCISE 1.1.3. Let R be a ring and M a left R-module. If I and J are submodules of M, then the *module quotient* is $I : J = \{r \in R \mid rJ \subseteq I\}$. Prove:

(1) $I : J$ is a two-sided ideal in R.
(2) $I : J = \operatorname{annih}_R((I+J)/I) = \operatorname{annih}_R(J/(I\cap J))$.

EXERCISE 1.1.4. Let $\theta : R \to S$ be a homomorphism of rings. Let M and N be S-modules. Via θ, M and N can be viewed as R-modules (see Example 1.1.11 (3)). Show that θ induces a well defined $\mathbb{Z}$-module monomorphism $H_\theta : \operatorname{Hom}_S(M,N) \to \operatorname{Hom}_R(M,N)$. (Note: The dual result, how the tensor group behaves when the ring in the middle is changed, is studied in Exercise 2.3.16.)

EXERCISE 1.1.5. Let $\theta : R \to S$ be a homomorphism of commutative rings. If M is an S-module, show that there is a commutative diagram of ring homomorphisms

$$\begin{tikzcd} R \arrow[r, "\lambda_R"] \arrow[d, "\theta"'] & \operatorname{Hom}_R(M,M) \\ S \arrow[r, "\lambda_S"] & \operatorname{Hom}_S(M,M) \arrow[u, "H_\theta"'] \end{tikzcd}$$

where λ_R and λ_S are the left regular representations of Example 1.1.13 and H_θ is one-to-one.

EXERCISE 1.1.6. Let R be a commutative ring and S a commutative R-algebra. Prove:

(1) The polynomial ring $R[x_1, \dots, x_n]$ in n indeterminates over R is a finitely generated R-algebra.
(2) S is a finitely generated R-algebra if and only if S is the homomorphic image of $R[x_1, \dots, x_n]$ for some n.
(3) (Algebra version of Finitely Generated over Finitely Generated is Finitely Generated) If T is a finitely generated S-algebra and S is a finitely generated R-algebra, then T is a finitely generated R-algebra.

EXERCISE 1.1.7. Let $n \geq 2$ be an integer and ζ a primitive nth root of unity in $\mathbb{C}$. Let R be a commutative $\mathbb{Z}[\zeta]$-algebra. Let $a \in R$ and set $S = R[x]/(x^n - a)$. Show that there is an R-algebra automorphism $\sigma : S \to S$ induced by the assignment $x \mapsto \zeta x$.

EXERCISE 1.1.8. Let A be a commutative ring and R a subring of A. The *conductor* from A to R is

$$R : A = \{\alpha \in A \mid \alpha A \subseteq R\}.$$

Prove that $R : A$ is an A-submodule of R, hence it is an ideal of both R and A.

EXERCISE 1.1.9. Let $I_1, I_2, \dots, I_n$ be pairwise comaximal ideals in the commutative ring R. Prove that $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$.

EXERCISE 1.1.10. Prove that if I and J are comaximal ideals in the commutative ring R, then for every $m \geq 1$ and $n \geq 1$, I^m and J^n are comaximal. Prove that in this case $I^m J^n = I^m \cap J^n$. (Hint: Apply the Binomial Theorem.)

EXERCISE 1.1.11. A *local ring* is a commutative ring R such that R has exactly one maximal ideal. If R is a local ring with maximal ideal $\mathfrak{m}$, then $R/\mathfrak{m}$ is called the *residue field* of R. If $(R, \mathfrak{m})$ and $(S, \mathfrak{n})$ are local rings and $f : R \to S$ is a homomorphism of rings, then we say f is a *local homomorphism of local rings* in case $f(\mathfrak{m}) \subseteq \mathfrak{n}$. Prove:

(1) If $(R, \mathfrak{m})$ is a local ring, then the group of units of R is equal to the set $R - \mathfrak{m}$.
(2) If $f : R \to S$ is a local homomorphism of local rings, then f induces a homomorphism of residue fields $R/\mathfrak{m} \to S/\mathfrak{n}$.

EXERCISE 1.1.12. Let R be a commutative ring. Denote by R^* the group of units in R. Show that the following are equivalent.

(1) R is a local ring (see Exercise 1.1.11).
(2) For every $r \in R$, either $r \in R^*$ or $1 - r \in R^*$.
(3) For every pair r, s in R, if $r + s = 1$, then either $r \in R^*$ or $s \in R^*$.

EXERCISE 1.1.13. For the following, let I, J and K be ideals in a commutative ring R. By Exercise 1.1.3, $I : J = \{r \in R \mid rJ \subseteq I\}$ is an ideal of R, and is called the ideal quotient, or colon ideal. Prove that the ideal quotient satisfies the following properties.

(1) $I \subseteq I : J$
(2) $(I : J)J \subseteq I$
(3) $(I : J) : K = I : JK = (I : K) : J$
(4) If $\{I_\alpha \mid \alpha \in S\}$ is a collection of ideals in R, then

$$\left(\bigcap_{\alpha \in S} I_\alpha\right) : J = \bigcap_{\alpha \in S} (I_\alpha : J)$$

(5) If $\{J_\alpha \mid \alpha \in S\}$ is a collection of ideals in R, then

$$I : \sum_{\alpha \in S} J_\alpha = \bigcap_{\alpha \in S} (I : J_\alpha)$$

2. The Well Ordering Principle and Some of Its Equivalents

Let X be a set and $\leq$ a binary relation on X which is reflexive, antisymmetric and transitive. Then we say $\leq$ is a *partial order* on X. We also say X is *partially ordered by* $\leq$. If $x, y \in X$, then we say x and y are *comparable* if $x \leq y$ or $y \leq x$. A *chain* is a partially ordered set with the property that any two elements are comparable. If $S \subseteq X$ is a nonempty subset, then S is partially ordered by the restriction of $\leq$ to $S \times S$. If the restriction of $\leq$ to S is a chain, then we say S is a *chain in* X.

Let X be partially ordered by $\leq$ and suppose S is a nonempty subset of X. Let $a \in S$. We say a is the *least* element of S if $a \leq x$ for all $x \in S$. If it exists, clearly the least element is unique. We say a is a *minimal* element of S in case $x \leq a$ implies $x = a$ for all $x \in S$. We say a is a *maximal* element of S in case $a \leq x$ implies $x = a$ for all $x \in S$. A *well ordered* set is a partially ordered set X such that every nonempty subset S has a least element. The reader should verify that a well ordered set is a chain. An element $u \in X$ is called an *upper bound* for S in case $x \leq u$ for all $x \in S$. An element $l \in X$ is called a *lower bound* for S in case $l \leq x$ for all $x \in S$. An element $U \in X$ is a *supremum*, or *least upper bound* for S, denoted $U = \sup(S)$, in case U is an upper bound for S and U is a lower bound for the set of all upper bounds for S. The reader should verify that the supremum is unique, if it exists. An element $L \in X$ is an *infimum*, or *greatest lower bound* for S, denoted $L = \inf(S)$, in case L is a lower bound for S and L is an upper bound for the set of all lower bounds for S. The reader should verify that the infimum is unique, if it exists. A *lattice* is a partially ordered set X such that $\sup\{x, y\}$ exists and $\inf\{x, y\}$ exists, for every pair of elements x, y in X.

Let X be partially ordered by $\leq$. We say that X satisfies the *minimum condition* if every nonempty subset of X contains a minimal element. We say that X satisfies the *maximum condition* if every nonempty subset of X contains a maximal element. We say that X satisfies the *descending chain condition* (DCC) if every chain in X of the form $\{\dots, x_3 \leq x_2 \leq x_1 \leq x_0\}$ is eventually constant. That is, there is a subscript n such that $x_n = x_i$ for all $i \geq n$. We say that X satisfies the *ascending chain condition* (ACC) if every chain in X of the form $\{x_0 \leq x_1 \leq x_2 \leq x_3, \dots\}$ is eventually constant.

PROPOSITION 1.2.1. *Let X be a set that is partially ordered by $\leq$.*

(1) X satisfies the descending chain condition (DCC) if and only if X satisfies the minimum condition.
(2) X satisfies the ascending chain condition (ACC) if and only if X satisfies the maximum condition.

AXIOM 1.2.2. *(The Well Ordering Principle) If X is a nonempty set, then there exists a partial order $\leq$ on X such that X is a well ordered set. That is, every nonempty subset of X has a least element.*

Let X be a set and $\leq$ a partial order on X. If $x, y \in X$, then we write $x < y$ in case $x \leq y$ and $x \neq y$. Suppose $C \subseteq X$ is a chain in X and $\alpha \in C$. The *segment of C determined by* α, written $(-\infty, \alpha)$, is the set of all elements $x \in C$ such that $x < \alpha$. A subset $W \subseteq C$ is called an *inductive subset* of C provided that for any $\alpha \in C$, if $(-\infty, \alpha) \subseteq W$, then $\alpha \in W$.

PROPOSITION 1.2.3. *(The Transfinite Induction Principle) Suppose X is a well ordered set and W is an inductive subset of X. Then $W = X$.*

PROOF. Suppose $X - W$ is nonempty. Let α be the least element of $X - W$. Then W contains the segment $(-\infty, \alpha)$. Since W is inductive, it follows that $\alpha \in W$, which is a contradiction. $\square$

PROPOSITION 1.2.4. *(Zorn's Lemma) Let X be a partially ordered set. If every chain in X has an upper bound, then X contains a maximal element.*

PROOF. By Axiom 1.2.2, there exists a well ordered set W and a one-to-one correspondence $\omega : W \to X$. Using Proposition 1.2.3, define a sequence $\{C(w) \mid w \in W\}$ of well ordered subsets of X. If w_0 is the least element of W, define $C(w_0) = \{\omega(w_0)\}$. Inductively assume $\alpha \in W - \{w_0\}$ and that for all $w < \alpha$, $C(w)$ is defined and the following are satisfied

(1) if $w_0 \le w_1 \le w_2 < \alpha$, then $C(w_1) \subseteq C(w_2)$,
(2) $C(w)$ is a well ordered chain in X, and
(3) $C(w) \subseteq \{\omega(i) \mid w_0 \le i \le w\}$.

Let $x = \omega(\alpha)$ and
$$F = \bigcup_{w<\alpha} C(w).$$
The reader should verify that F is a well ordered chain in X and $F \subseteq \{\omega(i) \mid w_0 \le i < \alpha\}$. Define $C(\alpha)$ by the rule
$$C(\alpha) = \begin{cases} F \cup \{x\} & \text{if } x \text{ is an upper bound for } F \\ F & \text{otherwise.} \end{cases}$$
The reader should verify that $C(\alpha)$ satisfies

(4) if $w_0 \le w_1 \le w_2 \le \alpha$, then $C(w_1) \subseteq C(w_2)$,
(5) $C(\alpha)$ is a well ordered chain in X, and
(6) $C(\alpha) \subseteq \{\omega(i) \mid w_0 \le i \le \alpha\}$.

By Proposition 1.2.3, the sequence $\{C(w) \mid w \in W\}$ is defined and the properties (4), (5) and (6) are satisfied for all $\alpha \in W$. Now set
$$G = \bigcup_{w<\alpha} C(w).$$
The reader should verify that G is a well ordered chain in X. By hypothesis, G has an upper bound, say u. We show that u is a maximal element of X. For contradiction's sake, assume X has no maximal element. Then we can choose the upper bound u to be an element of $X - G$. For some $w_1 \in W$ we have $u = \omega(w_1)$. For all $w < w_1$, u is an upper bound for $C(w)$. By the definition of $C(w_1)$, we have $u \in C(w_1)$. This is a contradiction, because $C(w_1) \subseteq G$. $\square$

DEFINITION 1.2.5. Let I be a set and $\{X_i \mid i \in I\}$ a family of sets indexed by I. The *product* is
$$\prod_{i \in I} X_i = \left\{ f : I \to \bigcup X_i \mid f(i) \in X_i \right\}.$$
An element f of the product is called a choice function, because f chooses one element from each member of the family of sets.

PROPOSITION 1.2.6. *(The Axiom of Choice) Let I be a set and $\{X_i \mid i \in I\}$ a family of nonempty sets indexed by I. Then the product $\prod_{i \in I} X_i$ is nonempty. That is, there exists a function f on I such that $f(i) \in X_i$ for each $i \in I$.*

PROOF. By Axiom 1.2.2, we can assume $\bigcup_{i \in I} X_i$ is well ordered. We can view X_i as a subset of $\bigcup_{i \in I} X_i$. For each $i \in I$, let x_i be the least element of X_i. The set of ordered pairs (i, x_i) defines the choice function. $\square$

3. Topological Spaces

DEFINITION 1.3.1. Let X be a set. A *topology* on X is a subset $\mathscr{T}$ of 2^X that satisfies the following properties:

(1) $X \in \mathscr{T}$.
(2) $\emptyset \in \mathscr{T}$.
(3) If $A, B \in \mathscr{T}$, then $A \cup B \in \mathscr{T}$.
(4) If $\{A_i \mid i \in I\}$ is a family of sets such that each $A_i \in \mathscr{T}$, then $\cap_i A_i \in \mathscr{T}$.

The elements of $\mathscr{T}$ are called *closed sets*. If $A \in \mathscr{T}$, then $X - A$ is called an *open set*. If $Y \subseteq X$, then $\mathscr{T}$ restricts to a topology on Y whose closed sets are $\{A \cap Y \mid A \in \mathscr{T}\}$.

DEFINITION 1.3.2. Let X and Y be topological spaces and $f : X \to Y$ a function. Then f is said to be *continuous*, if $f^{-1}(Y)$ is closed whenever Y is closed. Equivalently, f is continuous if $f^{-1}(U)$ is open whenever U is open. If f is continuous, and $g : Y \to Z$ is continuous, then one can check that $gf : X \to Z$ is continuous. We say X and Y are *homeomorphic*, if there exist continuous functions $f : X \to Y$ and $g : Y \to X$ such that $gf = 1_X$ and $fg = 1_Y$.

DEFINITION 1.3.3. Let X be a topological space and Y a nonempty subset. We say Y is *irreducible* if whenever $Y \subseteq Y_1 \cup Y_2$ and Y_1, Y_2 are closed subsets of X, then $Y \subseteq Y_1$, or $Y \subseteq Y_2$. We say Y is *connected* if whenever $Y \subseteq Y_1 \cup Y_2$ and Y_1, Y_2 are disjoint closed subsets of X, then $Y \subseteq Y_1$, or $Y \subseteq Y_2$. The empty set is not considered to be irreducible or connected. Notice that an irreducible set is connected.

If Z is a subset of the topological space X, then the *closure* of Z, denoted $\bar{Z}$, is the smallest closed subset of X that contains Z. Equivalently, $\bar{Z}$ is equal to the intersection of all closed sets that contain Z.

LEMMA 1.3.4. *Let X be a topological space.*

(1) If X is irreducible and $U \subseteq X$ is a nonempty open of X, then U is irreducible and dense.
(2) Let Z be a subset of X and denote by $\bar{Z}$ the closure of Z in X. Then Z is irreducible if and only if $\bar{Z}$ is irreducible.
(3) If X is irreducible, then X is connected.

PROOF. Is left to the reader. □

A topological space X is said to be *noetherian* if X satisfies the ascending chain condition on open sets. Some equivalent conditions are given by the next lemma.

LEMMA 1.3.5. *The following are equivalent, for a topological space X.*

(1) X satisfies the ascending chain condition on open sets.
(2) X satisfies the maximum condition on open sets.
(3) X satisfies the descending chain condition on closed sets.
(4) X satisfies the minimum condition on closed sets.

PROOF. Proposition 1.2.1 shows the equivalence of (1) and (2), as well as the equivalence of (3) and (4). The rest is left to the reader. □

LEMMA 1.3.6. *Let X be a topological space.*

(1) If $X = X_1 \cup \cdots \cup X_n$ and each X_i is noetherian, then X is noetherian.
(2) If X is noetherian and $Y \subseteq X$, then Y is noetherian.
(3) If X is noetherian, then X is compact. That is, every open cover of X contains a finite subcover.

PROOF. Is left to the reader. □

PROPOSITION 1.3.7. *Let X be a noetherian topological space and Z a nonempty closed subset of X.*

(1) There are unique irreducible closed subsets $Z_1,\dots,Z_r$ such that $Z = Z_1 \cup \cdots \cup Z_r$ and $Z_i \not\subseteq Z_j$ for all $i \neq j$. The sets Z_i are called the irreducible components *of Z.*
(2) There are unique connected closed subsets $Y_1,\dots,Y_c$ such that $Z = Y_1 \cup \cdots \cup Y_c$ and $Y_i \cap Y_j = \emptyset$ for all $i \neq j$. The sets Y_i are called the connected components *of Z.*
(3) The number of connected components is less than or equal to the number of irreducible components.

PROOF. (1): We first prove the existence of the decomposition. For contradiction's sake, assume there is a nonempty closed subset Y such that Y cannot be written as a union of a finite number of irreducible closed sets. Let $\mathscr{S}$ be the collection of all such subsets. By Lemma 1.3.5 (4), $\mathscr{S}$ has a minimal member, call it Y. Then Y is itself not irreducible, so we can write $Y = Y_1 \cup Y_2$ where each Y_i is a proper closed subset of Y. By minimality of Y, it follows that each Y_i is not in $\mathscr{S}$. Therefore each Y_i can be decomposed into irreducibles. This means $Y = Y_1 \cup Y_2$ can also be decomposed into irreducibles, which is a contradiction. So Z is not a counterexample. In other words, we can write $Z = Z_1 \cup \cdots \cup Z_r$ such that each Z_i is irreducible. If $Z_i \subseteq Z_j$ for some j different from i, then Z_i may be excluded.

Now we prove the uniqueness of the decomposition. Let $Z = Z_1 \cup \cdots \cup Z_r$ and $Z = W_1 \cup \cdots \cup W_p$ be two such decompositions. Then

$$Z_1 = (Z_1 \cap W_1) \cup \cdots \cup (Z_1 \cap W_p).$$

Since Z_1 is irreducible, $Z_1 = Z_1 \cap W_i$ for some i. Therefore $Z_1 \subseteq W_i$. Likewise $W_i \subseteq Z_j$ for some j. This implies

$$Z_1 \subseteq W_i \subseteq Z_j.$$

It follows that $Z_1 = W_i$. By a finite induction argument, we are done.

(2): Existence follows by the minimal counterexample method of Part (1). The rest is left to the reader.

(3): Each Z_i is connected, by Lemma 1.3.4. Then each Z_i belongs to a unique connected component of X. □

A topological space X is said to be a T_1-*space* if for every point $x \in X$ the subset $\{x\}$ is closed. We say X is *separated* (or *Hausdorff*, or a T_2-*space*), if for any two distinct points $x, y \in X$, there are neighborhoods $x \in U$ and $y \in V$ such that $U \cap V = \emptyset$. We say X is *compact* if for any open cover $\{U_i \mid i \in D\}$ of X, there is a finite subset $J \subseteq D$ such that $\{U_i \mid i \in D\}$ is an open cover of X. Let $\{X_i \mid i \in D\}$ be a family of topological spaces indexed by a set D. The *product topology* on $\prod_{i\in D} X_i$ is defined to be the finest topology such that all of the projection maps $\pi_i : \prod_{i\in D} X_i \to X_i$ are continuous.

4. Categories and Functors

A *category* consists of a collection of *objects* and a collection of *morphisms* between pairs of those objects. The composition of morphisms is defined and is again a morphism. For our purposes, a category will usually be one of the following:

(1) The category whose objects are modules over a ring R and whose morphisms are homomorphisms of modules. By ${}_R\mathfrak{M}$ we denote the category of all left R-modules together with R-module homomorphisms. By $\mathfrak{M}_R$ we denote the category of all right R-modules together with R-module homomorphisms. If A and B

are R-modules, the set of all R-module homomorphisms from A to B is denoted $\operatorname{Hom}_R(A,B)$.

(2) The category of whose objects are rings and whose morphisms are homomorphisms of rings. A subcategory would be the category whose objects are commutative rings.
(3) The category whose objects are finitely generated algebras over a fixed commutative ring R and whose morphisms are R-algebra homomorphisms.
(4) The category whose objects are sets and whose morphisms are functions.
(5) The category of pointed sets. A *pointed set* is a pair (X,x) where X is a nonempty set and x is a distinguished element of X called the *base point*. A morphism from a pointed set (X,x) to a pointed set (Y,y) is a function $f : X \to Y$ such that $f(x) = y$.

For any pair of objects A, B in a category $\mathfrak{C}$, the collection of all morphisms from A to B is denoted $\operatorname{Hom}_{\mathfrak{C}}(A,B)$. A *covariant functor* from a category $\mathfrak{C}$ to a category $\mathfrak{D}$ is a correspondence $\mathfrak{F} : \mathfrak{C} \to \mathfrak{D}$ which is a function on objects $A \mapsto \mathfrak{F}(A)$ and for any pair of objects $A,B \in \mathfrak{C}$, each morphism f in $\operatorname{Hom}_{\mathfrak{C}}(A,B)$ is mapped to a morphism $\mathfrak{F}(f)$ in $\operatorname{Hom}_{\mathfrak{D}}(\mathfrak{F}(A),\mathfrak{F}(B))$ such that the following are satisfied

(1) If $1 : A \to A$ is the identity map, then $\mathfrak{F}(1) : \mathfrak{F}(A) \to \mathfrak{F}(A)$ is the identity map.
(2) Given a commutative triangle in $\mathfrak{C}$

$$\begin{tikzcd} & B \arrow[dr, "g"] & \\ A \arrow[ur, "f"] \arrow[rr, "gf"] & & C \end{tikzcd}$$

the triangle

$$\begin{tikzcd} & \mathfrak{F}(B) \arrow[dr, "\mathfrak{F}(g)"] & \\ \mathfrak{F}(A) \arrow[ur, "\mathfrak{F}(f)"] \arrow[rr, "\mathfrak{F}(gf)"] & & \mathfrak{F}(C) \end{tikzcd}$$

commutes in $\mathfrak{D}$.

EXAMPLE 1.4.1. The opposite ring of R is denoted R^o. Multiplication in R^o is denoted by $*$ and is reversed from multiplication in R: $x * y = yx$. Any $M \in {}_R\mathfrak{M}$ can be made into a right R^o-module by defining $m * r = rm$. The reader should verify that this defines a covariant functor ${}_R\mathfrak{M} \to \mathfrak{M}_{R^o}$.

The definition of a *contravariant functor* is similar, except the arrows get reversed. That is, if $\mathfrak{F} : \mathfrak{C} \to \mathfrak{D}$ is a contravariant functor and f is an element of $\operatorname{Hom}_{\mathfrak{C}}(A,B)$, then $\mathfrak{F}(f)$ is in $\operatorname{Hom}_{\mathfrak{D}}(\mathfrak{F}(B),\mathfrak{F}(A))$.

If $\mathfrak{F} : \mathfrak{C} \to \mathfrak{D}$ is a covariant functor between categories of modules, then $\mathfrak{F}$ is *left exact* if for every short exact sequence

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{4.1}$$

in $\mathfrak{C}$, the corresponding sequence

$$0 \to \mathfrak{F}(A) \xrightarrow{\mathfrak{F}(\alpha)} \mathfrak{F}(B) \xrightarrow{\mathfrak{F}(\beta)} \mathfrak{F}(C)$$

is exact in $\mathfrak{D}$. We say $\mathfrak{F}$ is *right exact* if for every short exact sequence (4.1) in $\mathfrak{C}$, the sequence

$$\mathfrak{F}(A) \xrightarrow{\mathfrak{F}(\alpha)} \mathfrak{F}(B) \xrightarrow{\mathfrak{F}(\beta)} \mathfrak{F}(C) \to 0$$

is exact in $\mathfrak{D}$.

If $\mathfrak{F} : \mathfrak{C} \to \mathfrak{D}$ is a contravariant functor between categories of modules, then $\mathfrak{F}$ is *left exact* if for every short exact sequence (4.1) in $\mathfrak{C}$, the sequence

$$0 \to \mathfrak{F}(C) \xrightarrow{\mathfrak{F}(\beta)} \mathfrak{F}(B) \xrightarrow{\mathfrak{F}(\alpha)} \mathfrak{F}(A)$$

is exact in $\mathfrak{D}$. We say the contravariant functor $\mathfrak{F}$ is *right exact* if for every short exact sequence (4.1) in $\mathfrak{C}$, the sequence

$$\mathfrak{F}(C) \xrightarrow{\mathfrak{F}(\beta)} \mathfrak{F}(B) \xrightarrow{\mathfrak{F}(\alpha)} \mathfrak{F}(A) \to 0$$

is exact in $\mathfrak{D}$.

DEFINITION 1.4.2. Let $F : \mathfrak{A} \to \mathfrak{C}$ and $G : \mathfrak{C} \to \mathfrak{A}$ be covariant functors. We say that (F, G) is an *adjoint pair* if for every $A \in \mathfrak{A}$ and $C \in \mathfrak{C}$ there exists a bijection

$$\psi : \mathrm{Hom}_{\mathfrak{C}}(FA, C) \to \mathrm{Hom}_{\mathfrak{A}}(A, GC)$$

such that for any $\alpha : A \to A'$ in $\mathfrak{A}$, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathfrak{C}}(FA', C) \arrow[r, "\mathrm{H}_{F\alpha}"] \arrow[d, "\psi"'] & \mathrm{Hom}_{\mathfrak{C}}(FA, C) \arrow[d, "\psi"] \\
\mathrm{Hom}_{\mathfrak{A}}(A', GC) \arrow[r, "\mathrm{H}_{\alpha}"] & \mathrm{Hom}_{\mathfrak{A}}(A, GC)
\end{tikzcd}$$

commutes and given any $\gamma : C \to C'$ in ${}_S\mathfrak{M}$, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathfrak{C}}(FA, C) \arrow[r, "\mathrm{H}_{\gamma}"] \arrow[d, "\psi"'] & \mathrm{Hom}_{\mathfrak{C}}(FA, C') \arrow[d, "\psi"] \\
\mathrm{Hom}_{\mathfrak{A}}(A, GC) \arrow[r, "\mathrm{H}_{G\gamma}"] & \mathrm{Hom}_{\mathfrak{A}}(A, GC')
\end{tikzcd}$$

commutes. We say that ψ is *natural in the variable A and the variable C*.

Presently, we give an example of two functors that are adjoint pairs obtained by tensor products and groups of homomorphisms (see Theorem 2.4.10).

DEFINITION 1.4.3. Let $\mathfrak{C}$ and $\mathfrak{D}$ be categories of modules and suppose we have two functors $\mathfrak{F}$ and $\mathfrak{F}'$ from $\mathfrak{C}$ to $\mathfrak{D}$. We say that $\mathfrak{F}$ and $\mathfrak{F}'$ are *naturally equivalent* if for every module M in $\mathfrak{C}$ there is an isomorphism φ_M in $\mathrm{Hom}_{\mathfrak{D}}\big(\mathfrak{F}(M), \mathfrak{F}'(M)\big)$ such that, for every pair of modules M and N in $\mathfrak{C}$ and any $f \in \mathrm{Hom}_{\mathfrak{C}}(M, N)$, the diagram

$$\begin{tikzcd}
\mathfrak{F}(M) \arrow[r, "\mathfrak{F}(f)"] \arrow[d, "\varphi_M"'] & \mathfrak{F}(N) \arrow[d, "\varphi_N"] \\
\mathfrak{F}'(M) \arrow[r, "\mathfrak{F}'(f)"] & \mathfrak{F}'(N)
\end{tikzcd}$$

commutes. We denote by $I_{\mathfrak{C}}$ the identity functor on the category $\mathfrak{C}$ defined by $I_{\mathfrak{C}}(M) = M$ and $I_{\mathfrak{C}}(f) = f$, for modules M and maps f. Then we say two categories $\mathfrak{C}$ and $\mathfrak{D}$ are *equivalent* if there is a functor $\mathfrak{F} : \mathfrak{C} \to \mathfrak{D}$ and a functor $\mathfrak{G} : \mathfrak{D} \to \mathfrak{C}$ such that $\mathfrak{F} \circ \mathfrak{G}$ is naturally equivalent to $I_{\mathfrak{D}}$ and $\mathfrak{G}\circ\mathfrak{F}$ is naturally equivalent to $I_{\mathfrak{C}}$. The functors $\mathfrak{F}$ and $\mathfrak{G}$ are then referred to as *inverse equivalences*.

EXAMPLE 1.4.4. Let R be a ring. The reader should verify that the category of left R-modules, ${}_R\mathfrak{M}$, is equivalent to the category of right R^o-modules, $\mathfrak{M}_{R^o}$.

DEFINITION 1.4.5. Let $\mathfrak{C}$ and $\mathfrak{D}$ be categories of modules and $\mathfrak{F}:\mathfrak{C}\to\mathfrak{D}$ a covariant functor. We say that $\mathfrak{F}$ is *fully faithful* if

$$\operatorname{Hom}_{\mathfrak{C}}(A,B)\to\operatorname{Hom}_{\mathfrak{D}}(\mathfrak{F}(B),\mathfrak{F}(A))$$

is a one-to-one correspondence. We say that $\mathfrak{F}$ is *essentially surjective* if for every object D in $\mathfrak{D}$, there exists C in $\mathfrak{C}$ such that D is isomorphic to $\mathfrak{F}(C)$.

PROPOSITION 1.4.6. *Let $\mathfrak{C}$ and $\mathfrak{D}$ be categories of modules and $\mathfrak{F}:\mathfrak{C}\to\mathfrak{D}$ a covariant functor. Then $\mathfrak{F}$ establishes an equivalence of categories if and only if $\mathfrak{F}$ is fully faithful and essentially surjective.*

PROOF. Assume there is a functor $\mathfrak{G}:\mathfrak{D}\to\mathfrak{C}$ such that the functors $\mathfrak{F}$ and $\mathfrak{G}$ are inverse equivalences. By the natural equivalence of $\mathfrak{F}\circ\mathfrak{G}$ with the identity functor, we see that $\mathfrak{F}$ is essentially surjective. To prove that $\mathfrak{F}$ is fully faithful, we show that $\operatorname{Hom}_{\mathfrak{C}}(A,B)\to\operatorname{Hom}_{\mathfrak{D}}(\mathfrak{F}(A),\mathfrak{F}(B))$ is one-to-one and onto.

Suppose f, g are elements of $\operatorname{Hom}_{\mathfrak{C}}(A,B)$ with $\mathfrak{F}(f)=\mathfrak{F}(g)$ in $\operatorname{Hom}_{\mathfrak{D}}\big(\mathfrak{F}(A),\mathfrak{F}(B)\big)$. Then $\mathfrak{G}\big(\mathfrak{F}(f)\big)=\mathfrak{G}\big(\mathfrak{F}(g)\big)$ in $\operatorname{Hom}_{\mathfrak{C}}\Big(\mathfrak{G}\big(\mathfrak{F}(A)\big),\mathfrak{G}\big(\mathfrak{F}(B)\big)\Big)$. By the natural equivalence of $\mathfrak{G}\circ\mathfrak{F}$ with the identity functor, this implies that $f=g$. By a symmetric argument we see that

$$\operatorname{Hom}_{\mathfrak{D}}\big(\mathfrak{F}(A),\mathfrak{F}(B)\big)\to\operatorname{Hom}_{\mathfrak{C}}\Big(\mathfrak{G}\big(\mathfrak{F}(A)\big),\mathfrak{G}\big(\mathfrak{F}(B)\big)\Big) \tag{4.2}$$

is one-to-one.

Now suppose g is any element of $\operatorname{Hom}_{\mathfrak{D}}\big(\mathfrak{F}(A),\mathfrak{F}(B)\big)$. We then obtain the square

$$\begin{tikzcd}
\mathfrak{G}\big(\mathfrak{F}(A)\big) \arrow[r, "\mathfrak{G}(g)"] \arrow[d, "\varphi_A"'] & \mathfrak{G}\big(\mathfrak{F}(B)\big) \arrow[d, "\varphi_B"] \\
A \arrow[r, "f"] & B
\end{tikzcd}$$

where φ_A and φ_B, arise from the natural equivalence of $\mathfrak{G}\circ\mathfrak{F}$ with the identity and where $f=\varphi_B\mathfrak{G}(g)\varphi_A^{-1}$. On the other hand, we also have the square

$$\begin{tikzcd}
\mathfrak{G}\big(\mathfrak{F}(A)\big) \arrow[r, "\mathfrak{G}\left(\mathfrak{F}(f)\right)"] \arrow[d, "\varphi_A"'] & \mathfrak{G}\big(\mathfrak{F}(B)\big) \arrow[d, "\varphi_B"] \\
A \arrow[r, "f"] & B
\end{tikzcd}$$

from which we deduce that $\mathfrak{G}(g)=\mathfrak{G}\big(\mathfrak{F}(f)\big)$. Since (4.2) is one-to-one, it follows that $g=\mathfrak{F}(f)$. This shows $\mathfrak{F}$ is fully faithful.

For a proof of the converse, the reader is referred to a book on Category Theory. For example, see [**10**, Proposition (1.1), p. 4]. □

5. Prime Ideals and Prime Elements in Commutative Rings

DEFINITION 1.5.1. Let R be a commutative ring. An ideal I in R is *prime* in case R/I is an integral domain. An ideal I in R is *maximal* in case R/I is a field. A field is an integral domain, so a maximal ideal is a prime ideal. An integral domain has at least two elements, so the unit ideal is not prime.

Let a be an element of R which is not a unit and not a zero divisor. Then a is *irreducible* in case whenever $a = bc$, either b is a unit or c is a unit. We say that a is *prime* in case whenever $a \mid bc$, either $a \mid b$ or $a \mid c$.

LEMMA 1.5.2. *Let R be an integral domain and p an element of R.*

(1) p is prime if and only if (p) is a prime ideal.
(2) p is irreducible if and only if the principal ideal (p) is maximal among nonunit principal ideals of R.
(3) If p is prime, then p is irreducible.
(4) If p is irreducible and q is an associate of p, then q is irreducible.
(5) If p is prime and q is an associate of p, then q is prime.
(6) If p is irreducible, then the only divisors of p are units and associates of p.

PROPOSITION 1.5.3. *Let R be a ring and I an ideal in R. There is a one-to-one order-preserving correspondence between the ideals J such that $I \subseteq J \subseteq R$ and the ideals of R/I given by $J \mapsto J/I$. If R is commutative, then there is a one-to-one correspondence between prime ideals of R/I and prime ideals of R that contain I.*

PROPOSITION 1.5.4. *Let R be a commutative ring and P an ideal of R. Assume $P \neq R$. The following are equivalent.*

(1) P is a prime ideal. That is, R/P is an integral domain.
(2) For all $x, y \in R$, if $xy \in P$, then $x \in P$ or $y \in P$.
(3) For any ideals I, J in R, if $IJ \subseteq P$, then $I \subseteq P$ or $J \subseteq P$.

PROPOSITION 1.5.5. *Let R be a commutative ring.*

(1) An ideal M is a maximal ideal in R if and only if M is not contained in a larger proper ideal of R.
(2) If I is an ideal of R and $I \neq R$, then R contains a maximal ideal M such that $I \subseteq M$.

We end this short section with a proof that an integral domain R is a principal ideal domain if and only if R is a unique factorization domain such that every nonzero prime ideal of R is a maximal ideal. A ring R that has the ascending chain condition on left ideals is said to be *left noetherian*. Likewise, we say R is *right noetherian*, if the ACC holds for right ideals.

THEOREM 1.5.6. *If R is a principal ideal domain, then R is a noetherian unique factorization domain.*

PROOF. See [**19**, Theorem 3.4.15]. □

EXAMPLE 1.5.7. Let R be a unique factorization domain. If x is a nonzero nonunit in R, then the number of factors in a factorization of x into primes is unique ([**19**, Definition 3.4.11]). Let $\nu(x)$ be the number of factors in a prime factorization of x. Extend ν to a function from R to the well ordered set $\mathbb{N} \cup \{0\} \cup \{\infty\}$ by setting $\nu(0) = \infty$ and $\nu(x) = 0$ if x is a unit. The function ν satisfies:

(1) $\nu(xy) = \nu(x) + \nu(y)$.

(2) $\nu(x) = 0$ if and only if x is a unit.
(3) $\nu(x) = 1$ if and only if x is irreducible.

THEOREM 1.5.8. *If R is an integral domain that is not a field, then the following are equivalent.*

(1) R is a principal ideal domain.
(2) R is a unique factorization domain with the property that every nonzero prime ideal is a maximal ideal.

PROOF. (1) implies (2): A PID is a UFD, by Theorem 1.5.6. If P is a nonzero prime ideal in R, then $P = (\pi)$ is principal and π is irreducible. In an integral domain a principal ideal generated by an irreducible element is maximal among proper principal ideals, by [**19**, Theorem 3.4.5]. So P is a maximal ideal in R.

(2) implies (1): Assume R is a UFD and every nonzero prime ideal is maximal. As in Example 1.5.7, let $\nu : R \to \mathbb{Z} \cup \{\infty\}$ be the function defined by: $\nu(x)$ is the number of factors in a representation of x as a product of irreducibles. Given a nonzero ideal I, define $\nu(I)$ to be the minimum of $\{\nu(x) \mid x \in I\}$. Then $\nu(I) = 0$ if and only if $I = R$. If I is a prime ideal in R, then by Exercise 1.5.2 there is a prime element $\pi \in I$. By Lemma 1.5.2, (π) is a prime ideal and by hypothesis (π) is a maximal ideal in R. Hence $(\pi) \subseteq I$ implies $I = (\pi)$ is principal. This and [**19**, Corollary 3.4.14] imply that $\nu(I) = 1$ if and only if I is a prime ideal.

Let I be a nonzero ideal in R. The proof is by induction on $\nu(I)$. As seen already, if $\nu(I) \leq 1$, then I is principal. Inductively, assume $n > 1$ and that if J is an ideal of R with $\nu(J) < n$, then J is principal. Let I be an ideal with $\nu(I) = n$. We prove that I is principal. Let $x \in I$ be such that $\nu(x) = n$. Let p be an irreducible factor of x and write $x = px_1$. Then $\nu(x_1) = n - 1$. Let $y \in I - (0)$. Assume for sake of contradiction that y is not in (p). Then $(y) + (p) = (1)$ since (p) is a maximal ideal. For some $a, b \in R$ we have $1 = ay + bp$. Then $x_1 = ayx_1 + bpx_1 = ax_1y + bx$ is in I. This is a contradiction, since $\nu(x_1) = n - 1$ and $\nu(I) = n$. We conclude that $y \in (p)$, which proves that $I \subseteq (p)$. By Exercise 1.1.13, $I = (I : (p))(p)$, where $(I : (p))$ is the ideal quotient. In particular, $x = px_1$ and $x_1 \in (I : (p))$. This proves $\nu(I : (p)) \leq n - 1$. By our induction hypothesis, $I : (p) = (z)$ is principal. Then $I = (I : (p))(p) = (z)(p) = (zp)$ is principal, which completes the proof. $\square$

5.1. Exercises.

EXERCISE 1.5.1. Let R be an integral domain that satisfies the two properties:

(A) In R an irreducible element is a prime element.
(B) R satisfies the ascending chain condition on principal ideals. That is, given a chain of principal ideals $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots \subseteq \langle a_n \rangle \subseteq \cdots$, there exists $N \geq 1$ such that $\langle a_N \rangle = \langle a_{N+1} \rangle = \cdots$.

Follow the outline below to show that R is a unique factorization domain.

(1) Prove that if $a \in R$ is a nonunit, nonzero element of R, then the set
$$\mathscr{S} = \{p \in R \mid p \text{ is irreducible and } p \mid a\}$$
contains only a finite number of associate classes. In other words, up to associates, a has only a finite number of irreducible factors.
(2) Suppose a is a nonzero element in R, p is irreducible and p is a factor of a. Prove that for some $n \geq 1$ we have $a \in (p^n)$ and $a \notin (p^{n+1})$.
(3) Prove that if $a \in R$ is a nonunit and a nonzero element, then there exists an irreducible element p such that $p \mid a$.

(4) R is a unique factorization domain.

(Hint: Use the proof of [**19**, Theorem 3.4.15] as an outline.

EXERCISE 1.5.2. Let R be a UFD and P a nonzero prime ideal of R. Prove that P contains a prime element π of R. (Hint: Let $x \in P - (0)$. Show that P contains at least one prime divisor of x.)

EXERCISE 1.5.3. Let R be a commutative ring. Let $\operatorname{Max}(R)$ be the set of all maximal ideals in R and R^* the group of units of R. Show that $R - R^* = \bigcup\{\mathfrak{m} \mid \mathfrak{m} \in \operatorname{Max}(R)\}$.

6. Free Modules and Vector Spaces

6.1. Direct Products and Direct Sums of Rings. Let $\{R_i \mid i \in I\}$ be a family of rings. For each $i \in I$, the same symbol 0 is used to denote the additive identity of each R_i. Likewise, 1 denotes the multiplicative identity of each R_i. The *direct product* is

$$\prod_{i \in I} R_i = \left\{ f : I \to \bigcup_{i \in I} R_i \mid f(i) \in R_i \right\}.$$

Notice that as a set, it is the product of the underlying sets as defined in Definition 1.2.5. The direct product of a family of rings is a ring if addition and multiplication are defined coordinate-wise:

$$(f+g)(i) = f(i) + g(i)$$
$$(fg)(i) = f(i)g(i).$$

Since each R_i contains 0, the additive identity in the product is the function $f(i) = 0$. Since each R_i contains 1, the multiplicative identity in the product is the function $f(i) = 1$. The other ring axioms hold in the product because they hold coordinate-wise. For each $k \in I$ the canonical projection map

$$\pi_k : \prod_{i \in I} R_i \to R_k,$$

defined by the rule $\pi_k(f) = f(k)$, is an onto homomorphism of rings. There is a canonical injection map

$$\iota_k : R_k \to \prod_{i \in I} R_i$$

which maps $x \in R_k$ to $\iota_k(x)$ which is equal to x in coordinate k, and 0 elsewhere. Then ι_k is a one-to-one homomorphism of additive groups, ι_k is multiplicative and $\pi_k \iota_k = 1_{R_k}$. The function ι_k is not a homomorphism of rings, since $\iota_k(1) \neq 1$.

The *direct sum* of a family of rings, denoted $\bigoplus_{i \in I} R_i$, is the smallest subring of the direct product that contains the set

$$\left\{ f : I \to \bigcup_{i \in I} R_i \mid f(i) \in R_i \text{ and } f(i) = 0 \text{ for all but finitely many } i \in I \right\}.$$

The canonical projection map

$$\pi_k : \bigoplus_{i \in I} R_i \to R_k$$

is an onto homomorphism of rings. The canonical injection map

$$\iota_k : R_k \to \bigoplus_{i \in I} R_i$$

is a one-to-one homomorphism of additive groups, is multiplicative, and we have $\pi_k \iota_k = 1_{R_k}$. The direct product and the direct sum are equal if the index set is finite. If $I = \{1, 2, \dots, n\}$, then

$$\bigoplus_{i=1}^{n} R_i = R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(x_1, \dots, x_n) \mid x_i \in R_i\}$$

which as a set is the usual product.

6.2. Direct Product and Direct Sum of a Family of Modules. As mentioned above, we define the direct product and the direct sum of a family of R-modules $\{M_i \mid i \in I\}$ over an arbitrary index set I.

DEFINITION 1.6.1. Let R be a ring, I an index set and $\{M_i \mid i \in I\}$ a family of R-modules indexed by I. The direct product $\prod_{i \in I} M_i = \{f : I \to \bigcup_{i \in I} \mid f(i) \in M_i\}$ is an abelian group. The binary operation is coordinate-wise addition: $(f+g)(i) = f(i) + g(i)$. The identity element, denoted 0, is the constant function $0(i) = 0$. The inverse of f is defined by $(-f)(i) = -f(i)$. We turn the direct product $\prod_{i \in I} M_i$ into an R-module by defining the R-action coordinate-wise: $(rf)(i) = rf(i)$. The R-module $\prod_{i \in I} M_i$ is called the *direct product* of $\{M_i \mid i \in I\}$. For each $k \in I$ there are the canonical injection and projection maps

$$M_k \xrightarrow{\iota_k} \prod_{i \in I} M_i \xrightarrow{\pi_k} M_k$$

where $\pi_k(f) = f(k)$ and for $x \in M_k$, $\iota_k(x)$ is x in coordinate k and 0 otherwise. Then $\pi_k \iota_k = 1_{M_k}$. The functions ι_k and π_k are R-module homomorphisms.

The *direct sum* of $\{M_i \mid i \in I\}$ is denoted $\bigoplus_{i \in I} M_i$ and is defined to be the submodule of the direct product generated by the set $\bigcup_{k \in I} \iota_k(M_k)$. It is routine to check that

$$\bigoplus_{i \in I} M_i = \left\{ f : I \to \bigcup_{i \in I} M_i \mid f(i) \in M_i \text{ and } f(i) = 0 \text{ for all but finitely many } i \in I \right\}.$$

For each $k \in I$ the canonical injection map ι_k factors through the direct sum. That is, $\iota_k : M_k \to \bigoplus_{i \in I} M_i$ is a one-to-one homomorphism of R-modules. All of the maps

$$M_k \xrightarrow{\iota_k} \bigoplus_{i \in I} M_i \xrightarrow{\subseteq} \prod_{i \in I} M_i \xrightarrow{\pi_k} M_k$$

are R-module homomorphisms. The restriction of π_k to the direct sum is an onto homomorphism of R-modules $\pi_k : \bigoplus_{i \in I} M_i \to M_k$. We have $\pi_k \iota_k = 1_{M_k}$. The direct sum $\bigoplus_{i \in I} M_i$ is sometimes called the *external direct sum* to distinguish it from the internal direct sum of submodules defined in Definition 1.6.3 below.

If the index set I is $\{1, \dots, n\}$ and $M_1, \dots, M_n$ are R-modules, then the direct product and the direct sum are equal. In this case, the direct sum is sometimes denoted $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

PROPOSITION 1.6.2. *Let R be a ring, I an index set and $\{M_i \mid i \in I\}$ a family of R-modules indexed by I. Let M be an R-module.*

(1) Given any family $\{\psi_i : M \to M_i \mid i \in I\}$ of R-module homomorphisms, there exists a unique R-module homomorphism $\theta : M \to \prod_{i \in I} M_i$ such that for each $j \in I$ the diagram

$$\begin{tikzcd} & \prod_{i \in I} M_i \arrow[d, "\pi_j"] \\ M \arrow[ur, dashed, "\exists \theta"] \arrow[r, "\psi_j"'] & M_j \end{tikzcd}$$

commutes and $\pi_j \theta = \psi_j$.

(2) *Given any family* $\{\phi_i : M_i \to M \mid i \in I\}$ *of* R*-module homomorphisms, there exists a unique* R*-module homomorphism* $\theta : \bigoplus_{i\in I} M_i \to M$ *such that for each* $j \in I$ *the diagram*

$$\begin{tikzcd} \bigoplus_{i\in I} M_i \arrow[dr, dashed, "\exists\theta"] & \\ M_j \arrow[u, "\iota_j"] \arrow[r, "\phi_j"'] & M \end{tikzcd}$$

commutes and $\theta \iota_j = \phi_j$.

PROOF. Part (1) is Exercise 1.6.14 (1). Part (2) is Exercise 1.6.15 (1). $\square$

DEFINITION 1.6.3. Let I be an index set and $\{S_i \mid i \in I\}$ a family of submodules of the R-module M. The submodule of M generated by the set $\bigcup_{i\in I} S_i$ is called the *sum* of the submodules and is denoted $\sum_{i\in I} S_i$. Let $\bigoplus_{i\in I} S_i$ be the external direct sum of the R-modules $\{S_i \mid i \in I\}$. By Proposition 1.6.2 there exists an R-module homomorphism $\phi : \bigoplus_{i\in I} S_i \to M$ defined by $\phi(f) = \sum_{i\in I} f(i)$. Therefore the image of ϕ is equal to the sum $\sum_{i\in I} S_i$. We say that M is the *internal direct sum* of the submodules $\{S_i \mid i \in I\}$ in case ϕ is an isomorphism. In this case we write $M = \bigoplus_{i\in I} S_i$.

Proposition 1.6.4 lists some useful necessary and sufficient conditions for a module M to be the internal direct sum of a family of submodules.

PROPOSITION 1.6.4. *Let* I *be an index set and* $\{S_i \mid i \in I\}$ *a family of submodules of the* R*-module* M*. Then the following are equivalent.*

(1) $M = \bigoplus_{i\in I} S_i$ *is the internal direct sum of the submodules* $\{S_i \mid i \in I\}$.

(2) *For each* $x \in M$ *there is a unique representation of* x *in the form* $x = \sum_{i\in I} x_i$ *where each* x_i *comes from* S_i *and for all but finitely many* $i \in I$ *we have* $x_i = 0$.

(3) *The following are satisfied:*
   (a) $M = \sum_{i\in I} S_i$ *is the sum of the submodules* $\{S_i \mid i \in I\}$*, and*
   (b) *for every finite subset* $\{k_1, \dots, k_n\}$ *of* I*, if* $x_{k_i} \in S_{k_i}$ *for* $1 \le i \le n$*, and* $0 = \sum_{i=1}^n x_{k_i}$*, then* $x_{k_i} = 0$ *for each* i.

(4) *The following are satisfied:*
   (a) $M = \sum_{i\in I} S_i$ *is the sum of the submodules* $\{S_i \mid i \in I\}$*, and*
   (b) *for every* $k \in I$*,* $S_k \cap \sum_{i\in I-\{k\}} S_i = \{0\}$.

DEFINITION 1.6.5. If M is an R-module and N is an R-submodule of M, then N is a *direct summand* of M if there is a submodule L of M such that $M = N \oplus L$.

LEMMA 1.6.6. *Let* R *be a ring,* M *an* R*-module, and* N *an* R*-submodule of* M*. The following are equivalent.*

(1) N *is a direct summand of* M*. That is,* $M = N \oplus L$ *for some submodule* L *of* M.

(2) *There exists* $\pi \in \operatorname{Hom}_R(M,M)$ *such that*
   (a) $\pi^2 = \pi$ *(that is,* π *is idempotent),*
   (b) *for each* $m \in M$*,* $\pi(m) \in N$*, and*
   (c) *for each* $x \in N$*,* $\pi(x) = x$.

(3) *The short exact sequence*

$$0 \to N \to M \to M/N \to 0$$

is split exact.

(4) *There exists* $\phi \in \operatorname{Hom}_R(M,N)$ *such that for each* $x \in N$*,* $\phi(x) = x$.

6.3. Free Modules.

DEFINITION 1.6.7. Let R be any ring. An R-module M is finitely generated if there is a finite subset $\{x_1,\dots,x_n\}$ of M such that $M = Rx_1 + \cdots + Rx_n$. Thus, M is finitely generated if and only if M is equal to the sum of a finite number of cyclic submodules. If M has a finite generating set, then by the Well Ordering Principle, there exists a generating set with minimal cardinality. We call such a generating set a *minimal generating set*. The *rank of* M, written $\operatorname{Rank}(M)$, is defined to be the number of elements in a minimal generating set.

DEFINITION 1.6.8. Let R be a ring and I any index set. For $i \in I$, let $R_i = R$ as R-modules. By Example 1.1.11, R is a left R-module. Denote by R^I the R-module direct sum $\bigoplus_{i\in I} R_i$. If $I = \{1,2,\dots,n\}$, then write $R^{(n)}$ for R^I. Let M be an R-module. We say M is *free* if M is isomorphic to R^I for some index set I. If $X = \{x_1,\dots,x_n\}$ is a finite subset of M, define $\phi_X : R^{(n)} \to M$ by $\phi_X(r_1,\dots,r_n) = r_1x_1 + \dots r_nx_n$. The reader should verify that ϕ_X is an R-module homomorphism. We say X is a *linearly independent set* in case ϕ_X is one-to-one. An arbitrary subset $Y \subseteq M$ is a *linearly independent set* if every finite subset of Y is linearly independent. The function $\delta : I \times I \to \{0,1\}$ defined by

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \tag{6.1}$$

is called the Kronecker *delta function*. The *standard basis* for R^I is $\{e_i \in R^I \mid i \in I\}$ where $e_i(j) = \delta_{ij}$. The reader should verify that the standard basis is a linearly independent generating set for R^I.

LEMMA 1.6.9. *An R-module M is free if and only if there exists a subset $X = \{b_i \mid i \in I\} \subseteq M$ which is a linearly independent generating set for M. A linearly independent generating set is called a* basis *for M.*

PROOF. Given a basis $\{b_i \mid i \in I\}$ define $\phi : R^I \to M$ by $\phi(f) = \sum_{i\in I} f(i)b_i$. This is well defined since $f(i)$ is nonzero on a finite subset of I. Clearly ϕ is a homomorphism. Because X generates M and is linearly independent, the map ϕ is one-to-one and onto. The converse is left to the reader. $\square$

EXAMPLE 1.6.10. We have already seen examples of free modules.

(1) If R is any ring, then the ring of polynomials $R[x]$ is a free R-module and the set $\{1,x,x^2,\dots,x^i,\dots\}$ is a basis.
(2) If R is a commutative ring and $f \in R[x]$ is a monic polynomial of degree n, then the Division Algorithm implies $S = R[x]/(f)$ is a free R-module of rank n. The set $\{1,x,x^2,\dots,x^{n-1}\}$ is a basis.
(3) If R is a commutative ring, G a group, and $R(G)$ the group ring (see Example 1.1.4), then $R(G)$ is a free R module with basis $\{g \mid g \in G\}$.

LEMMA 1.6.11. *Let R be a ring and M an R-module.*

(1) Let F be a free R-module and $\{b_i \mid i \in I\}$ a basis for F. For any function $y : I \to M$, there exists a unique R-module homomorphism $\theta : F \to M$ such that $\theta(b_i) = y_i$ for each $i \in I$ and the diagram

$$\begin{tikzcd} I \arrow[rr, "y"] \arrow[dr, "b"'] & & M \\ & F \arrow[ur, dashed, "\exists\theta"'] & \end{tikzcd}$$

commutes.

(2) *There exists a free R-module F and a surjective homomorphism $F \to M$.*
(3) *M is finitely generated if and only if M is the homomorphic image of a free R-module $R^{(n)}$ for some n.*

DEFINITION 1.6.12. Let R be a ring and M an R-module. We say that M is *of finite presentation* if there exists an exact sequence

$$R^{(m)} \to R^{(n)} \to M \to 0$$

for some m and n.

A *vector space* is a module over a division ring. A submodule of a vector space is called a *subspace*. Elements of a vector space are called a *vectors*. If D is a division ring and V, W are D-vector spaces, then a homomorphism $\phi \in \operatorname{Hom}_D(V,W)$ is called a *linear transformation*. A generating set for V as a D-module is called a *spanning set*.

THEOREM 1.6.13. *Let D be a division ring and V a nonzero vector space over D.*

(1) *Every linearly independent subset of V is contained in a basis for V.*
(2) *If $S \subseteq V$ is a generating set for V, then S contains a basis for V.*
(3) *V is a free D-module.*

PROOF. (3) follows from either (1) or (2).

(1): Let X be a linearly independent subset of V. Let S be the set of all $Y \subseteq V$ such that Y is linearly independent and $X \subseteq Y$. Applying Zorn's Lemma to S, let B be a maximal member. The reader should prove that B is a basis for V.

(2): Let X be a generating set for V over D. Let S be the set of all $Y \subseteq X$ such that Y is linearly independent. Applying Zorn's Lemma to S, let B be a maximal member. The reader should prove that B is a basis for V. □

THEOREM 1.6.14. *Let V be a finitely generated vector space over the division ring D and $B = \{b_1, \dots, b_n\}$ a basis for V.*

(1) *If $Y = \{y_1, \dots, y_m\}$ is a linearly independent set in V, then $m \le n$. We can re-order the elements of B such that $\{y_1, \dots, y_m, b_{m+1}, \dots, b_n\}$ is a basis for V.*
(2) *Every basis for V has n elements.*

Let D be a division ring and V a vector space over D. If V is finitely generated and nonzero, then we define the *dimension* of V, written $\dim_D(V)$, to be the number of elements in a basis for V. If $V = (0)$, set $\dim_D(V) = 0$ and if V is not finitely generated, set $\dim_D(V) = \infty$. If R is a commutative ring and F is a finitely generated free R-module, then by Exercise 1.6.9, any two bases for F have the same number of elements. We define the *rank* of F, written $\operatorname{Rank}_R(F)$, to be the number of elements in a basis for F. This definition of rank agrees with that of Definition 1.6.7, by Exercise 1.6.10.

6.4. Exercises.

EXERCISE 1.6.1. Let R be a ring and M a left R-module. Prove that if I and J are submodules of M, then $\operatorname{annih}_R(I+J) = \operatorname{annih}_R(I) \cap \operatorname{annih}_R(J)$.

EXERCISE 1.6.2. Suppose S is a ring and R is a subring of S. Let I be an index set and view the free R-module R^I as a subset of the free S-module S^I.

(1) Prove that if $X \subseteq R^I$ is a generating set for R^I, then $X \subseteq S^I$ is a generating set for the S-module S^I.

(2) Assume S is commutative, I is finite, and X is a basis for the free R-module R^I. Prove that X is a basis for the free S-module S^I.

EXERCISE 1.6.3. Let R be a ring and

$$0 \to L \to M \to N \to 0$$

an exact sequence of R-modules. Prove:

(1) If M is finitely generated, then N is finitely generated.
(2) If L and N are both finitely generated, then M is finitely generated.

EXERCISE 1.6.4. Let R be a ring and

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

a short exact sequence of R-modules. Prove that the following are equivalent.

(1) f has a left inverse which is an R-module homomorphism. That is, there exists $\phi : M \to L$ such that $\phi f = 1_L$.
(2) g has a right inverse which is an R-module homomorphism. That is, there exists $\psi : N \to M$ such that $g\psi = 1_N$.

EXERCISE 1.6.5. Let R be a ring and

$$0 \to L \to M \to N \to 0$$

a split exact sequence of R-modules. Prove that M is isomorphic to $L \oplus N$ as R-modules.

EXERCISE 1.6.6. Let m and n be positive integers. Let $\eta : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the natural map. If ι is the set inclusion map, show that the sequence

$$0 \to m\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\iota} \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\eta} \mathbb{Z}/m\mathbb{Z} \to 0$$

is an exact sequence of $\mathbb{Z}$-modules. Show that it is split exact if and only if $\gcd(m,n) = 1$.

EXERCISE 1.6.7. Let R be a ring and B an R-module. Suppose $B = B_1 \oplus B_2$ and let $\pi : B \to B_2$ be the projection. Suppose $\sigma : A \to B$ is one-to-one and consider the composition homomorphism $\pi\sigma : A \to B_2$. If $A_1 = \ker(\pi\sigma)$ and $A_2 = \operatorname{im}(\pi\sigma)$, show that there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "\alpha"] \arrow[d, "\sigma_1"'] & A \arrow[r, "\beta"] \arrow[d, "\sigma"] & A_2 \arrow[r] \arrow[d, "\sigma_2"] & 0 \\
0 \arrow[r] & B_1 \arrow[r, "\iota"] & B \arrow[r, "\pi"] & B_2 \arrow[r] & 0
\end{tikzcd}$$

satisfying the following.

(1) α, ι, and σ_2 are the set inclusion maps.
(2) σ_1 is the restriction of σ to A_1.
(3) The two horizontal rows are split exact sequences.

EXERCISE 1.6.8. Let R be a ring. Show that the direct sum of short exact sequences is a short exact sequence. That is, assume J is an index set and that for each $j \in J$ there is an exact sequence

$$0 \to A_j \to B_j \to C_j \to 0$$

of R-modules. Show that the sequence

$$0 \to \bigoplus_{j \in J} A_j \to \bigoplus_{j \in J} B_j \to \bigoplus_{j \in J} C_j \to 0$$

is exact.

EXERCISE 1.6.9. Let R be a commutative ring and F a finitely generated free R-module. Show that any two bases for F have the same number of elements. (Hint: Let $\mathfrak{m}$ be a maximal ideal and consider $F/\mathfrak{m}F$ as a vector space over $R/\mathfrak{m}$.)

EXERCISE 1.6.10. Let D be a division ring, V a nonzero vector space over D, and $B \subseteq V$. Prove that the following are equivalent.

(1) B is a basis for V. That is, B is a linearly independent spanning set for V.
(2) B is a spanning set for V and no proper subset of B is a spanning set for V.

EXERCISE 1.6.11. Let R_1 and R_2 be rings and $R = R_1 \oplus R_2$.

(1) If M_1 and M_2 are left R_1 and R_2-modules respectively, show how to make $M_1 \oplus M_2$ into a left R-module.
(2) If M is a left R-module, show that there are R-submodules M_1 and M_2 of M such that $M = M_1 \oplus M_2$ and for each i, M_i is a left R_i-module. See Corollary 3.4.7 for a version of this when M is a finitely generated projective module over a commutative ring.

EXERCISE 1.6.12. Let G be a group and H a subgroup. For any commutative ring R, let $\theta : R(H) \to R(G)$ be the homomorphism of group rings induced by the set inclusion man $H \to G$ (see Example 1.1.4). Show that $R(G)$ is a free $R(H)$-module.

EXERCISE 1.6.13. Let R be a commutative ring, G a group, and $R(G)$ the group ring (see Example 1.1.4). Let A be an R-algebra and $h : G \to A^*$ a homomorphism from G to the group of units of A. Show that there is a unique homomorphism of R-algebras $\phi : R(G) \to A$ such that $\phi(rg) = rh(g)$ for all $r \in R$ and $g \in G$.

EXERCISE 1.6.14. Let R be a ring, I an index set and $\{M_i \mid i \in I\}$ a family of R-modules. Show that the direct product is the solution to a *universal mapping problem*. For each $j \in I$, let $\pi_j : \prod_{i\in I} M_i \to M_j$ denote the projection homomorphism onto coordinate j.

(1) Suppose X is an R-module and $f_j : X \to M_j$ is an R-module homomorphism for each $j \in I$. Show that there exists a unique R-module homomorphism f such that for each $j \in I$ the diagram

$$\begin{tikzcd} X \arrow[d, dashed, "\exists! f"'] \arrow[dr, "f_j"] & \\ \prod_{i\in I} M_i \arrow[r, "\pi_j"'] & M_j \end{tikzcd}$$

commutes.
(2) Suppose P is an R-module, $p_j : P \to M_j$ is an R-module homomorphism for each $j \in I$, and P satisfies the universal mapping property of Part (1). That is, if X is an R-module and $f_j : X \to M_j$ is an R-module homomorphism for each $j \in I$, then there exists a unique R-module homomorphism φ such that for each $j \in I$ the diagram

$$\begin{tikzcd} X \arrow[d, dashed, "\exists! \varphi"'] \arrow[dr, "f_j"] & \\ P \arrow[r, "p_j"'] & M_j \end{tikzcd}$$

commutes. Prove that $P \cong \prod_{i\in I} M_i$.

EXERCISE 1.6.15. Let R be a ring, I an index set and $\{M_i \mid i \in I\}$ a family of R-modules. In this exercise it is shown that the direct sum is the solution to a *universal mapping problem*. For each $j \in I$, let $\iota_j : M_j \to \bigoplus_{i\in I} M_i$ denote the injection homomorphism into coordinate j.

(1) Suppose X is an R-module and that for each $j \in I$ there is an R-module homomorphism $f_j : M_j \to X$. Show that there exists a unique R-module homomorphism f such that for each $j \in I$ the diagram

$$\begin{tikzcd} M_j \arrow[r, "\iota_j"] \arrow[dr, "f_j"'] & \bigoplus_{i\in I} M_i \arrow[d, dashed, "\exists! f"] \\ & X \end{tikzcd}$$

commutes.

(2) Suppose S is an R-module, $\lambda_j : M_j \to S$ is an R-module homomorphism for each $j \in I$, and S satisfies the universal mapping property of Part (1). That is, if X is an R-module and $f_j : M_j \to X$ is an R-module homomorphism for each $j \in I$, then there exists a unique R-module homomorphism φ such that for each $j \in I$ the diagram

$$\begin{tikzcd} M_j \arrow[r, "\lambda_j"] \arrow[dr, "f_j"'] & S \arrow[d, dashed, "\exists! \varphi"] \\ & X \end{tikzcd}$$

commutes. Prove that $S \cong \bigoplus_{i\in I} M_i$.

EXERCISE 1.6.16. Let R be a ring, and M an R-module with submodules S and T. Show that if $S+T = M$, then there is an isomorphism of R-modules $S \oplus T \cong M \oplus S \cap T$.

EXERCISE 1.6.17. Let R be a commutative ring. Show that if I and J are comaximal ideals in R, then there is an isomorphism of R-modules $I \oplus J \cong R \oplus IJ$.

7. Matrix Theory

7.1. The Characteristic Polynomial.

DEFINITION 1.7.1. Let R be any ring, M a free R-module of rank m and N a free R-module of rank n. Let $X = \{x_1,\dots,x_m\}$ be a basis for M and $Y = \{y_1,\dots,y_n\}$ a basis for N. Given $\phi \in \operatorname{Hom}_R(M,N)$, ϕ maps $x_j \in X$ to a linear combination of Y. That is,

$$\phi(x_j) = \sum_{i=1}^{n} \phi_{ij} y_i$$

where the elements ϕ_{ij} are in R. The *matrix of ϕ with respect to the bases X and Y* is defined to be $M(\phi,X,Y) = (\phi_{ij})$, which is a matrix in $M_{nm}(R)$. Matrix multiplication agrees with composition of functions, provided the matrices are treated as having entries from the opposite ring R^o. That is, if P is a free R-module with basis $Z = \{z_1,\dots,z_p\}$ and $\psi \in \operatorname{Hom}_R(N,P)$, then

$$M(\psi\phi,X,Z) = M(\psi,Y,Z)M(\phi,X,Y),$$

provided the matrix multiplication takes place over the ring R^o.

In Proposition 1.7.2, by e_{ij} we denote the elementary matrix in $M_{nm}(R)$ with 1 in position (i,j) and 0 elsewhere.

PROPOSITION 1.7.2. *Let R be any ring.*

(1) *$M_{nm}(R)$ is a free R-module of rank nm, the set $\{e_{ij} \mid 1 \le i \le n, 1 \le j \le m\}$ is a basis.*
(2) *If M is a free R-module of rank m with basis X, and N is a free R-module of rank n with basis Y, then there is a $\mathbb{Z}$-module isomorphism $\operatorname{Hom}_R(M,N) \cong M_{nm}(R)$ defined by $\phi \mapsto M(\phi, X, Y)$. If R is a commutative ring, then this is an R-module isomorphism and $\operatorname{Hom}_R(M,N)$ is a free R-module of rank mn.*
(3) *There is an isomorphism of rings $\operatorname{Hom}_R(M,M) \cong M_n(R^o)$. If R is commutative, this is an isomorphism of R-algebras.*

DEFINITION 1.7.3. Let R be a commutative ring and M and N two R-modules. For $n \ge 1$, let $M^n = M \oplus \cdots \oplus M$ denote the direct sum of n copies of M. An *alternating multilinear form* is a function $f : M^n \to N$ satisfying the following two properties.

(1) For each coordinate i, f is R-linear. That is,

$$f(x_1, \dots, x_{i-1}, \alpha u + \beta v, x_{i+1}, \dots, x_n) = \\ \alpha f(x_1, \dots, x_{i-1}, u, x_{i+1}, \dots, x_n) + \beta f(x_1, \dots, x_{i-1}, v, x_{i+1}, \dots, x_n).$$

(2) $f(x_1, , \dots, x_n) = 0$ whenever $x_i = x_j$ for some pair $i \ne j$.

DEFINITION 1.7.4. The *determinant* of the matrix $A = (a_{ij}) \in M_n(R)$ is

$$\det(A) = \det(a_{ij}) = \sum_{\vec{j} \in S_n} \operatorname{sign}(\vec{j}) a_{j_1,1} \cdots a_{j_n,n}.$$

By viewing the columns of a matrix in $M_n(R)$ as vectors in R^n, we identify $M_n(R)$ with $(R^n)^n$. By [**19**, Lemma 6.3.2], the determinant function is the unique alternating multilinear form $\det : M_n(R) \to R$ such that $\det(I_n) = 1$.

For $A \in M_n(R)$, let A_{ij} be the matrix in $M_{n-1}(R)$ obtained by deleting row i and column j from A. Then $\det(A_{ij})$ is called the *minor* of A in position (i, j) and $(-1)^{i+j} \det(A_{ij})$ is called the *cofactor* of A in position (i, j).

LEMMA 1.7.5. *If A is a matrix in $M_n(R)$, then the following are true.*

(1) *If $B \in M_n(R)$, then $\det(AB) = \det(A)\det(B)$.*
(2) *A is invertible if and only if $\det(A)$ is a unit in R.*
(3) *For each row i, $\det(A) = \sum_{j=1}^n a_{ij}(-1)^{i+j} \det(A_{ij})$.*
(4) *For each column j, $\det(A) = \sum_{i=1}^n a_{ij}(-1)^{i+j} \det(A_{ij})$.*

It follows from Lemma 1.7.5 that the determinant is constant on similarity classes of matrices. By Proposition 1.7.2, we define the determinant of an endomorphism $\phi \in \operatorname{Hom}_R(M,M)$, if M is a finitely generated free R-module.

DEFINITION 1.7.6. Let R be a commutative ring and $M \in M_n(R)$. If x is an indeterminate, then we can view M as a matrix in $M_n(R[x])$. The *characteristic polynomial* of M is $\operatorname{char.poly}_R(M) = \det(xI_n - M)$, which is a polynomial in $R[x]$. Computing the determinant using row expansion along row one, it is easy to see that $\operatorname{char.poly}_R(M)$ is monic and has degree n. The characteristic polynomial is constant on similarity classes. If P is a finitely generated free R-module and $\phi \in \operatorname{Hom}_R(P,P)$, then the characteristic polynomial of ϕ is defined to be the characteristic polynomial of the matrix of ϕ with respect to any basis of P. If A is an R-algebra which is free of finite rank and $\alpha \in A$, then we have the left regular representation $\lambda_A : A \to \operatorname{Hom}_R(A,A)$ of A as a ring of R-module homomorphisms of A (see Example 1.1.13). Under λ_A, the element $\alpha \in A$ is mapped to λ_α, which is "left multiplication by α". The characteristic polynomial of α is defined to be the characteristic polynomial of λ_α.

THEOREM 1.7.7. *(Cayley-Hamilton Theorem) Let R be a commutative ring, M an n-by-n matrix over R, and $p(x) = \mathrm{char.poly}_R(M)$ the characteristic polynomial of M. Then $p(M) = 0$.*

DEFINITION 1.7.8. Let R be any ring and let M and N be left R-modules. Given two homomorphisms f, g in $\mathrm{Hom}_R(M,N)$, we say f and g are *equivalent*, if there exist automorphisms $\phi \in \mathrm{Hom}_R(N,N)$ and $\psi \in \mathrm{Hom}_R(M,M)$ such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \psi\big\downarrow & & \big\downarrow\phi \\ M & \xrightarrow{g} & N \end{array}$$

commutes. It is routine to check that equivalence of matrices defines an equivalence relation on $\mathrm{Hom}_R(M,N)$.

Lemma 1.7.9 is a very special case of the Five Lemma (Theorem 2.5.1).

LEMMA 1.7.9. *Let R be a ring and let M and N be left R-modules. If f and g are equivalent homomorphisms in $\mathrm{Hom}_R(M,N)$, then $\ker f \cong \ker g$, $\operatorname{im} f \cong \operatorname{im} g$, and $\operatorname{coker} f \cong \operatorname{coker} g$.*

PROOF. There exist automorphisms $\phi \in \mathrm{Hom}_R(N,N)$ and $\psi \in \mathrm{Hom}_R(M,M)$ such that $\phi f = g\psi$. Therefore, ψ maps $\ker f$ isomorphically onto $\ker g$, and ϕ maps $\operatorname{im} f$ isomorphically onto $\operatorname{im} g$. The composition

$$N \xrightarrow{\phi} N \xrightarrow{\eta} \operatorname{coker} g$$

is onto and the kernel is equal to $\operatorname{im} f$. By Theorem 1.1.12, $\eta\phi$ factors through $\operatorname{coker} f$ giving the isomorphism $\operatorname{coker} f \cong \operatorname{coker} g$. $\square$

DEFINITION 1.7.10. Let R be a commutative ring. Two matrices A, B in $M_{nm}(R)$ are said to be *equivalent* if there exist invertible matrices $Q_l \in M_n(R)$ and $Q_r \in M_m(R)$ such that $B = Q_l A Q_r$. It is routine to check that equivalence of matrices defines an equivalence relation on $M_{nm}(R)$. As in Proposition 1.7.2, multiplication from the left by A and B define homomorphisms ϕ_A, ϕ_B in $\mathrm{Hom}_R(R^m, R^n)$. Hence A and B are equivalent matrices if and only if ϕ_A and ϕ_B are equivalent homomorphisms in the sense of Definition 1.7.8.

DEFINITION 1.7.11. Let R be a commutative ring and A a nonzero n-by-m matrix in $M_{nm}(R)$. Let e_{ij} be the elementary matrix in $M_n(R)$ with 1 in position (i,j) and 0 elsewhere. If $(a_1,\dots,a_n) \in R^n$, then $\mathrm{diag}(a_1,\dots,a_n)$ denotes the diagonal matrix $a_1e_{11} + \cdots + a_ne_{nn}$. In particular, $I = \mathrm{diag}(1,\dots,1)$ is the identity matrix in $M_n(R)$. The three types of *elementary row operations* on A are defined below where matrices multiplied from the left are in $M_n(R)$.

(1) Multiplication of a row by a unit. Let $u \in R^*$ be a unit in R and denote by $L_i(u)$ the diagonal matrix $\mathrm{diag}(1,\dots,u,\dots,1)$ with u in row i and 1 on the rest of the diagonal. Clearly, $L_i(u)$ is invertible with inverse $L_i(u^{-1})$ and the product $L_i(u)A$ is the matrix obtained by multiplying row i of A by u.
(2) Adding a scalar multiple of row j to row i. If $i \neq j$, let $\Delta_{ij}(v) = I + ue_{ij}$, where $v \in R$. Then $\Delta_{ij}(v)\Delta_{ij}(-v) = (I + ue_{ij})(I - ue_{ij}) = I$ (see [**19**, Example 6.1.5]). Therefore, $\Delta_{ij}(v)$ is invertible with inverse $\Delta_{ij}(-v)$. The product $\Delta_{ij}(v)A$ is the matrix obtained by adding v times row j of A to row i.

(3) Switch rows i and j. If $i \neq j$, let T_{ij} denote the matrix obtained by switching rows i and j of I. Clearly $T_{ij}^2 = I$ and the product $T_{ij}A$ is the matrix obtained by switching rows i and j of A.

An elementary row operation on A corresponds to multiplication by an invertible matrix, hence results in a matrix that is equivalent to A.

DEFINITION 1.7.12. In the notation of Definition 1.7.11, the three types of *elementary column operations* on A are defined below where matrices multiplied from the right are in $M_m(R)$:

(1) Multiplication of a column by a unit. The product $AL_j(u)$ is the matrix obtained by multiplying column j of A by u.
(2) Adding a scalar multiple of column i to column j. The product $A\Delta_{ij}(v)$ is the matrix obtained by adding v times column i of A to column j.
(3) Switch columns i and j. The product AT_{ij} is the matrix obtained by switching columns i and j of A.

An elementary column operation on A corresponds to multiplication by an invertible matrix, hence results in a matrix that is equivalent to A.

7.2. Modules over a Principal Ideal Domain.

DEFINITION 1.7.13. Let R be an integral domain and M an R-module. If $x \in M$, then we say x is a *torsion element* of M in case there exists a nonzero $r \in R$ such that $rx = 0$. If every element of M is torsion, then we say M is torsion. Since R is an integral domain, the set of all torsion elements in M is a submodule of M, which is denoted M_t. If $M_t = 0$, then we say M is *torsion free*.

Let R be a principal ideal domain (or PID for short) and M a finitely generated R-module. If $r \in R$, then the "left multiplication by r" map is denoted by $\ell_r : M \to M$, and is defined by $\ell_r(x) = rx$. Then ℓ_r is an R-module homomorphism. Let π be a prime element in R and n a positive integer. The kernel of ℓ_{π^n} is contained in the kernel of $\ell_{\pi^{n+1}}$. Therefore the union $M(\pi) = \bigcup_{n>0} \ker(\ell_{\pi^n})$ is a submodule of M. If $x \in M$, then there is an R-module homomorphism $\theta_x : R \to M$ defined by $\theta_x(r) = rx$. The kernel of θ_x is a principal ideal Ra, for some $a \in R$ and we call a the *order of x*. The order of x is unique up to associates in R.

Proofs of Theorems 1.7.14, 1.7.15, 1.7.16, and 1.7.17 can be found in [**19**, Section 4.6].

THEOREM 1.7.14. *Let R be a PID and M a nonzero finitely generated R-module. If M is free and S is a submodule, then* $\operatorname{Rank}(S) \le \operatorname{Rank}(M)$. *The following are equivalent.*

(1) M is torsion free.
(2) M is free.
(3) Every nonzero submodule of M is free.

THEOREM 1.7.15. *If R is a PID and M a finitely generated R-module, then there is a finitely generated free submodule F such that M is the internal direct sum $M = F \oplus M_t$. The rank of F is uniquely determined by M.*

THEOREM 1.7.16. *(Basis Theorem – Elementary Divisor Form) Let R be a PID and M a finitely generated torsion R-module.*

(1) $M = \bigoplus_\pi M(\pi)$ where π runs through a finite set of primes in R.
(2) For each prime π such that $M(\pi) \neq 0$, there exists a basis $\{a_1, \dots, a_m\}$ such that $M(\pi) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_m$ where the order of a_i is equal to π^{e_i} and $e_1 \ge e_2 \ge \cdots \ge e_m$.

(3) M is uniquely determined by the primes π that occur in (2) and the integers e_i that occur in (3).

The prime powers π^{e_i} that occur are called the elementary divisors *of M.*

THEOREM 1.7.17. *(Basis Theorem – Invariant Factor Form) Let R be a PID and M a finitely generated torsion R-module. The following are true. There exist $r_1,\dots,r_\ell \in R$ such that $r_1 \mid r_2 \mid r_3 \mid \cdots \mid r_\ell$ and*

$$M \cong R/(r_1R) \oplus \cdots \oplus R/(r_\ell R).$$

The integer ℓ is uniquely determined by M. Up to associates in R, the elements r_i are uniquely determined by M. The elements $r_1,\dots,r_\ell$ are called the invariant factors *of M.*

LEMMA 1.7.18. *Let R be a principal ideal domain and $A = (a_{ij})$ a nonzero matrix in $M_{nm}(R)$. Then A is equivalent to a matrix $B = (b_{ij})$ such that b_{11} divides every other entry of B.*

PROOF. As in Example 1.5.7, let $\nu(x)$ be the number of factors in a prime factorization of x. Now let $V = \{\nu(x) \mid x \text{ is an entry in a matrix that is equivalent to } A\}$. Let $\nu(\alpha)$ be the minimum in V and $B = (b_{ij})$ a matrix that is equivalent to A such that α is an entry in B. By multiplying B from the left and right by appropriate matrices T_{1i} and T_{1j}, we can assume $\alpha = b_{11}$. We prove that α divides every entry in B. For sake of contradiction, assume not. So α is not a unit and there is some b_{ij} in B such that α does not divide b_{ij}. There are three cases. Because the statement of the theorem depends only on the equivalence class of B, throughout the proof we will repetitively replace B with a matrix that is obtained from B by an elementary row or column operation.

Case 1: $j = 1$. After multiplying by T_{2i} we assume α does not divide b_{21}. By [**19**, Corollary 3.4.9], let $d = \gcd(\alpha, b_{21})$ and write $d = \alpha x + b_{21}y$. If $u = \alpha/d$ and $v = b_{21}/d$, then $1 = ux + vy$. Notice

$$\begin{bmatrix} x & y \\ -v & u \end{bmatrix} \begin{bmatrix} u & -y \\ v & x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

shows that the matrix $\begin{bmatrix} x & y \\ -v & u \end{bmatrix}$ is invertible. If we set

$$C = \left(\begin{bmatrix} x & y \\ -v & u \end{bmatrix} \oplus I \right) B = (c_{ij})$$

then $c_{11} = d$. But d is a proper factor of α, C is a matrix that is equivalent to B and B is equivalent to A. Therefore, this is a contradiction to the choice of α.

Case 2: Suppose α divides column one of B, but there is some b_{1j} that is not a multiple of α. Transposing all of the row and column arguments of Case 1 shows B is equivalent to a matrix $C = (c_{ij})$ and $\nu(c_{11}) < \nu(\alpha)$, a contradiction.

Case 3: Suppose α divides every entry in column one and row one of B. Factoring α from each entry in column one, we write $a_{i1} = \alpha b_i$ for $2 \le i \le n$. Likewise, factoring row one, we have $a_{1j} = \alpha c_j$ for $2 \le j \le m$. Eliminate all nonzero entries below the diagonal in column one and to the right of the diagonal in row one by the matrix product:

$$C = \Delta_{21}(-b_2)\cdots\Delta_{n1}(-b_n)B\Delta_{12}(-c_2)\cdots\Delta_{1m}(-c_m).$$

Then C is the matrix direct sum $(\alpha) \oplus C_1$ where C_1 is an $(n-1)$-by-$(m-1)$ matrix over R. Moreover, since α does not divide B we know α does not divide C_1. There is some c_{ij} in C such that $1 < i \le n$, $1 < j \le m$ and α does not divide c_{ij}. Then $C\Delta_{j1}(1)$ is equivalent to C and has an entry in column one that is not a multiple of α. By Case 1 applied to $C\Delta_{j1}(1)$, we get a contradiction. $\square$

THEOREM 1.7.19. *(Smith Normal Form) Let R be a principal ideal domain and $A = (a_{ij})$ a nonzero matrix in $M_{nm}(R)$. Then A is equivalent to a matrix of the form* $\operatorname{diag}(d_1, d_2, \dots, d_r) \oplus 0$ *where $d_1, \dots, d_r$ are nonzero elements of R and $d_1 \mid d_2 \mid \cdots \mid d_r$. The matrix* $\operatorname{diag}(d_1, d_2, \dots, d_r) \oplus 0$ *is called the* Smith normal form *of A.*

PROOF. Inductively assume $m \geq 1$, $n \geq 1$, and that the result holds for any matrix over R of size $(n-1)$-by-$(m-1)$. Because the statement of the theorem depends only on the equivalence class of A, throughout the proof we will repetitively replace A with a matrix that is equivalent to A. For instance, by Lemma 1.7.18, we can assume entry a_{11} in A divides all other entries in A. Use the method of Case 3 in the proof of Lemma 1.7.18 to eliminate all nonzero entries below the diagonal in column one and to the right of the diagonal in row one. Call the new matrix B. Then B is the matrix direct sum $(a_{11}) \oplus B_1$ where B_1 is an $(n-1)$-by-$(m-1)$ matrix over R. If $m = 1$ or $n = 1$ or B_1 is a zero matrix, then we are done and B is the Smith normal form of A. This proves the basis step for an induction proof. Otherwise, B_1 is a nonzero matrix and a_{11} divides every entry in B_1. By the induction hypothesis applied to B_1, there exist invertible matrices Q_l of rank $n-1$ and Q_r of rank $m-1$ such that $Q_l B_1 Q_r = \operatorname{diag}(d_2, \dots, d_r) \oplus 0$ is in Smith normal form. Moreover, a_{11} divides the diagonal entries $d_2, \dots, d_r$ since a_{11} divides all entries of B_1. Set $P_l = (1) \oplus Q_l$ and $P_r = (1) \oplus Q_r$. Then $P_l B P_r$ is in Smith normal form with $d_1 = a_{11}$ in the upper left position. □

COROLLARY 1.7.20. *Let R be a principal ideal domain, F a free R-module of rank n, and S a submodule of F. Then there exist a basis $\{y_1, \dots, y_n\}$ of F and nonzero elements $d_1, \dots, d_r$ in R satisfying the following.*

(1) (Simultaneous Bases Theorem) $\{d_1 y_1, d_2 y_2, \dots, d_r y_r\}$ is a free basis for S.
(2) $d_1 \mid d_2 \mid \cdots \mid d_r$.
(3) The elements in the list $d_1, \dots, d_r$ that are not units are precisely the invariant factors of the quotient module F/S.
(4) The elements $d_1, \dots, d_r$ are uniquely determined up to associates by S and F.

PROOF. (1) and (2): By Theorem 1.7.14, S is a finitely generated free R-module. Let $\{s_1, \dots, s_m\}$ be a generating set for S and $\{u_1, \dots, u_n\}$ a basis for F. For $1 \leq j \leq m$ write $s_j = \sum_{i=1}^{n} a_{ij} u_i$ and set $A = (a_{ij})$ the associated matrix in $M_{nm}(R)$. Let $\phi_A : R^m \to F$ be the homomorphism defined by left multiplication by A. The image of ϕ_A is the column space of A, which is equal to the submodule S. By Theorem 1.7.19, there exist bases $X = \{x_1, \dots, x_m\}$ for R^m and $Y = \{y_1, \dots, y_n\}$ for F such that the matrix $M(\phi_A, X, Y)$ is in Smith normal form $\operatorname{diag}(d_1, \dots, d_r) \oplus 0$. This means $\{d_1 y_1, \dots, d_r y_r\}$ is a basis for S.

(3) and (4): By (1),

$$F/S \cong \frac{Ry_1}{Rd_1 y_1} \oplus \frac{Ry_2}{Rd_2 y_2} \oplus \cdots \oplus \frac{Ry_r}{Rd_r y_r} \oplus Ry_{r+1} \oplus \cdots \oplus Ry_n.$$

The R-module $\frac{Ry_i}{Rd_i y_i}$ is nonzero if and only if d_i is not a unit. If $d_q, \dots, d_r$ are the nonunits, then the torsion submodule of F/S is isomorphic to $R/Rd_q \oplus \cdots \oplus RRd_r$. By Theorem 1.7.17, the elements $d_q, \dots, d_r$ are the invariant factors of F/S. The numbers q and r are uniquely determined by F/S. Up to associates the elements $d_1, \dots, d_r$ are uniquely determined by F/S. □

COROLLARY 1.7.21. *Let R be a principal ideal domain and A a nonzero matrix in $M_{nm}(R)$. If $D = \operatorname{diag}(d_1, \dots, d_r) \oplus 0$ and $E = \operatorname{diag}(e_1, \dots, e_s) \oplus 0$ are two matrices in Smith normal form such that A is equivalent to both D and E, then $r = s$ and for each i the elements d_i and e_i are associates.*

PROOF. This follows from Corollary 1.7.20 and Lemma 1.7.9. $\square$

7.3. Block Matrices. The main result of this section is Theorem 1.7.23 which is a determinant formula for a matrix A in $M_{mn}(R)$, where A is viewed as a matrix in $M_m(M_n(R))$. Such a matrix is called a *block matrix*. The theorem and its proof are from [**56**]. We begin by fixing some notation and establishing the context of the theorem. Let R be a commutative ring and S a commutative R-subalgebra of $M_n(R)$. We view $M_{mn}(R)$ as the ring of m-by-m matrices over $M_n(R)$. Thus, a matrix M in $M_m(S)$ can be viewed as a matrix in $M_{mn}(R)$. We have the lattice of R-algebras

$$\begin{tikzcd} M_m(S) \arrow[r] & M_{mn}(R) \\ S \arrow[u] \arrow[r] & M_n(R) \arrow[u] \\ R \arrow[u] \arrow[ur] & \end{tikzcd} \tag{7.1}$$

where an arrow denotes subring. When M is viewed as a matrix in $M_m(S)$, the determinant is denoted $\det_S(M)$. By $\det_R(M)$ we denote the determinant when M is viewed as a matrix with entries in R. In the context of (7.1), there are three such determinant maps

$$\begin{tikzcd} M_m(S) \arrow[rr, "\subseteq"] \arrow[d, "\det_S"'] & & M_{mn}(R) \arrow[d, "\det_R"] \\ S \arrow[r, "\subseteq"] & M_n(R) \arrow[r, "\det_R"] & R \end{tikzcd} \tag{7.2}$$

and the purpose of Theorem 1.7.23 below is to show that (7.2) is a commutative diagram.

EXAMPLE 1.7.22. Let R be a commutative ring and x an indeterminate. If $n \geq 1$ and $M_n(R)$ is the ring of n-by-n matrices over R, then we can identify the ring of polynomials over $M_n(R)$ with the ring of matrices over $R[x]$. That is,

$$M_n(R)[x] = M_n(R[x]).$$

In fact, given a polynomial $f = \sum_{i=0}^m A_i x^i$ in the left-hand side, we can view $x^i = x^i I_n$ as a matrix, and $f = \sum_{i=0}^m A_i(x^i I_n)$ is an element of the right-hand side. Conversely, if $M = (f_{ij})$ is in the right-hand side, then we can write each polynomial f_{ij} in the form $f_{ij} = \sum_{k\geq 0} a_{ijk}x^k$ where it is understood that only a finite number of the coefficients are nonzero. For a fixed $k \geq 0$, let M_k be the matrix (a_{ijk}). Then M is equal to the polynomial $M = \sum_{k\geq 0} M_k x^k$ in the left-hand side.

THEOREM 1.7.23. *In the above context, the following are true for any matrix A in* $M_m(S)$.

(1) $\det_R(A) = \det_R(\det_S(A))$. *In other words, diagram* (7.2) *commutes.*
(2) $\operatorname{char.poly}_R(A) = \det_{R[x]}(\operatorname{char.poly}_S(A))$.

PROOF. Part (2) follows from (1). The proof of (1) is by induction on m. If $m = 1$, then $\det_S$ is the identity map and there is nothing to prove. Assume $m \geq 1$ and that the determinant formula of the theorem holds for every matrix in $M_m(S)$. Let $A = (a_{ij})$ be a matrix in $M_{m+1}(S)$. Partition A into four blocks

$$A = \begin{bmatrix} a_{11} & \dots & a_{1m} & a_{1,m+1} \\ \vdots & \vdots & \vdots & \\ a_{m1} & \dots & a_{mm} & a_{m,m+1} \\ a_{m+1,1} & \dots & a_{m+1,m} & a_{m+1,m+1} \end{bmatrix} = \begin{bmatrix} A_0 & B \\ C & D \end{bmatrix}$$

where A_0 is the m-by-m matrix obtained by deleting row $m+1$ and column $m+1$ from M, B is the m-by-1 column matrix $(a_{1,m+1},\dots,a_{m,m+1})^t$, C is the 1-by-m row matrix $(a_{m+1,1},\dots,a_{m+1,m})$, and $D=(d)$ is the 1-by-1 matrix $(a_{m+1,m+1})$.

To prove the determinant formula for the matrix A, we use what can be viewed as a "homotopy trick". Let x be an indeterminate. As in Example 1.7.22, we view the ring $M_{mn}(R)$ as the subring of $M_{mn}(R[x])$ corresponding to the polynomials in x of degree 0. Likewise $M_m(S)$ is a subring of $M_m(S[x])$. Let $\theta : R[x] \to R$ be the evaluation homomorphism defined by $x \mapsto 0$. By [**19**, Exercise 6.3.21], the diagram

$$\begin{tikzcd} M_n(R[x]) \arrow[r, "\theta"] \arrow[d, "\det_{R[x]}"'] & M_n(R) \arrow[d, "\det_R"] \\ R[x] \arrow[r, "\theta"] & R \end{tikzcd} \tag{7.3}$$

commutes. The counterpart of (7.3) with S instead of R also commutes. The strategy is to replace A with a matrix A_x in the ring $M_{m+1}(S[x])$ such that $\theta(A_x)=A$ and show that the equation

$$\det_{R[x]}(A_x) = \det_{R[x]}\left(\det_{S[x]}(A_x)\right) \tag{7.4}$$

holds in the ring $R[x]$. The equation

$$\det_R(A) = \det_R(\det_S(A)) \tag{7.5}$$

then follows from (7.3) and (7.4).

Let A_x be the matrix $\begin{bmatrix} A_0 & B \\ C & (d+x) \end{bmatrix}$ obtained by adding x to the entry in position $m+1,m+1$ of A. Then A_x is in the ring $M_{m+1}(S[x])$ and $\theta(A_x)=A$. The equation

$$\begin{bmatrix} A_0 & B \\ C & (d+x) \end{bmatrix} \begin{bmatrix} (d+x)I_m & 0 \\ -C & (1) \end{bmatrix} = \begin{bmatrix} (d+x)A_0 - BC & B \\ 0 & (d+x) \end{bmatrix} \tag{7.6}$$

holds in the ring $M_{m+1}(S[x])$. Taking determinants in (7.6), we use Lemma 1.7.5 to get the equation

$$\det_{S[x]}(A_x)(d+x)^m = \det_{S[x]}\left((d+x)A_0 - BC\right)(d+x) \tag{7.7}$$

in the ring $S[x]$. The equation (7.7) holds in the ring $M_n(R[x])$, and taking determinants we get the equation

$$\det_{R[x]}\left(\det_{S[x]}(A_x)\right)\det_{R[x]}(d+x)^m = \det_{R[x]}\left(\det_{S[x]}((d+x)A_0 - BC)\right)\det_{R[x]}(d+x) \tag{7.8}$$

in the ring $R[x]$. The equation (7.6) holds in the ring $M_{mn}(R[x])$, and taking determinants we get the equation

$$\det_{R[x]}(A_x)\det_{R[x]}(d+x)^m = \det_{R[x]}\left((d+x)A_0 - BC\right)\det_{R[x]}(d+x) \tag{7.9}$$

in the ring $R[x]$. By induction on m, we have

$$\det_{R[x]}\left((d+x)A_0 - BC\right) = \det_{R[x]}\left(\det_{S[x]}\left((d+x)A_0 - BC\right)\right)$$

which implies the right hand side of (7.9) is equal to the right hand side of (7.8). Equating the left hand sides of (7.9) and (7.8), we get the equation

$$\det_{R[x]}(A_x)\det_{R[x]}(d+x)^m = \det_{R[x]}\left(\det_{S[x]}(A_x)\right)\det_{R[x]}(d+x)^m \tag{7.10}$$

in $R[x]$. But $\det_{R[x]}(d+x)$ is a monic polynomial of degree n, hence is not a zero divisor. Canceling in (7.10) yields the equation (7.4) in $R[x]$. From (7.4) we get (7.5), and this completes the induction proof. □

PROPOSITION 1.7.24. *Let R be a commutative ring and assume A, B, C, D are matrices in $M_n(R)$. Let $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. Then M is a block matrix in $M_{2n}(R)$.*

(1) If $AC = CA$, then $\det(M) = \det(AD - CB)$.
(2) If $CD = DC$, then $\det(M) = \det(AD - BC)$.
(3) If $BD = DB$, then $\det(M) = \det(DA - BC)$.
(4) If $AB = BA$, then $\det(M) = \det(DA - CB)$.

PROOF. (1): The proof is based on the commutative diagram (7.3). We replace M with the matrix $M_x = \begin{bmatrix} A + xI_n & B \\ C & D \end{bmatrix}$ which is in the ring $M_{2n}(R[x])$. Notice that $\theta(M_x) = M$. Since $AC = CA$, the equation

$$\begin{bmatrix} I_n & 0 \\ -C & A + xI_n \end{bmatrix} \begin{bmatrix} A + xI_n & B \\ C & D \end{bmatrix} = \begin{bmatrix} A + xI_n & B \\ 0 & AD - CB + xD \end{bmatrix} \tag{7.11}$$

holds in the ring $M_{2n}(R[x])$. Take determinants in (7.11). Using Lemma 1.7.5 and Exercise 1.7.3, the equation

$$\det(A + xI_n)\det(M_x) = \det(A + xI_n)\det(AD - CB + xD) \tag{7.12}$$

holds in the ring $R[x]$. Now $\det(A + xI_n)$ is a monic polynomial of degree n, hence is not a zero divisor in $R[x]$. Therefore, (7.12) yields the polynomial identity

$$\det(M_x) = \det(AD - CB + xD) \tag{7.13}$$

in which both sides are polynomials of degree n. By the commutative diagram (7.3), evaluating (7.13) at $x = 0$ yields the formula $\det(M) = \det(AD - CB)$.

The proofs of (2), (3), and (4) are similar and left to the reader. □

7.4. Exercises.

EXERCISE 1.7.1. Let R be a commutative ring and M a finitely generated free R-module of rank n. Let $\phi \in \operatorname{Hom}_R(M, M)$. Show that if $\operatorname{char.poly}_R(\phi) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then $\operatorname{trace}(\phi) = -a_{n-1}$ and $\det(\phi) = (-1)^n a_0$.

EXERCISE 1.7.2. Let R be a commutative ring and suppose A is an R-algebra which is finitely generated and free of rank n as an R-module. We have $\theta : A \to \operatorname{Hom}_R(A, A)$, the left regular representation of A in $\operatorname{Hom}_R(A, A)$ which is defined by $\alpha \mapsto \ell_\alpha$. Define $T_R^A : A \to R$ by the assignment $\alpha \mapsto \operatorname{trace}(\ell_\alpha)$. We call T_R^A the *trace from A to R*. Define $N_R^A : A \to R$ by the assignment $\alpha \mapsto \det(\ell_\alpha)$. We call N_R^A the *norm from A to R*.

(1) Show that $T_R^A(r\alpha + s\beta) = rT_R^A(\alpha) + sT_R^A(\beta)$, if $r, s \in R$ and $\alpha, \beta \in A$.
(2) Show that $N_R^A(\alpha\beta) = N_R^A(\alpha)N_R^A(\beta)$ and $N_R^A(r\alpha) = r^n N_R^A(\alpha)$, if $r \in R$ and $\alpha, \beta \in A$.

EXERCISE 1.7.3. Let R be a commutative ring, $m \geq 1$, and $n \geq 1$. Let $A \in M_m(R)$ and $D \in M_n(R)$. Let M be a block triangular matrix of the form $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ or $\begin{bmatrix} A & 0 \\ C & D \end{bmatrix}$. Show that $\det(M) = \det(A)\det(D)$. (Hint: Use induction on m and Lemma 1.7.5.)

EXERCISE 1.7.4. Let S be a commutative R-algebra that is a finitely generated free R-module of rank n. Let A be an S-algebra that is a finitely generated free S-module of rank m. Then for any $a \in A$,

(1) $T_R^A(a) = T_R^S\left(T_S^A(a)\right)$, and
(2) $N_R^A(a) = N_R^S\left(N_S^A(a)\right)$.

See Exercise 1.7.2 for the definition of the trace and norm functions. (Hint: After choosing free bases for A and S, reduce this to statements about block matrices over R. Prove (1) directly and for (2) apply Theorem 1.7.23.)

EXERCISE 1.7.5. Let R be any ring, M and N finitely generated R-modules, and $\phi \in \operatorname{Hom}_R(M,N)$.

(1) Show that there exist positive integers m and n, epimorphisms $f : R^m \to M$, $g : R^n \to N$, and $\theta \in \operatorname{Hom}_R(R^m, R^n)$ such that the diagram

$$\begin{tikzcd} R^m \arrow[r, "\theta"] \arrow[d, "f"'] & R^n \arrow[d, "g"] \\ M \arrow[r, "\phi"] & N \end{tikzcd}$$

commutes. Therefore, given generators for M and N, ϕ can be represented as a matrix.

(2) Show that there exists a monic polynomial $p(x) \in R[x]$ such that $p(\phi) = 0$. (Hint: Apply the Cayley-Hamilton Theorem to the map θ.)

8. Finitely Generated Field Extensions

8.1. Algebraic Closure, Existence and Uniqueness. We prove that a field has an algebraic closure which is unique up to isomorphism.

PROPOSITION 1.8.1. *Let k be a field.*

(1) Let f be a polynomial in $k[x]$ of positive degree n. There exists a splitting field F/k for f such that $\dim_k(F) \leq n!$.
(2) Let S be a set of polynomials in $k[x]$. There exists a splitting field F/k for S.
(3) There exists an algebraic closure Ω/k for k.

PROOF. (1): Factor $f = p_1 \dots p_m$ in $k[x]$ where each p_i is irreducible. If $\deg p_i = 1$ for each i, then take $F = k$ and stop. Otherwise, assume $\deg p_1 > 1$ and by Kronecker's Theorem ([**19**, Theorem 5.2.4]), there is an extension field F_1/k such that $F_1 = k(\alpha)$ and $p_1(\alpha) = 0$. Note that $f(\alpha) = 0$ and $\dim_k(F_1) = \deg p_1 \leq n$. Factor $f = (x-\alpha)g$ in $F_1[x]$. By induction on n, there exists a splitting field F/F_1 for g and $\dim_{F_1}(F) \leq (n-1)!$. So f splits in F and there exist roots $u_1, \dots, u_m$ of f such that $F = F_1(u_1, \dots, u_m) = k(\alpha, u_1, \dots, u_m)$. Lastly, $\dim_k(F) = \dim_k(F_1)\dim_{F_1}(F) \leq n!$.

(2): Assume every element of S has degree greater than one. If not, simply take $F = k$ and stop. The proof is by transfinite induction, Proposition 1.2.3. By the Well Ordering Principle, Axiom 1.2.2, assume S is indexed by a well ordered index set I. For any $\gamma \in I$, let p_γ be the corresponding element of S and let $S(\gamma) = \{p_\alpha \in S \mid \alpha \leq \gamma\}$. Let p_1 be the first element of S and use Part (1) to construct a splitting field F_1/k for p_1. Let $\gamma \in I$ and assume $1 < \gamma$. Inductively, assume that we have constructed for each $\alpha < \gamma$ an extension field F_α/k that is a splitting field for $S(\alpha)$. Assume moreover that the set $\{F_\alpha \mid \alpha < \gamma\}$ is an ascending chain. That is, if $\alpha < \beta < \gamma$, then $F_\alpha \subseteq F_\beta$. It follows that $E = \bigcup_{\alpha<\gamma} F_\alpha$ is an extension field of k and E is a splitting field for $\bigcup_{\alpha<\gamma} S(\alpha)$. Use Part (1) to construct a splitting field F_γ for p_γ over E. Then F_γ/k is a splitting field for $S(\gamma)$. By induction, the field $F = \bigcup_{\gamma\in S} F_\gamma$ is an extension field of k and F is a splitting field for S.

(3) Apply Part (2) to the set of all nonconstant polynomials in $k[x]$. □

LEMMA 1.8.2. *Let $\sigma : k \to K$ be an isomorphism of fields. Let S be a set of polynomials in $k[x]$ and $\sigma(S)$ its image in $K[x]$. Let F/k be a splitting field for S. Let L/K be an extension field such that every polynomial in $\sigma(S)$ splits in L. Then σ extends to a homomorphism of k-algebras $\bar{\sigma} : F \to L$. If L is a splitting field for $\sigma(S)$, then $\bar{\sigma}$ is an isomorphism.*

PROOF. Step 1: Assume $S = \{f\}$ contains only one polynomial and F is a splitting field for f. If $F = k$, then take $\bar{\sigma} = \sigma$ and stop. Otherwise, $\dim_k(F) > 1$ and there is an irreducible factor g of f such that $\deg g > 1$. Let α be a root of g in F and β a root of $\sigma(g)$ in L. By [**19**, Theorem 5.1.6] there is a k-algebra isomorphism $\tau : k(\alpha) \to K(\beta)$ such that $\tau(\alpha) = \beta$. Also, F is a splitting field for f over $k(\alpha)$, and $\dim_{k(\alpha)}(F) < \dim_k(F)$. By induction on $\dim_k(F)$, τ can be extended to a k-algebra homomorphism $\bar{\sigma} : F \to L$. A root of f is mapped under $\bar{\sigma}$ to a root of $\sigma(f)$. Since f splits in F, $\sigma(f)$ splits in $\bar{\sigma}(F)$. By [**19**, Corollary 3.6.9], $\sigma(f)$ has at most $\deg(f)$ roots in L, and they all belong to $\bar{\sigma}(F)$. If $\lambda \in L$ is a root of $\sigma(f)$, then $\lambda \in \bar{\sigma}(F)$. If L/K is generated by roots of $\sigma(f)$, then $L \subseteq \bar{\sigma}(F)$ and $\bar{\sigma}$ is an isomorphism.

Induction step: Consider the set $\mathscr{S}$ of all k-algebra isomorphisms $\tau : E \to M$ where E is an intermediate field of F/k and M is an intermediate field of L/K. Define a partial order on $\mathscr{S}$. If $\tau : E \to M$ and $\tau_1 : E_1 \to M_1$ are two members of $\mathscr{S}$, then say $\tau < \tau_1$ in case $E \subseteq E_1$ and τ is equal to the restriction of τ_1. Since $\sigma : k \to K$ is in $\mathscr{S}$, the set is nonempty. Any chain in $\mathscr{S}$ is bounded above by the union. By Zorn's Lemma, Proposition 1.2.4, there is a maximal member, say $\tau : E \to M$. We need to show that $E = F$. If not, then Step 1 shows how to extend τ, which leads to a contradiction. Also $\tau(F)$ contains every root of every polynomial in $\sigma(S)$, so τ is onto if L is a splitting field of $\sigma(S)$. □

COROLLARY 1.8.3. *Let k be a field.*

(1) If S is a set of polynomials in $k[x]$, the splitting field of S is unique up to k-algebra isomorphism.
(2) If Ω is an algebraic closure of k and F/k is an algebraic extension field, then there is a k-algebra homomorphism $F \to \Omega$.
(3) The algebraic closure of k is unique up to k-algebra isomorphism.

PROOF. (1): Follows straight from Lemma 1.8.2.

(2): Let X be a set of algebraic elements of F such that $F = k(X)$. For each $\alpha \in X$, let $\operatorname{Irr.poly}_k(\alpha)$ denote the irreducible polynomial of α over k. Let $S = \{\operatorname{Irr.poly}_k(\alpha) \mid \alpha \in X\}$. By Proposition 1.8.1, let E/F be a splitting field for S over F. The set of all roots of elements of S contains X as well as a generating set for E over F. Therefore E/k is a splitting field for S over k. By Lemma 1.8.2, there is a k-algebra homomorphism $\tau : E \to \Omega$. The restriction, $\tau|_F : F \to \Omega$ is the desired k-algebra homomorphism.

(3): Let Ω' be another algebraic closure. Applying Part (2), there exists a homomorphism $\theta : \Omega' \to \Omega$. By Lemma 1.8.2, θ is an isomorphism. □

8.2. The Trace Map and Norm Map. Let F/k be a finite dimensional separable extension of fields. In this section we show that there is a trace map $T_k^F : F \to k$ which is a k-linear homomorphism, and a norm map $N_k^F : F^* \to k^*$ which is a homomorphism of multiplicative abelian groups. To define the trace and norm maps we first embed F into a Galois extension K/k with Galois group G. Then F corresponds to a subgroup $H = G_F$. We show that the trace and norm maps are defined by a complete set of coset representatives for G/H. The resulting trace map and norm map agree with the usual trace and norm maps defined in Exercise 1.7.2. In the present context, we show that T_k^F is nonzero, hence is a free generator for the F-vector space $\operatorname{Hom}_k(F,k)$. We will see in Corollary 5.6.8 below that a finite dimensional extension of fields F/k is separable if, and only if, the trace map T_k^F is a free generator for the F-vector space $\operatorname{Hom}_k(F,k)$. For a generalization of the trace and norm maps defined below, see the corestriction homomorphism of Definition 8.5.15 (3).

LEMMA 1.8.4. *Let K/k be a Galois extension with finite group G. Let H be a subgroup of G with $[G:H] = m$. Let $\{\tau_1,\dots,\tau_m\}$ be a complete set of left coset representatives for H in G. Let $F = K^H$. The following are true.*

(1) The assignment $x \mapsto y = \sum_{i=1}^m \tau_i(x)$ defines a k-linear transformation $T_k^F : F \to k$ which does not depend on the choice of left coset representatives for H in G.
(2) The assignment $x \mapsto z = \prod_{i=1}^m \tau_i(x)$ defines a homomorphism of multiplicative groups $N_k^F : F^* \to k^*$ which does not depend on the choice of left coset representatives for H in G.
(3) For any $\alpha \in F$, $T_k^F(\alpha)$ is the trace and $N_k^F(\alpha)$ is the determinant of $\ell_\alpha : F \to F$.
(4) The functions $T_k^F : F \to k$ and $N_k^F : F \to k$ depend on F and k, not K.

PROOF. We prove (1), the proof of (2) is similar. Let $\{\rho_1,\dots,\rho_m\}$ be another complete set of left coset representatives for H in G and $x \in F = K^H$. After a permutation, we can assume $\tau_i H = \rho_i H$ for each i. So there exist $h_i \in H$ such that $\tau_i h_i = \rho_i$. For every $x \in F$, $y = \sum_{i=1}^m \tau_i(x) = \sum_{i=1}^m \tau_i h_i(x) = \sum_{i=1}^m \rho_i(x)$. By [**19**, Example 2.4.6], G acts as a group of permutations on G/H. If $\sigma \in G$, then $\sigma\tau_i H = \sigma\tau_j H$ if and only if $\tau_i H = \tau_j H$. That is, $\{\sigma\tau_i \mid 1 \le i \le m\}$ is a complete set of coset representatives, and $\sigma(y) = \sum_{i=1}^m \sigma\tau_i(x) = y$. So $y \in K^G = k$. Since each $\sigma \in G$ is k-linear, so is the function T_k^F.

(3): Let $\alpha \in F = K^H$ and consider the polynomial

$$g = \prod_{\sigma\in G}(x - \sigma(\alpha)) = \prod_{i=1}^m \prod_{\rho\in H}(x - \tau_i\rho(\alpha)) = \left(\prod_{i=1}^m (x - \tau_i(\alpha))\right)^{[H:1]}.$$

As in Exercise 1.8.3, the polynomial g is the characteristic polynomial of $\ell_\alpha : K \to K$, and $f = \prod_{i=1}^m (x - \tau_i(\alpha))$ is the characteristic polynomial of $\ell_\alpha : F \to F$. The only irreducible factor of f in $k[x]$ is $\operatorname{Irr.poly}_k(\alpha)$. By Exercise 1.7.1, $T_k^F(\alpha)$ is the trace and $N_k^F(\alpha)$ is the determinant of $\ell_\alpha : F \to F$.

(4): Follows from (3). □

DEFINITION 1.8.5. Let F/k be a finite dimensional separable extension. Let K/k be a Galois extension with finite group G which contains F as an intermediate field. Then there is a subgroup H of G such that $F = K^H$. As in Lemma 1.8.4, if $\{\tau_1,\dots,\tau_m\}$ is a complete set of left coset representatives for H, then for $x \in F = K^H$, $T_k^F(x) = \sum_{i=1}^m \tau_i(x)$ and $N_k^F(x) = \prod_{i=1}^m \tau_i(x)$. Note that both T_k^F and N_k^F are functions from F to k. The function T_k^F, which is called the *trace from F to k*, is k-linear and represents an element of $\operatorname{Hom}_k(F,k)$. The function N_k^F, called the *norm from F to k*, induces a homomorphism of multiplicative groups $F^* \to k^*$. The trace map is generalized to a separable extension of commutative rings in Section 5.6.2.

LEMMA 1.8.6. *In the context of Lemma 1.8.4 and Definition 1.8.5,*

(1) There exists $c \in F$ such that $T_k^F(c) = 1$.
(2) $\operatorname{Hom}_k(F,k)$ is an F-vector space of dimension 1 and $\{T_k^F\}$ is a basis.
(3) If $\{\lambda_1,\dots,\lambda_m\}$ is a k-basis for F, then there exist elements $\{\mu_1,\dots,\mu_m\}$ in F such that
  (a) $T_k^F(\mu_j\lambda_i) = \delta_{ij}$ (Kronecker delta), and
  (b) for each $\sigma \in G$: $\lambda_1\sigma(\mu_1)+\cdots+\lambda_m\sigma(\mu_m) = \begin{cases} 1 & \text{if } \sigma \in H \\ 0 & \text{if } \sigma \notin H \end{cases}$.

PROOF. (1): By [**19**, Lemma 5.5.1], there is $b \in K$ such that $1 = \sum_{\sigma\in G}\sigma(b)$. Let $c = \sum_{\rho\in H}\rho(b)$. Then $c \in F$ and $1 = \sum_{\sigma\in G}\sigma(b) = \sum_{i=1}^m \tau_i \sum_{\rho\in H}\rho(b) = \sum_{i=1}^m \tau_i(c)$.

(2): As we have seen already (Example 1.1.13), the field F is a k-algebra, hence it acts as a ring of k-homomorphisms on itself. Let $\theta : F \to \operatorname{Hom}_k(F,F)$ be the left regular representation of F in $\operatorname{Hom}_k(F,F)$. Using θ we can turn $\operatorname{Hom}_k(F,k)$ into a right F-vector space. For every $f \in \operatorname{Hom}_k(F,k)$ and $\alpha \in F$, define $f\alpha$ to be $f \circ \ell_\alpha$. By counting dimensions, it is easy to see that $\operatorname{Hom}_k(F,k)$ is an F-vector space of dimension one. As an F-vector space, any nonzero element $f \in \operatorname{Hom}_k(F,k)$ is a generator. By (1), T_k^F is a generator for $\operatorname{Hom}_k(F,k)$. This implies for every $f \in \operatorname{Hom}_k(F,k)$ there is a unique $\alpha \in F$ such that $f(x) = T_k^F(\alpha x)$ for all $x \in F$. The mapping $F \to \operatorname{Hom}_k(F,k)$ given by $\alpha \mapsto T_k^F \circ \ell_\alpha$ is an isomorphism of k-vector spaces.

(3): Let $\{\lambda_1,\dots,\lambda_m\}$ be a k-basis for F. For each $j = 1,2,\dots,m$, let $f_j : F \to k$ be the projection onto coordinate j. That is, $f_j(\lambda_i) = \delta_{ij}$ (Kronecker delta) and $\{(\lambda_j, f_j) \mid j = 1,\dots,m\}$ is a dual basis for F. For each $x \in F$, $x = \sum_{j=1}^m f_j(x)\lambda_j$. Since T_k^F is a generator for $\operatorname{Hom}_k(F,k)$ over F, there exist unique $\mu_1,\dots,\mu_m$ in F such that for each $x \in F$, $f_j(x) = T_k^F(\mu_j x) = \sum_{i=1}^m \tau_i(\mu_j x)$. We have $T_k^F(\mu_j\lambda_i) = f_j(\lambda_i) = \delta_{ij}$, which is (a). For (b), consider

$$\begin{aligned} x &= \sum_{j=1}^m f_j(x)\lambda_j \\ &= \sum_{j=1}^m \sum_{i=1}^m \tau_i(\mu_j x)\lambda_j \\ &= \sum_{i=1}^m \left(\tau_i(x) \sum_{j=1}^m \tau_i(\mu_j)\lambda_j \right). \end{aligned}$$

Since $G_F = H$, for exactly one $i_0 \in \{1,\dots,m\}$, we have $\tau_{i_0} \in H$. In other words, $\tau_i(x) = x$ for all $x \in F$ if and only if $i = i_0$ if and only if $\tau_i \in H$. By [**19**, Theorem 5.3.7], $\{\tau_1,\dots,\tau_m\}$ are linearly independent over F. If $\sigma \in G$, then $\sigma \equiv \tau_i \pmod{H}$ for a unique i. Then $\sigma(x) = \tau_i(x)$ for all $x \in F$. Hence

$$\sum_{j=1}^m \sigma(\mu_j)\lambda_j = \begin{cases} 1 & \text{if } \sigma \in H \\ 0 & \text{if } \sigma \notin H. \end{cases}$$

This is (b). □

8.3. Finite Fields.

THEOREM 1.8.7. *Let F be a finite field with $\operatorname{char} F = p$. Let k be the prime subfield of F and $n = \dim_k(F)$.*

(1) The group of units of F is a cyclic group.
(2) $F = k(u)$ is a simple extension, for some $u \in F$.
(3) The order of F is p^n.
(4) F is the splitting field for the separable polynomial $x^{p^n} - x$ over k.
(5) F/k is a separable extension. F is a perfect field.
(6) Any two finite fields of order p^n are isomorphic as fields.
(7) F/k is a Galois extension.
(8) The Galois group $\operatorname{Aut}_k(F)$ is cyclic of order n and is generated by the Frobenius homomorphism $\varphi : F \to F$ defined by $\varphi(x) = x^p$.
(9) If d is a positive divisor of n, then $E = \{u \in F \mid u^{p^d} = u\}$ is an intermediate field of F/k which satisfies the following.
  (a) $\dim_E(F) = n/d$, and $\dim_k(E) = d$.
  (b) If φ is the generator for $\operatorname{Aut}_k(F)$, then $\operatorname{Aut}_E(F)$ is the cyclic subgroup generated by φ^d.
  (c) E/k is Galois and $\operatorname{Aut}_k(E)$ is the cyclic group of order d generated by the restriction $\varphi|_E$.
(10) If E is an intermediate field of F/k, and $d = \dim_k(E)$, then d divides n and E is the field described in Part (9).

8.4. Transcendence Bases. Let F/k be an extension of fields and $\Xi \subseteq F$. We say Ξ is *algebraically dependent* over k if there exist n distinct elements $\xi_1, \dots, \xi_n$ in Ξ and a nonzero polynomial $f \in k[x_1, \dots, x_n]$ such that $f(\xi_1, \dots, \xi_n) = 0$. Otherwise we say Ξ is *algebraically independent*. A *transcendence base* for F/k is a subset $\Xi \subseteq F$ which satisfies

(1) Ξ is algebraically independent over k and
(2) if $\Xi \subseteq Z$ and Z is algebraically independent over k, then $\Xi = Z$.

THEOREM 1.8.8. *Let F/k be an extension of fields.*

(1) Assume F is a finitely generated field extension of k. If Ξ is a finite subset of F such that F is algebraic over $k(\Xi)$, then there is a subset of Ξ that is a transcendence base for F/k. A finite transcendence base for F/k exists.
(2) If $\Xi = \{\xi_1, \dots, \xi_n\}$ is a finite transcendence base for F over k, then any other transcendence base for F over k also has cardinality n.

If F/k is an extension of fields such that a finite transcendence base exists, then the *transcendence degree* of F/k, denoted $\operatorname{tr.deg}_k(F)$, is the number of elements in any transcendence base of F over k.

8.5. Exercises.

EXERCISE 1.8.1. Let k be a field, a, b, c some elements of k and assume $a \neq b$. Let $f = (x-a)(x-b)$ and $g = (x-c)^2$. Prove:

(1) There is an isomorphism of k-algebras $k[x]/(f) \cong k \oplus k$.
(2) There is an isomorphism of k-algebras $k[x]/(g) \cong k[x]/(x^2)$.
(3) If h is a monic irreducible quadratic polynomial in $k[x]$, then the k-algebras $k[x]/(f)$, $k[x]/(g)$, and $k[x]/(h)$ are pairwise nonisomorphic.

EXERCISE 1.8.2. Let k be a field and A a finite dimensional k-algebra. Prove that if $\dim_k(A) = 2$, then

(1) A is commutative.
(2) A is either a field extension of k, or isomorphic as a k-algebra to one of the two rings in parts (1) or (2) of Exercise 1.8.1.

EXERCISE 1.8.3. Let F/k be a Galois extension of fields with finite group G. Let α be an arbitrary element of F, and set

$$g = \prod_{\sigma \in G} (x - \sigma(\alpha)).$$

Show that $g \in k[x]$ and the only irreducible factor of g in $k[x]$ is $\operatorname{Irr.poly}_k(\alpha)$.

EXERCISE 1.8.4. Let R be a UFD with quotient field K. Assume the characteristic of R is not equal to 2. Let $a \in R$ be an element which is not a square in R and $f = x^2 - a \in R[x]$. Let $S = R[x]/(f)$, $L = K[x]/(f)$.

(1) Show that there is a commutative square

$$\begin{tikzcd} S \arrow[r] & L \\ R \arrow[u] \arrow[r] & K \arrow[u] \end{tikzcd}$$

where each arrow is the natural map and each arrow is one-to-one.

(2) Show that L is the quotient field of S.

(3) $\operatorname{Aut}_K L = \langle \sigma \rangle$ is a cyclic group of order two and L/K is a Galois extension.

(4) If $\sigma : L \to L$ is the automorphism of order two, then σ restricts to an R-automorphism of S.

(5) The norm map $N_K^L : L \to K$ restricts to a norm map $N_R^S : S \to R$.

EXERCISE 1.8.5. If F/k is an extension of finite fields, show that the image of the norm map $N_k^F : F^* \to k^*$ is equal to k^*.

EXERCISE 1.8.6. Let k be a field and A a k-algebra which is algebraic over k. Let $u \in A$ and let $\operatorname{min.poly}_k(u)$ be the minimal polynomial of u in $k[x]$. Prove the following.

(1) u is invertible if and only if $\operatorname{min.poly}_k(u)$ has a nonzero constant term.

(2) If u is not invertible, then u is a zero divisor.

CHAPTER 2

Modules

This chapter contains a deeper study of modules. The material presented here is fundamental and will be applied in all of the following chapters. Throughout, the ground ring R will be a general ring. That is, R is not assumed to be commutative. By default, an R-module M will be a left R-module. For many of the constructions, the module will be a right R-module, or a two-sided R-module.

In Section 2.1 we introduce the notion of progenerator modules, which is a class of modules that have many of the categorical properties of finitely generated free modules. Our first version of Nakayama's Lemma appears in Section 2.2. This is an important theorem about finitely generated modules over a commutative ring. It states that if M is nonzero and finitely generated, then there is a maximal left ideal $\mathfrak{m}$ of R such that $\mathfrak{m}M \neq M$. There is a version for noncommutative rings in Chapter 4.2.

We define the tensor product $M \otimes_R N$ for a right R-module M and left R-module N over a ring R. This important construction allows us to define the tensor functor by fixing either M or N and treating the other as a variable. Likewise, the group of homomorphisms $\operatorname{Hom}_R(M,N)$ is defined for any ring R and left R-modules M and N. There are two possible hom functors defined by fixing either M or N and treating the other as a variable. Some important relations arise when the tensor and hom functors are composed. The first of these so-called "Hom Tensor Relations" are proved in Section 2.4.3.

Section 2.5 is a short introduction to the theory of Homological Algebra. We prove three fundamental theorems, namely the Five Lemma, the Snake Lemma, and the Product Lemma.

The notion of injective module appears in Section 2.6. In this short introduction, some of the important properties satisfied by injective modules are derived.

In Section 2.7 we define the direct limit of a directed family of R-modules and the inverse limit of an inverse system of R-modules. For these two important constructions many of the fundamental properties are derived.

This chapter ends with a proof of the classical Morita Theorems. For a ring R and a left R-progenerator module M, the main theorem states that there is an equivalence between the category of right R-modules and the category of left modules over the endomorphism ring $\operatorname{Hom}_R(M,M)$.

1. Progenerator Modules

Proposition 2.1.1 lists three fundamental properties of a projective module. The definition follows the proposition.

PROPOSITION 2.1.1. *Let R be a ring and M an R-module. The following are equivalent.*

(1) There is a free R-module F and M is isomorphic to a direct summand of F.

(2) *Every short exact sequence of R-modules*

$$0 \to A \to B \xrightarrow{\beta} M \to 0$$

is split exact.

(3) *For any diagram of R-modules*

$$\begin{tikzcd}
& M \arrow[d, "\phi"] \arrow[dl, dashed, "\exists\psi"'] & \\
A \arrow[r, "\alpha"] & B \arrow[r] & 0
\end{tikzcd}$$

with the bottom row exact, there exists an R-module homomorphism $\psi : M \to A$ *such that* $\alpha\psi = \phi$.

PROOF. (3) implies (2): Start with the diagram

$$\begin{tikzcd}
& & & M \arrow[d, "="] \arrow[dl, dashed, "\exists\psi"'] & \\
0 \arrow[r] & A \arrow[r] & B \arrow[r, "\beta"] & M \arrow[r] & 0
\end{tikzcd}$$

where we assume the bottom row is exact. By Part (3) there exists $\psi : M \to B$ such that $\beta\psi = 1_M$. Then ψ is the splitting map.

(2) implies (1): Take I to be the set M. Let $B = R^I$ be the free R-module on I. Take $\beta : B \to M$ to be $\beta(f) = \sum f(i)i$. The reader should verify that this is a well defined epimorphism. By Part (2) the exact sequence

$$B \xrightarrow{\beta} M \to 0$$

splits. By Exercise 1.6.5, M is isomorphic to a direct summand of B.

(1) implies (3): We are given a free module F and $F \cong M \oplus M'$. Let $\pi : F \to M$ be the projection onto the first factor and let $\iota : M \to F$ be the splitting map to π. Given the diagram of R-modules in Part (3), consider this augmented diagram

$$\begin{tikzcd}
& F \arrow[d, shift right, "\pi"'] \arrow[ddl, dashed, "\exists\gamma"'] & \\
& M \arrow[u, shift right, "\iota"'] \arrow[d, "\phi"] \arrow[dl, dashed, "\exists\psi"] & \\
A \arrow[r, "\alpha"] & B \arrow[r] & 0.
\end{tikzcd}$$

First we show that there exists γ making the outer triangle commutative, then we use γ to construct ψ. Pick a basis $\{e_i \mid i \in I\}$ for F. For each $i \in I$ set $b_i = \phi\pi(e_i) \in B$. Since α is onto, lift each b_i to get $a_i \in A$ such that $\alpha(a_i) = b_i$ (this uses the Axiom of Choice, Proposition 1.2.6). Define $\gamma : F \to A$ on the basis elements by $\gamma(e_i) = a_i$ and extend by linearity. By construction, $\alpha\gamma = \phi\pi$. Applying ι to both sides gives $\alpha\gamma\iota = \phi\pi\iota$. But $\pi\iota = 1_M$, hence $\alpha\gamma\iota = \phi$. Define ψ to be $\gamma\iota$. $\square$

DEFINITION 2.1.2. Let R be a ring and M an R-module. We say M is a *projective* R-module if M satisfies any of the equivalent conditions of Proposition 2.1.1.

EXAMPLE 2.1.3. A free module trivially satisfies Proposition 2.1.1 (1), hence a free module is a projective module.

EXAMPLE 2.1.4. Let D be a division ring and $R = M_2(D)$ the ring of two-by-two matrices over D. As a left D-module, R is free of rank 4. Let

$$e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

The reader should verify the following facts.

(1) e_1 and e_2 are orthogonal idempotents.
(2) Re_1 is the set of all matrices with second column consisting of zeros.
(3) Re_2 is the set of all matrices with first column consisting of zeros.
(4) $\dim_D(Re_1) = \dim_D(Re_2) = 2$.
(5) $R = Re_1 \oplus Re_2$ as R-modules.

By (5), Re_1 and Re_2 are projective R-modules. It follows from the rank formula proved in Proposition 2.1.13 below that Re_1 and Re_2 are not free R-modules.

EXAMPLE 2.1.5. If $R = M_n(D)$ is the ring of n-by-n matrices over a division ring D, then we will see in Example 4.4.2 that R is a simple artinian ring. By Theorem 4.3.3, every R-module is projective. If $n \geq 2$, then using the method of Example 2.1.4 one can show that R contains left ideals that are not free.

EXAMPLE 2.1.6. Here is a list of rings with the property that every finitely generated projective module is free.

(1) A vector space over a division ring is free, by Theorem 1.6.13.
(2) Let R be a principal ideal domain and M a finitely generated projective R-module. By Proposition 2.1.1, M is isomorphic to a submodule of a finitely generated free R-module. By Theorem 1.7.14, M is free.
(3) Let R be a commutative local ring. If M is projective, then Kaplansky proved that M is free. If M is finitely generated, we prove this in Proposition 3.4.2.
(4) We will not give a proof, but if k is a field and $R = k[x_1, \dots, x_n]$, then Quillen and Suslin proved that any finitely generated projective R-module is free [**51**, Theorem 4.62]. The same conclusion is true if k is a principal ideal domain [**51**, Theorem 4.63] or [**37**, Theorem V.2.9].

EXAMPLE 2.1.7. Here is another example of a projective module that is not free. Let $R = \mathbb{Z}/6$ be the ring of integers modulo 6. In R let $I = \{0, 2, 4\}$ be the ideal generated by the coset containing 2. Let $J = \{0, 3\}$. Then R is the internal direct sum $R = I \oplus J$. Then both I and J are projective R-modules by Proposition 2.1.1 (1). But I is not free, since it has only 3 elements. Likewise J is not free.

COROLLARY 2.1.8. *Let R be a ring and M a finitely generated projective R-module. Then M is of finite presentation over R (Definition 1.6.12). There exists a finitely generated projective R-module N such that $M \oplus N$ is a finitely generated free R-module.*

PROOF. Is left to the reader. $\square$

DEFINITION 2.1.9. Let M be an R-module. A *dual basis* for M is a set of ordered pairs $\{(m_i, f_i) \mid i \in I\}$ over an index set I consisting of $m_i \in M$, $f_i \in \operatorname{Hom}_R(M, R)$ and satisfying

(1) For each $m \in M$, $f_i(m) = 0$ for all but finitely many $i \in I$, and
(2) for all $m \in M$, $m = \sum_{i \in I} f_i(m) m_i$.

LEMMA 2.1.10. *(Dual Basis Lemma) Let R be a ring and M an R-module. Then M is projective if and only if M has a dual basis $\{(m_i, f_i) \mid i \in I\}$ consisting of $m_i \in M$, $f_i \in \operatorname{Hom}_R(M, R)$ as in Definition 2.1.9. Moreover, the R-module M is finitely generated if and only if I can be chosen to be a finite set.*

PROOF. Assume M is projective. Let $\{m_i \mid i \in I\} \subseteq M$ be a generating set for the R-module M. Let $\{e_i \mid i \in I\}$ be the standard basis for R^I. Using Lemma 1.6.11, define an onto homomorphism $\pi : R^I \to M$ by $\pi(e_i) = m_i$. By Proposition 2.1.1 (3) with $M = B$ and $\alpha = \pi$, there is a splitting map $\iota : M \to R^I$ such that $\pi\iota = 1$. Let $\pi_i : R^I \to R$ be the projection onto the ith summand. For each $f \in R^I$, $\pi_i(f) = f(i)$. Then $h = \sum_{i\in I} \pi_i(h)e_i$ for each $h \in R^I$. For each $i \in I$, set $f_i = \pi_i \circ \iota$. By definition of π_i, for each $m \in M$, $f_i(m) = 0$ for all but finitely many $i \in I$. For any $m \in M$

$$\begin{aligned}\sum_{i\in I} f_i(m)m_i &= \sum_{i\in I} \pi_i(\iota(m))\pi(e_i)\\ &= \pi\left(\sum_{i\in I} \pi_i(\iota(m))e_i\right)\\ &= \pi(\iota(m))\\ &= m.\end{aligned}$$

This shows $\{(m_i, f_i) \mid i \in I\}$ satisfies both parts of Definition 2.1.9, hence is a dual basis.

Conversely, assume $\{(m_i, f_i) \mid i \in I\}$ is a dual basis. We show that M is a direct summand of R^I. Define $\iota : M \to R^I$ by $\iota(m)(j) = f_j(m)$. Define $\pi : R^I \to M$ by $\pi(h) = \sum_{i\in I} h(i)m_i$. The reader should verify that π and ι are R-linear. The proof follows from

$$\begin{aligned}\pi(\iota(m)) &= \sum_{i\in I} \iota(m)(i)m_i\\ &= \sum_{i\in I} f_i(m)m_i\\ &= m.\end{aligned}$$

□

LEMMA 2.1.11. *Let R be a ring and M an R-module. The set*

$$\mathfrak{T}_R M = \left\{ \sum_{i=1}^{n} f_i(m_i) \mid n \geq 1, f_i \in \operatorname{Hom}_R(M,R), m_i \in M \right\}$$

is a 2-sided ideal in R. The ideal $\mathfrak{T}_R M$ is called the trace ideal *of M in R.*

PROOF. The proof is left to the reader. (Hint: Make $\operatorname{Hom}_R(M,R)$ into a right R-module by the action $(fr)(m) = f(m)r$.) □

DEFINITION 2.1.12. Let R be a ring and M an R-module. We say that M is a *generator* over R in case $\mathfrak{T}_R M = R$. We say that M is a *progenerator* over R in case M is finitely generated, projective and a generator over R.

PROPOSITION 2.1.13. *Let $\theta : R \to S$ be a homomorphism of rings and let M be an S-module. Using θ, we can view S and M as R-modules.*

(1) (Finitely Generated over Finitely Generated is Finitely Generated) If S is a finitely generated R-module and M is a finitely generated S-module, then M is a finitely generated R-module.
(2) (Projective over Projective is Projective) If S is a projective R-module and M is a projective S-module, then M is a projective R-module.
(3) (A Generator over a Generator is a Generator) If S is a generator over R and M is a generator over S, then M is a generator over R.
(4) (A Progenerator over a Progenerator is a Progenerator) If S is a progenerator over R and M is a progenerator over S, then M is a progenerator over R.

(5) *(Free over Free is Free) If S is free as an R-module and M is free as an S-module, then M is free as an R-module. If M has a finite basis over S , and S has a finite basis over R, then M has a finite basis over R. In this case, if R and S are both commutative, then* $\operatorname{Rank}_R(M) = \operatorname{Rank}_S(M)\operatorname{Rank}_R(S)$. *If R and S are fields, then* $\dim_R(S)$ *and* $\dim_S(M)$ *are both finite if and only if* $\dim_R(M)$ *is finite.*

PROOF. (1): The proof of this part is left to the reader.

(2): There exists a dual basis $\{(m_i, f_i) \mid i \in I\}$ for M over S where $m_i \in M$ and $f_i \in \operatorname{Hom}_S(M,S)$ and $f_i(m) = 0$ for almost all $i \in I$ and $\sum_i f_i(m)m_i = m$ for all $m \in M$. There exists a dual basis $\{(s_j, g_j) \mid j \in J\}$ for S over R where $s_j \in S$ and $g_j \in \operatorname{Hom}_R(S,R)$ and $g_j(s) = 0$ for almost all $j \in J$ and $\sum_j g_j(s)s_j = s$ for all $s \in S$. For each $(i, j) \in I \times J$ the composition of functions $g_j f_i$ is in $\operatorname{Hom}_R(M,R)$ and the product $s_j m_i$ is in M. For each $m \in M$ we have

$$\begin{aligned}
\sum_{(i,j)\in I\times J} g_j(f_i(m))s_j m_i &= \sum_{i\in I}\Big(\sum_{j\in J} g_j(f_i(m))s_j\Big)m_i \\
&= \sum_{i\in I} f_i(m)m_i \\
&= m.
\end{aligned}$$

Under the finite hypotheses, both I and J can be taken to be finite.

(3): For some $m > 0$ there exist $\{f_1,\dots,f_m\} \subseteq \operatorname{Hom}_S(M,S)$ and $\{x_1,\dots,x_m\} \subseteq M$ such that $1 = \sum_{i=1}^m f_i(x_i)$. For some n there exist $\{g_1,\dots,g_n\} \subseteq \operatorname{Hom}_R(S,R)$ and $\{s_1,\dots,s_n\} \subseteq S$ such that $1 = \sum_{j=1}^n g_j(s_j)$. For each (i, j), $g_j f_i \in \operatorname{Hom}_R(M,R)$ and $s_j m_i \in M$ and

$$\begin{aligned}
\sum_{i=1}^m \sum_{j=1}^n g_j f_i(s_j m_i) &= \sum_{i=1}^m \sum_{j=1}^n g_j\big(s_j f_i(m_i)\big) \\
&= \sum_{j=1}^n g_j\Big(s_j \sum_{i=1}^m f_i(m_i)\Big) \\
&= \sum_{j=1}^n g_j(s_j) \\
&= 1.
\end{aligned}$$

(4): Follows from Parts (1), (2) and (3).

(5): Start with a free basis $\{m_i \mid i \in I\}$ for M over S where $m_i \in M$. If we let $f_i \in \operatorname{Hom}_S(M,S)$ be the coordinate projection onto the submodule Sm_i (in Definition 1.6.1 this projection map was called π_i), then we have a dual basis $\{(m_i, f_i) \mid i \in I\}$ for M over S. Likewise, there exists a dual basis $\{(s_j, g_j) \mid j \in J\}$ for S over R where $\{s_j \mid j \in J\}$ is a free basis and $g_j : S \to R$ is the projection homomorphism onto coordinate j. By (2), $\{(s_j m_i, g_j f_i)\}$ is a dual basis for M over R. The reader should verify that $\{s_j m_i\}$ is a free basis and the formula for the ranks. □

EXAMPLE 2.1.14. Let R be a ring with no zero divisors. Let I be a nonzero left ideal of R. Then I is an R-module. Since $\operatorname{annih}_R(I) = (0)$, I is faithful. If $a \in R$, the principal ideal $I = Ra$ is a free R-module and $\operatorname{Rank}_R(I) = 1$.

EXAMPLE 2.1.15. Let k be a field of characteristic different from 2. Let x and y be indeterminates over k. Let $f = y^2 - x(x^2 - 1)$. Set $S = k[x,y]/(f)$ and let $M = (x,y)$ be the maximal ideal of S generated by the images of x and y. By Exercise 2.2.1, S is an integral domain. By Exercise 2.2.2, M is not free. In this example, we prove that M is projective.

The proof consists of constructing a dual basis for M. An arbitrary element $m \in M$ can be written in the form $m = ax + by$, for some $a, b \in S$. From

$$\begin{aligned}\left(\frac{x^2-1}{y}\right)m &= \frac{x^2-1}{y}(ax+by)\\ &= \frac{ax(x^2-1)+by(x^2-1)}{y}\\ &= \frac{ay^2+by(x^2-1)}{y}\\ &= ay+b(x^2-1)\end{aligned}$$

we see that $\left(\frac{x^2-1}{y}\right)m \in S$. For each $m \in M$ we have

$$m = mx^2 - m(x^2-1) = mx^2 - \left(\frac{x^2-1}{y}\right)my.$$

This also shows that M is generated by x^2 and y. Define the dual basis. Set $m_1 = x^2$ and $m_2 = y$. Define $\phi_i : M \to S$ by $\phi_1(m) = m$ and $\phi_2(m) = -\left(\frac{x^2-1}{y}\right)m$. Since $m = \phi_1(m)m_1 + \phi_2(m)m_2$ for every $m \in M$, $\{(m_1,\phi_1),(m_2,\phi_2)\}$ is a dual basis and M is a projective S-module. To see how this fits into the Dual Basis Lemma 2.1.10, notice that a splitting of

$$\begin{aligned}S^2 &\xrightarrow{\pi} M\\ (a,b) &\mapsto ax^2+by\end{aligned}$$

is $\phi : M \to S^2$ which is given by

$$\begin{aligned}\phi(m) &= (\phi_1(m), \phi_2(m))\\ &= \left(m, -\left(\frac{x^2-1}{y}\right)m\right).\end{aligned}$$

Notice that $\phi(x) = (x, -y)$ and $\phi(y) = (y, -(x^2-1))$.

EXAMPLE 2.1.16. Let $\mathbb{R}$ be the field of real numbers. Let x and y be indeterminates over $\mathbb{R}$. Let $f = x^2 + y^2 - 1$. Set $S = \mathbb{R}[x,y]/(f)$ and let $M = (x, y-1)$ be the maximal ideal of S generated by the images of x and $y-1$. By Exercise 2.2.3, S is an integral domain. By Exercise 2.2.4, M is not free. In this example, we prove that M is projective. The proof consists of constructing a dual basis for M. An arbitrary element $m \in M$ can be written in the form $m = ax + b(y-1)$, for some $a, b \in S$. From

$$\begin{aligned}\left(\frac{y+1}{x}\right)m &= \frac{y+1}{x}(ax+b(y-1))\\ &= \frac{ax(y+1)+b(y^2-1)}{x}\\ &= \frac{ax(y+1)-bx^2}{x}\\ &= a(y+1)-bx\end{aligned}$$

we see that $\left(\frac{y+1}{x}\right)m \in S$. For each $m \in M$ we have

$$\begin{aligned} m &= \frac{y+1}{2}m - \frac{y-1}{2}m \\ &= \left(\frac{y+1}{2x}\right)mx - \frac{m}{2}(y-1). \end{aligned}$$

Define the dual basis. Set $m_1 = x$ and $m_2 = y-1$. Define $\phi_i : M \to S$ by $\phi_1(m) = \left(\frac{y+1}{2x}\right)m$ and $\phi_2(m) = \frac{-m}{2}$. Since $m = \phi_1(m)m_1 + \phi_2(m)m_2$ for every $m \in M$, $\{(m_1,\phi_1),(m_2,\phi_2)\}$ is a dual basis and M is a projective S-module. To see how this fits into the Dual Basis Lemma 2.1.10, notice that the splitting of

$$\begin{aligned} S^2 &\xrightarrow{\pi} M \\ (a,b) &\mapsto ax + b(y-1) \end{aligned}$$

is $\iota : M \to S^2$ which is given by

$$\begin{aligned} \iota(m) &= (\phi_1(m), \phi_2(m)) \\ &= \left(\frac{y+1}{2x}m, \frac{-m}{2}\right). \end{aligned}$$

Notice that $\iota(x) = (\frac{y+1}{2}, \frac{-x}{2})$ and $\iota(y-1) = (\frac{-x}{2}, \frac{-y-1}{2})$.

2. Nakayama's Lemma

Let R be a ring, $A \subseteq R$ a left ideal of R, and M an R-module. We denote by AM the R-submodule of M generated by all elements of the form am, where $a \in A$ and $m \in M$.

LEMMA 2.2.1. *(Nakayama's Lemma) Let R be a commutative ring and M a finitely generated R-module. An ideal A of R has the property that $AM = M$ if and only if $A + \operatorname{annih}_R(M) = R$.*

PROOF. Assume $A + \operatorname{annih}_R(M) = R$. Write $1 = \alpha + \beta$ for some $\alpha \in A$ and $\beta \in \operatorname{annih}_R(M)$. Given m in M, $m = 1m = (\alpha+\beta)m = \alpha m + \beta m = \alpha m$. Therefore $AM = M$.

Conversely, say $AM = M$. Choose a generating set $\{m_1, \dots, m_n\}$ for M over R. Define

$$\begin{aligned} M = M_1 &= Rm_1 + \cdots + Rm_n \\ M_2 &= Rm_2 + \cdots + Rm_n \\ &\vdots \\ M_n &= Rm_n \\ M_{n+1} &= 0. \end{aligned}$$

We prove that for every $i = 1, 2, \dots, n+1$, there exists α_i in A such that $(1-\alpha_i)M \subseteq M_i$. Since $(1-0)M = M \subseteq M_1$, take $\alpha_1 = 0$. Proceed inductively. Let $i \geq 1$ and assume $\alpha_i \in A$ and $(1-\alpha_i)M \subseteq M_i$. Then

$$\begin{aligned} (1-\alpha_i)M &= (1-\alpha_i)AM \\ &= A(1-\alpha_i)M \\ &\subseteq AM_i. \end{aligned}$$

In particular, $(1-\alpha_i)m_i \in AM_i = Am_i + Am_{i+1} + \cdots + Am_n$. So there exist $\alpha_{ii}, \dots, \alpha_{im} \in A$ such that
$$(1-\alpha_i)m_i = \sum_{j=i}^{n} \alpha_{ij} m_j.$$
Subtracting
$$(1-\alpha_i-\alpha_{ii})m_i = \sum_{j=i+1}^{n} \alpha_{ij} m_j$$
is in M_{i+1}. Look at
$$\begin{aligned}(1-\alpha_i)(1-\alpha_i-\alpha_{ii})M &= (1-\alpha_i-\alpha_{ii})\big((1-\alpha_i)M\big)\\ &\subseteq (1-\alpha_i-\alpha_{ii})M_i\\ &\subseteq M_{i+1}.\end{aligned}$$
Set $\alpha_{i+1} = -(-\alpha_i - \alpha_{ii} - \alpha_i + \alpha_i^2 + \alpha_i\alpha_{ii})$. Then $\alpha_{i+1} \in A$ and $(1-\alpha_{i+1})M \subseteq M_{i+1}$. By finite induction, $(1-\alpha_{n+1})M = 0$. Hence $1-\alpha_{n+1} \in \operatorname{annih}_R(M)$ and $1 \in A + \operatorname{annih}_R(M)$. □

COROLLARY 2.2.2. *Let R be a commutative ring and M a finitely generated R-module. If $\mathfrak{m}M = M$ for every maximal ideal $\mathfrak{m}$ of R, then $M = 0$.*

PROOF. If $M \neq 0$, then $1 \notin \operatorname{annih}_R(M)$. Some maximal ideal $\mathfrak{m}$ contains $\operatorname{annih}_R(M)$. So $\mathfrak{m} + \operatorname{annih}_R(M) = \mathfrak{m} \neq R$. By Nakayama's Lemma 2.2.1, $\mathfrak{m}M \neq M$. □

PROPOSITION 2.2.3. *Let R be a commutative ring and M a finitely generated and projective R-module. Then $\mathfrak{T}_R(M) \oplus \operatorname{annih}_R(M) = R$.*

PROOF. There exists a dual basis $\{(m_i, f_i) \mid 1 \le i \le n\}$ for M. For each $m \in M$, we see that $m = f_1(m)m_1 + \cdots + f_n(m)m_n$ is in $\mathfrak{T}_R(M)M$. Then $\mathfrak{T}_R(M)M = M$. By Nakayama's Lemma 2.2.1, $\mathfrak{T}_R(M) + \operatorname{annih}_R(M) = R$. Now check that $\mathfrak{T}_R(M)\operatorname{annih}_R(M) = 0$. A typical generator for $\mathfrak{T}_R(M)$ is $f(m)$ for some $m \in M$ and $f \in \operatorname{Hom}_R(M,R)$. Given $\alpha \in \operatorname{annih}_R(M)$, we see that $\alpha f(m) = f(\alpha m) = f(0) = 0$. By Exercise 1.1.9, $\mathfrak{T}_R(M) \cap \operatorname{annih}_R(M) = 0$. □

COROLLARY 2.2.4. *Let R be a commutative ring and M an R-module. Then the following are true.*

(1) M is an R-progenerator if and only if M is finitely generated projective and faithful.
(2) Assume R has no idempotents except 0 and 1. Then M is an R-progenerator if and only if M is finitely generated, projective, and $M \neq (0)$.

PROOF. (1): By Proposition 2.2.3, $\mathfrak{T}_R(M) = R$ if and only if $\operatorname{annih}_R(M) = (0)$ which is true if and only if M is faithful.

(2): If 0 and 1 are the only idempotents, then $\operatorname{annih}_R(M) = (0)$. □

Here is another variation of Nakayama's Lemma.

COROLLARY 2.2.5. *Let R be a commutative ring. Suppose I is an ideal in R, M is an R-module, and there exist submodules A and B of M such that $M = A + IB$. If*

(1) I is nilpotent (that is, $I^n = 0$ for some $n > 0$), or
(2) I is contained in every maximal ideal of R and M is finitely generated,

then $M = A$.

PROOF. Notice that

$$\begin{aligned} M/A &= \frac{A+IB}{A} \\ &\subseteq \frac{A+IM}{A} \\ &\subseteq I(M/A) \\ &\subseteq M/A. \end{aligned}$$

Assuming (1) we get $M/A = I(M/A) = \cdots = I^n(M/A) = 0$. Assume (2) and let $\mathfrak{m}$ be an arbitrary maximal ideal of R. Then $M/A = I(M/A) \subseteq \mathfrak{m}(M/A)$. By Corollary 2.2.2, $M/A = 0$. □

2.1. Exercises.

EXERCISE 2.2.1. For the following, let k be a field of characteristic different from 2. Let $R = k[x]$ and f be the polynomial $f = y^2 - x(x^2-1)$ in $R[y]$. Let S be the factor ring

$$S = \frac{k[x,y]}{(y^2 - x(x^2-1))}.$$

Elements of S are cosets represented by polynomials in $k[x,y]$. For example, in S the polynomial x represents a coset. When it is clear that we are referring to a coset in S, we choose not to adorn the polynomial with an extra "bar", "tilde" or "mod" symbol. So, for the sake of notational simplicity in what follows, we refer to a coset by one of its representatives. The following is an outline of a proof that S is not a UFD. In particular, S is not a PID.

(1) Use Exercise 1.8.4 to show that $S = R[y]/(f) = k[x][y]/(f)$ is an extension ring of R and there is an R-algebra automorphism $\sigma : S \to S$ defined by $y \mapsto -y$. The norm map $N_R^S : S \to R$ is defined by $u \mapsto u\sigma(u)$.
(2) Use the norm map to prove that the group of invertible elements of S is equal to the nonzero elements in k.
(3) Show that x and y are irreducible in S. (Hint: First show that x is not a norm. That is, x is not in the image of N_R^S. Likewise $x-1$ and $x+1$ are not norms.)
(4) Prove that S is not a UFD. In particular, S is not a PID.

EXERCISE 2.2.2. In what follows, let S be the ring defined in Exercise 2.2.1. Any ideal in S is an S-module. Let $M = (x,y)$ denote the ideal in S generated by x and y. To show that M is not a free S-module, prove the following:

(1) If J is a nonzero ideal of S, then as an S-module J is faithful.
(2) The principal ideal (x) is not a maximal ideal in S.
(3) The ideal $M = (x,y)$ is a maximal ideal in S. The factor ring S/M is a field.
(4) The ideal M is not a principal ideal. (Hint: Lemma 1.5.2,(2).)
(5) The ideal M^2 is a principal ideal in S. (Hint: $x \in M^2$.)
(6) Over the field S/M, the vector space M/M^2 has dimension one. (Hint: $y \in M$, but $y \notin M^2$.)
(7) M is not a free S module. (Hint: Exercise 1.1.1. If M were free, it would have rank one.)

EXERCISE 2.2.3. Let $R = \mathbb{R}[x]$ and f be the polynomial $f = y^2 + x^2 - 1$ in $R[y]$. Let S be the factor ring

$$S = \frac{\mathbb{R}[x,y]}{(y^2 + x^2 - 1)}.$$

The following is an outline of a proof that S is not a UFD. In particular, S is not a PID.

(1) Use Exercise 1.8.4 to show that $S = R[y]/(f) = \mathbb{R}[x][y]/(f)$ is an extension ring of R and there is an R-algebra automorphism $\sigma : S \to S$ defined by $y \mapsto -y$. The norm map $N_R^S : S \to R$ is defined by $u \mapsto u\sigma(u)$.
(2) Use the norm map to prove that the group of invertible elements of S is equal to the nonzero elements in $\mathbb{R}$.
(3) Show that x and $y-1$ are irreducible in S. (Hint: First show that x is not a norm from S.)
(4) Prove that S is not a UFD. In particular, S is not a PID.

EXERCISE 2.2.4. In what follows, let S be the ring defined in Exercise 2.2.3. Any ideal in S is an S-module. Let $M = (x, y-1)$ denote the ideal in S generated by x and $y-1$. To show that M is not a free S-module, prove the following:

(1) The principal ideal (x) is not a maximal ideal in S.
(2) The ideal $M = (x, y-1)$ is a maximal ideal in S. The factor ring S/M is a field.
(3) The ideal M is not a principal ideal. (Hint: Lemma 1.5.2,(2).)
(4) The ideal M^2 is a principal ideal in S. (Hint: $y-1 \in M^2$.)
(5) Over the field S/M, the vector space M/M^2 has dimension one. (Hint: $x \in M$, but $x \notin M^2$.)
(6) M is not a free S module. (Hint: Exercise 1.1.1. If M were free, it would have rank one.)

EXERCISE 2.2.5. Let R be any ring and M an R-module. Suppose there is an infinite exact sequence

$$\cdots \to A_{n+1} \to A_n \to \cdots \to A_2 \to A_1 \to A_0 \to M \to 0 \tag{2.1}$$

of R-modules. If each A_i is a free R-module, then we say (2.1) is a *free resolution* of M. Use Lemma 1.6.11 and induction to show that a free resolution exists for any R and any M. Since a free module is also projective, this also shows that M has a *projective resolution*.

EXERCISE 2.2.6. Let R be a ring and $\{M_i \mid i \in I\}$ a family of R-modules. Show that the direct sum $\bigoplus_{i\in I} M_i$ is projective over R if and only if each M_i is projective over R.

EXERCISE 2.2.7. Let R be a unique factorization domain. Let α be a nonzero element of R which is not invertible.

(1) Show that $\operatorname{Hom}_R(R[\alpha^{-1}], R) = (0)$.
(2) Show that $R[\alpha^{-1}]$ is not a projective R-module.

EXERCISE 2.2.8. This is a slight generalization of Exercise 2.2.7. Let R be an integral domain. Let α be a nonzero element of R such that the ideals $I^n = (\alpha^n)$ satisfy the identity $\bigcap_{n>0}(\alpha^n) = (0)$. Show that $R[\alpha^{-1}]$ is not a projective R-module.

EXERCISE 2.2.9. Let R be a ring and M a left R-module. Prove that the following are equivalent.

(1) M is an R-generator.
(2) The R-module R is the homomorphic image of a direct sum $M^{(n)}$ of finitely many copies of M.
(3) The R-module R is the homomorphic image of a direct sum M^I of copies of M over some index set I.
(4) Every left R-module A is the homomorphic image of a direct sum M^I of copies of M over some index set I.

EXERCISE 2.2.10. Let $\phi : R \to S$ be a local homomorphism of commutative local rings. Assume S is a finitely generated R-module, and $\mathfrak{m}$ is the maximal ideal of R. Show that if the map $R/\mathfrak{m} \to S/\mathfrak{m}S$ induced by ϕ is an isomorphism, then ϕ is onto. (Hint: S is generated by $\phi(R)$ and $\mathfrak{m}S$.)

EXERCISE 2.2.11. Let R be a commutative ring and J an ideal in R. Prove:

(1) If J is a direct summand of R (that is, $R = J \oplus I$ for some ideal I), then $J^2 = J$.
(2) If J is a finitely generated ideal, and $J^2 = J$, then J is a direct summand of R.

EXERCISE 2.2.12. State and prove a version of Exercise 1.6.14 for rings. That is, show that the product $\prod_{i \in I} R_i$ of a family $\{R_i \mid i \in I\}$ of rings is the solution to a universal mapping problem.

EXERCISE 2.2.13. This exercise is based on Example 2.1.15. Let k be a field of characteristic different from 2, $S = k[x,y]/(y^2 - x(x^2-1))$, and $M = (x,y)$ the maximal ideal of S generate by x and y. Prove that the assignment

$$(m_1, m_2) \mapsto \left(-\left(\frac{x^2-1}{y}\right) m_1 + m_2, x m_1 - \left(\frac{x^2-1}{y}\right) m_2 \right)$$

defines an isomorphism of S-modules: $M \oplus M \cong S \oplus S$.

EXERCISE 2.2.14. Let R be a local ring with maximal ideal $\mathfrak{m}$ and S a commutative R-algebra. Assume S is a finitely generated R-module and $S/\mathfrak{m}S$ is a field. Show that S is a local ring with maximal ideal $\mathfrak{m}S$.

3. Tensor Product

Given a ring R and M and N, we already defined the direct product $M \times N$. In this section we define another product, called the tensor product. The tensor product of a right R-module M and left R-module N is an abelian group denoted $M \otimes_R N$. In general, $M \otimes_R N$ is not an R-module. If R is commutative and A and B are two R-algebras, then the tensor product $A \otimes_R B$ is an R-algebra. When M is fixed and N is treated as a variable, $M \otimes_R (\cdot)$ defines an important functor from the category of left R-modules to the category of abelian groups. Similarly, $(\cdot) \otimes_R N$ defines a functor from the category of right R-modules to the category of abelian groups. When R is commutative and S is an R-algebra, $S \otimes_R (\cdot)$ defines a functor from the category of left R-modules to the category of left S-modules. This section contains many of the fundamental properties of tensor products and the tensor functors.

3.1. Tensor Product of Modules and Homomorphisms.

DEFINITION 2.3.1. Let R be a ring, $M \in \mathfrak{M}_R$ and $N \in {}_R\mathfrak{M}$. Let C be a $\mathbb{Z}$-module. Let $f : M \times N \to C$ be a function. Then f is an *R-balanced map* if it satisfies

(1) $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$,
(2) $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$, and
(3) $f(mr, n) = f(m, rn)$.

for all possible $m_i \in N$, $n_i \in N$, $r \in R$.

DEFINITION 2.3.2. Let R be a ring, $M \in \mathfrak{M}_R$ and $N \in {}_R\mathfrak{M}$. The *tensor product* of M and N over R consists of an abelian group, denoted $M \otimes_R N$, and an R-balanced map $\tau : M \times N \to M \otimes_R N$ satisfying the following universal mapping property. If C is an abelian group and $f : M \times N \to C$ is R-balanced, then there exists a unique homomorphism $\phi : M \otimes_R N \to C$ such that $\phi\tau = f$. Hence the diagram

$$\begin{tikzcd} M \times N \arrow[r, "\tau"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, dashed, "\exists\phi"] \\ & C \end{tikzcd}$$

commutes. The element $\tau(x,y)$ is denoted $x \otimes y$.

THEOREM 2.3.3. *Let R be a ring, $M \in \mathfrak{M}_R$ and $N \in {}_R\mathfrak{M}$.*

(1) The tensor product $M \otimes_R N$ exists and is unique up to isomorphism of abelian groups.
(2) The image of τ generates $M \otimes_R N$. That is, every element of $M \otimes_R N$ can be written as a finite sum of the form $\sum_{i=1}^{n} \tau(m_i, n_i)$.

PROOF. Part (2) follows from the proof of Part (1).

(1): Existence of $M \otimes_R N$. Let $F = \mathbb{Z}^{M \times N}$ be the free $\mathbb{Z}$-module on the set $M \times N$. Write (x,y) as the basis element of F corresponding to (x,y). Let K be the subgroup of F generated by all elements of the form

(1) $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$,
(2) $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$, and
(3) $(mr, n) - (m, rn)$.

We show that F/K satisfies Definition 2.3.2. Define $\tau : M \times N \to F/K$ by $\tau(x,y) = (x,y) + K$. Clearly τ is R-balanced. Since F has a basis consisting of the elements of the form (x,y), the image of τ contains a generating set for the abelian group F/K.

Now we show that F/K satisfies the universal mapping property. Assume that we have a balanced map $f : M \times N \to C$. By Lemma 1.6.11 we define a $\mathbb{Z}$-module homomorphism $h : F \to C$. On a typical basis element (x,y), h is defined to be $h(x,y) = f(x,y)$. This diagram

$$\begin{tikzcd} M \times N \arrow[r, "\tau"] \arrow[dr, "f"'] & F/K \arrow[d, dashed, "\exists\phi"] & F \arrow[l, "\eta"'] \arrow[dl, "h"] \\ & C & \end{tikzcd}$$

commutes. The reader should verify that K is contained in the kernel of h, since f is balanced. So h factors through F/K, showing that ϕ exists. Since F/K is generated by elements of the form $(x,y) + K$ and $\phi((x,y) + K) = f(x,y)$, it is clear that ϕ is unique.

Uniqueness of $M \otimes_R N$. Suppose there exist an abelian group T and an R-balanced map $t : M \times N \to T$ such that Definition 2.3.2 is satisfied. We show that T is isomorphic to $M \otimes_R N$. There exist f and ϕ such that $\tau = ft$ and $t = \phi\tau$. That is, the diagrams

$$\begin{tikzcd} M \times N \arrow[r, "t"] \arrow[dr, "\tau"'] & T \arrow[d, "f"] \\ & M \otimes_R N \end{tikzcd} \qquad \begin{tikzcd} M \times N \arrow[r, "t"] \arrow[dr, "\tau"'] & T \\ & M \otimes_R N \arrow[u, "\phi"'] \end{tikzcd}$$

commute. Notice that both $\psi = 1$ and $\psi = f\phi$ make the diagram

$$\begin{tikzcd} M \times N \arrow[r, "\tau"] \arrow[dr, "\tau"'] & M \otimes_R N \arrow[d, dashed, "\exists\psi"] \\ & M \otimes_R N \end{tikzcd}$$

commute. By the uniqueness of ψ, it follows that $f\phi = 1$. Likewise, $\phi f = 1$. $\square$

EXAMPLE 2.3.4. Let R, M, N be as in Theorem 2.3.3.

(1) It follows from the proof of Theorem 2.3.3 (1) that the identities

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$$
$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$$
$$mr \otimes n = m \otimes rn$$

hold in $M \otimes_R N$.

(2) In $M \otimes_R N$ the zero element is $0 \otimes 0$. Usually the representation of zero is not unique. For instance,

$$x \otimes 0 = x \otimes 0(0) = (x)0 \otimes 0 = 0 \otimes 0,$$

and

$$0 \otimes y = (0)0 \otimes y = 0 \otimes 0(y) = 0 \otimes 0.$$

EXAMPLE 2.3.5. Let $\mathbb{Q}$ denote the additive group of rational numbers. Let $n > 1$. Let $\mathbb{Z}/n$ denote the cyclic group of integers modulo n. A typical generator of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n$ looks like $(a/b) \otimes c$, for $a, b, c \in \mathbb{Z}$. Therefore

$$\frac{a}{b} \otimes c = \frac{na}{nb} \otimes c = \frac{a}{nb} \otimes n(c) = \frac{a}{b} \otimes 0 = 0 \otimes 0$$

which proves $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n = 0$.

LEMMA 2.3.6. *Let $f : M \to M'$ in $\mathfrak{M}_R$ and $g : N \to N'$ in ${}_R\mathfrak{M}$. Then there is a homomorphism of abelian groups*

$$f \otimes g : M \otimes_R N \to M' \otimes_R N'$$

which satisfies $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.

PROOF. Define $\rho : M \times N \to M' \otimes_R N'$ by $\rho(x, y) = f(x) \otimes g(y)$. The reader should check that ρ is balanced. $\square$

LEMMA 2.3.7. *Given*

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$$

in $\mathfrak{M}_R$ and

$$N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3$$

in ${}_R\mathfrak{M}$, the triangle

$$\begin{tikzcd} & M_2 \otimes_R N_2 \arrow[dr, "f_2 \otimes g_2"] & \\ M_1 \otimes_R N_1 \arrow[ur, "f_1 \otimes g_1"] \arrow[rr, "f_2 f_1 \otimes g_2 g_1"] & & M_3 \otimes_R N_3 \end{tikzcd}$$

in the category of $\mathbb{Z}$-modules commutes so that $(f_2 \otimes g_2)(f_1 \otimes g_1) = (f_2 f_1 \otimes g_2 g_1)$.

PROOF. Left to the reader. $\square$

DEFINITION 2.3.8. If S and R are rings and $M \in \mathfrak{M}_R$ and $M \in {}_S\mathfrak{M}$, then M is a *left S right R bimodule* if $s(mr) = (sm)r$ for all possible $s \in S$, $m \in M$ and $r \in R$. Denote by ${}_S\mathfrak{M}_R$ the category of all left S right R bimodules. We say that M is a *left R left S bimodule* if M is both a left R-module and a left S-module and $r(sm) = s(rm)$ for all possible $r \in R$, $m \in M$ and $s \in S$. Denote by ${}_{R-S}\mathfrak{M}$ the category of all left R left S bimodules.

EXAMPLE 2.3.9. Let R and S be two rings.

(1) If I is an ideal in R, the associative law for multiplication in R shows that I is a left R right R bimodule.
(2) If R is a commutative ring, any left R-module M can be made into a left R right R bimodule by defining mr to be rm.
(3) If R is a subring of S, the associative law for multiplication in S shows that S is a left R right R bimodule.
(4) If $\phi : R \to S$ is a homomorphism of rings, then the image of ϕ is a subring of S. As in (3) and Example 1.1.11, we see that R acts on S from both the left and right by the rules $rx = \phi(r)x$ and $xr = x\phi(r)$. The associative law for multiplication in S shows that S is a left R right R bimodule.

If R is a noncommutative ring, the tensor product $M \otimes_R N$ cannot be turned into an R-module per se. If S is another ring and M or N is a bimodule over R and S, then we can turn $M \otimes_R N$ into an S-module. Lemma 2.3.10 lists four such possibilities.

LEMMA 2.3.10. *Let R and S be rings.*

(1) *If M and M' are in ${}_S\mathfrak{M}_R$, and N and N' are in ${}_R\mathfrak{M}$, then the following are true.*
   (a) *$M \otimes_R N$ is in ${}_S\mathfrak{M}$, with the action of S given by $s(m \otimes n) = sm \otimes n$.*
   (b) *If $f : M \to M'$ and $g : N \to N'$ are homomorphisms in ${}_S\mathfrak{M}_R$ and ${}_R\mathfrak{M}$ respectively, then $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ is a homomorphism in ${}_S\mathfrak{M}$.*
(2) *If M and M' are in $\mathfrak{M}_R$, and N and N' are in ${}_{R-S}\mathfrak{M}$, then the following are true.*
   (a) *$M \otimes_R N$ is in ${}_S\mathfrak{M}$, with the action of S given by $s(m \otimes n) = m \otimes sn$.*
   (b) *If $f : M \to M'$ and $g : N \to N'$ are homomorphisms in $\mathfrak{M}_R$ and ${}_{R-S}\mathfrak{M}$ respectively, then $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ is a homomorphism in ${}_S\mathfrak{M}$.*
(3) *If M and M' are in $\mathfrak{M}_{R-S}$, and N and N' are in ${}_R\mathfrak{M}$, then the following are true.*
   (a) *$M \otimes_R N$ is in $\mathfrak{M}_S$, with the action of S given by $(m \otimes n)s = ms \otimes n$.*
   (b) *If $f : M \to M'$ and $g : N \to N'$ are homomorphisms in $\mathfrak{M}_{R-S}$ and ${}_R\mathfrak{M}$ respectively, then $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ is a homomorphism in $\mathfrak{M}_S$.*
(4) *If M and M' are in $\mathfrak{M}_R$, and N and N' are in ${}_R\mathfrak{M}_S$, then the following are true.*
   (a) *$M \otimes_R N$ is in $\mathfrak{M}_S$, with the action of S given by $(m \otimes n)s = m \otimes ns$.*
   (b) *If $f : M \to M'$ and $g : N \to N'$ are homomorphisms in $\mathfrak{M}_R$ and ${}_R\mathfrak{M}_S$ respectively, then $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ is a homomorphism in $\mathfrak{M}_S$.*

PROOF. (1): Given $s \in S$ define $\ell_s : M \times N \to M \otimes_R N$ by $\ell_s(x,y) = s(x \otimes y) = sx \otimes y$. Check that ℓ_s is balanced, hence the action by S on $M \otimes_R N$ is well defined. The rest of (a) is left to the reader. For (b) the reader should verify that $f \otimes g$ is S-linear.

The proofs of (2) – (4) are similar and left to the reader. □

COROLLARY 2.3.11. *Let R be a commutative ring. If M and N are R-modules, then the following are true.*

(1) *$M \otimes_R N$ is a left R-module by the rule: $r(m \otimes n) = rm \otimes n = m \otimes rn$.*
(2) *If $f : M \to M'$ and $g : N \to N'$ are homomorphisms of R-modules, then $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ is a homomorphism of R-modules.*

PROOF. Apply Lemma 2.3.10. $\square$

COROLLARY 2.3.12. *Let $\theta : R \to S$ be a homomorphism of rings. If M and M' are R-modules, then the following are true.*

(1) $S \otimes_R M$ is a left S-module under the action $s_1(s_2 \otimes m) = s_1 s_2 \otimes m$.
(2) If $f : M \to M'$ is an R-module homomorphism, then $1 \otimes f : S \otimes_R M \to S \otimes_R M'$ is an S-module homomorphism.

PROOF. This follows from Lemma 2.3.10 since by Example 2.3.9 parts (3) and (4), S is a left S right R bimodule. $\square$

LEMMA 2.3.13. *If R is a ring, then $R \otimes_R M \cong M$ as left R-modules under the map $x \otimes y \mapsto xy$.*

PROOF. Since $R \in {}_R\mathfrak{M}_R$, given $M \in {}_R\mathfrak{M}$ we view $R \otimes_R M$ as a left R-module. Define $f : R \times M \to M$ by $f(x,y) = xy$. Since M is an R-module, f is balanced. There exists $\phi : R \otimes_R M \to M$ such that the diagram

$$\begin{tikzcd} R \times M \arrow[r, "\tau"] \arrow[dr, "f"'] & R \otimes_R M \arrow[d, "\phi"] \\ & M \end{tikzcd}$$

commutes. Define $\psi : M \to R \otimes M$ by $x \mapsto 1 \otimes x$. The reader should verify that ψ is R-linear. Notice that $\phi\psi(x) = \phi(1 \otimes x) = x$. On a typical generator $\psi\phi(x \otimes y) = 1 \otimes xy = x \otimes y$. It follows that ϕ and ψ are inverses. $\square$

LEMMA 2.3.14. *(Tensor Product Is Associative) Let R and S be rings and assume $L \in \mathfrak{M}_R$, $M \in {}_R\mathfrak{M}_S$ and $N \in {}_S\mathfrak{M}$. Then $(L \otimes_R M) \otimes_S N$ is isomorphic as an abelian group to $L \otimes_R (M \otimes_S N)$ under the map which sends $(x \otimes y) \otimes z$ to $x \otimes (y \otimes z)$.*

PROOF. Fix $z \in N$ and define

$$\begin{gathered} L \times M \xrightarrow{\rho_z} L \otimes_R (M \otimes_S N) \\ (x,y) \mapsto x \otimes (y \otimes z). \end{gathered}$$

The reader should verify that ρ_z is R-balanced. Therefore,

$$\begin{gathered} L \otimes_R M \xrightarrow{f_z} L \otimes_R (M \otimes_S N) \\ x \otimes y \mapsto x \otimes (y \otimes z). \end{gathered}$$

is a well defined homomorphism of groups. The function

$$\begin{aligned} &(L \otimes_R M) \times N \xrightarrow{f} L \otimes_R (M \otimes_S N) \\ &\big(\sum_i x_i \otimes y_i, z\big) \mapsto f_z\big(\sum_i x_i \otimes y_i\big) = \sum_i x_i \otimes (y_i \otimes z). \end{aligned}$$

is well defined. The following equations show that f is balanced.

$$\begin{aligned}
f\big(\sum_i x_i\otimes y_i, z_1+z_2\big) &= \sum_i x_i \otimes \big(y_i\otimes(z_1+z_2)\big)\\
&= \sum_i x_i\otimes(y_i\otimes z_1 + y_i\otimes z_2)\\
&= \sum_i x_i\otimes(y_i\otimes z_1)+\sum_i x_i\otimes(y_i\otimes z_2)\\
&= f\big(\sum_i x_i\otimes y_i, z_1\big)+f\big(\sum_i x_i\otimes y_i, z_2\big)
\end{aligned}$$

$$\begin{aligned}
f\Big(\sum_{i=1}^{k} x_i\otimes y_i + \sum_{i=k+1}^{\ell} x_i\otimes y_i, z\Big) &= \sum_{i=1}^{\ell} x_i\otimes(y_i\otimes z)\\
&= \sum_{i=1}^{k} x_i\otimes(y_i\otimes z)+\sum_{i=k+1}^{\ell} x_i\otimes(y_i\otimes z)\\
&= f\Big(\sum_{i=1}^{k} x_i\otimes y_i, z\Big)+f\Big(\sum_{i=k+1}^{\ell} x_i\otimes y_i, z\Big)
\end{aligned}$$

$$\begin{aligned}
f\big(\sum_i x_i\otimes y_i s, z\big) &= \sum_i x_i\otimes(y_i s\otimes z)\\
&= \sum_i x_i\otimes(y_i\otimes sz)\\
&= f\big(\sum_i x_i\otimes y_i, sz\big)
\end{aligned}$$

In the diagram

$$\begin{tikzcd}
(L\otimes_R M)\times_S N \arrow[r, "\tau"] \arrow[dr, "f"'] & (L\otimes_R M)\otimes_S N \arrow[d, "\phi"]\\
& L\otimes_R(M\otimes_S N)
\end{tikzcd}$$

the homomorphism ϕ is well defined. The inverse of ϕ is defined in a similar way. $\square$

Lemma 2.3.15 shows that tensoring distributes across a direct sum. The analogous result for a direct product is false if the index set is infinite. For a counterexample, see Example 3.5.10.

LEMMA 2.3.15. *(Tensor Product Distributes over a Direct Sum) Let M and $\{M_i\}_{i\in I}$ be right R-modules. Let N and $\{N_j\}_{j\in J}$ be left R-modules. There are isomorphisms of abelian groups*

$$M\otimes_R\Big(\bigoplus_{j\in J} N_j\Big)\cong\bigoplus_{j\in J}(M\otimes_R N_j)$$

and

$$\Big(\bigoplus_{i\in I} M_i\Big)\otimes_R N\cong\bigoplus_{i\in I}(M_i\otimes_R N).$$

PROOF. Define $\rho : \big(\bigoplus M_i\big)\times N\to\bigoplus\big(M_i\otimes N\big)$ by $\rho(f,n)=g$ where $g(i)=f(i)\otimes n$. We prove that ρ is balanced. First, say $f_1,f_2\in\bigoplus M_i$ and $\rho(f_1+f_2,n)=g$, $\rho(f_1,n)=g_1$

and $\rho(f_2,n) = g_2$. Then

$$\begin{aligned} g(i) &= \big(f_1(i) + f_2(i)\big) \otimes n \\ &= f_1(i) \otimes n + f_2(i) \otimes n \\ &= g_1(i) + g_2(i) \end{aligned}$$

which shows $g = g_1 + g_2$. Next say $\rho(fr,n) = g$ and $\rho(f,rn) = h$. Then

$$\begin{aligned} g(i) &= \big(fr(i) \otimes n \\ &= f(i)r \otimes n \\ &= f(i) \otimes rn \\ &= h(i) \end{aligned}$$

which shows $g = h$. Clearly $\rho(f,n_1+n_2) = \rho(f,n_1) + \rho(f,n_2)$. Therefore the homomorphism ϕ exists and the diagram

$$\begin{tikzcd} \big(\bigoplus M_i\big) \times N \arrow[r, "\tau"] \arrow[dr, "\rho"'] & \big(\bigoplus M_i\big) \otimes N \arrow[d, "\phi"] \\ & \bigoplus \big(M_i \otimes N\big) \end{tikzcd}$$

commutes. Let $\iota_j : M_j \to \bigoplus M_i$ be the injection of the jth summand into the direct sum. Let $\psi_j = \iota_j \otimes 1$. Then $\psi_j : M_j \otimes N \to \big(\bigoplus M_i\big) \otimes N$. Define $\psi = \bigoplus \psi_i$ to be the direct sum map of Exercise 1.6.15. Then $\psi : \bigoplus \big(M_i \otimes N\big) \to \big(\bigoplus M_i\big) \otimes N$. The reader should verify that ϕ and ψ are inverses of each other. $\square$

LEMMA 2.3.16. *Let R be a ring, M a right R-module and N a left R-module. Then $M \otimes_R N \cong N \otimes_{R^o} M$ under the map $x \otimes y \mapsto y \otimes x$.*

PROOF. Define $\rho : M \times N \to N \otimes_{R^o} M$ by $\rho(x,y) = y \otimes x$. Then

$$\begin{aligned} \rho(x_1 + x_2, y) &= y \otimes (x_1 + x_2) \\ &= y \otimes x_1 + y \otimes x_2 \\ &= \rho(x_1,y) + \rho(x_2,y). \end{aligned}$$

Likewise $\rho(x, y_1 + y_2) = \rho(x,y_1) + \rho(x,y_2)$. Also

$$\begin{aligned} \rho(xr,y) &= y \otimes xr \\ &= y \otimes r * x \\ &= y * r \otimes x \\ &= ry \otimes x \\ &= \rho(x,ry) \end{aligned}$$

which shows ρ is balanced. There exists a homomorphism ϕ and the diagram

$$\begin{tikzcd} M \times N \arrow[r, "\tau"] \arrow[dr, "\rho"'] & M \otimes_R N \arrow[d, "\phi"] \\ & N \otimes_{R^o} M \end{tikzcd}$$

commutes. Since $R = (R^o)^o$, it is clear that ϕ is an isomorphism. $\square$

3.2. Tensor Functor.

LEMMA 2.3.17. *Let R be a ring.*

(1) *If M is a right R-module, then tensoring with M defines a covariant functor $M \otimes_R (\cdot) : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$ from the category of left R-modules to the category of abelian groups.*
(2) *If S is a ring and M is a left S right R bimodule, then $M \otimes_R (\cdot)$ defines a covariant functor from ${}_R\mathfrak{M}$ to ${}_S\mathfrak{M}$.*
(3) *If R is a commutative ring and M is an R module, then $M \otimes_R (\cdot)$ defines a covariant functor from ${}_R\mathfrak{M}$ to ${}_R\mathfrak{M}$.*
(4) *If $\theta : R \to S$ is a homomorphism of rings, then $S \otimes_R (\cdot)$ defines a covariant functor from ${}_R\mathfrak{M}$ to ${}_S\mathfrak{M}$.*

If N is a left R-module, then versions of (1) – (3) hold for the functor defined by $(\cdot) \otimes_R N$ provided the roles of left and right are switched. The right hand version of (4) holds for the functor defined by $(\cdot) \otimes_R B$.

PROOF. (1): For any object N in the category ${}_R\mathfrak{M}$ we can construct the $\mathbb{Z}$-module $M \otimes_R N$. Given any homomorphism $f \in \operatorname{Hom}_R(A,B)$, there is a homomorphism $1 \otimes f : M \otimes_R A \to M \otimes_R B$. By Lemma 2.3.7, the composition of functions is preserved by tensoring with M.

For Part (2), use Part (1) and Lemma 2.3.10. For Part (3), use Part (1) and Corollary 2.3.11. For Part (4), use Part (1) and Corollary 2.3.12. □

LEMMA 2.3.18. *(Tensoring Is Right Exact.) Let R be a ring and M a right R-module. Given a short exact sequence in ${}_R\mathfrak{M}$*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

the sequence

$$M \otimes_R A \xrightarrow{1\otimes\alpha} M \otimes_R B \xrightarrow{1\otimes\beta} M \otimes_R C \to 0$$

is an exact sequence of $\mathbb{Z}$-modules.

PROOF. Step 1: Show that $1 \otimes \beta$ is onto. Given an element $x \otimes c$ in $M \otimes_R C$, use the fact that β is onto and find $b \in B$ such that $\beta(b) = c$. Notice that $(1 \otimes \beta)(x \otimes b) = x \otimes c$. The image of $1 \otimes \beta$ contains a generating set for $M \otimes_R C$.

Step 2: $\operatorname{im}(1 \otimes \alpha) \subseteq \ker(1 \otimes \beta)$. By Lemma 2.3.7, $(1 \otimes \beta) \circ (1 \otimes \alpha) = 1 \otimes \beta\alpha = 1 \otimes 0 = 0$.

Step 3: $\operatorname{im}(1 \otimes \alpha) \supseteq \ker(1 \otimes \beta)$. Write $E = \operatorname{im}(1 \otimes \alpha)$. By Step 2, $E \subseteq \ker(1 \otimes \beta)$ so $1 \otimes \beta$ factors through $M \otimes_R B/E$, giving

$$\bar{\beta} : \frac{M \otimes_R B}{E} \to M \otimes_R C.$$

It is enough to show that $\bar{\beta}$ is an isomorphism. To do this, we construct the inverse map. First, let $c \in C$ and consider two elements b_1, b_2 in $\beta^{-1}(c)$. Then $\beta(b_1 - b_2) = \beta(b_1) - \beta(b_2) = c - c = 0$. That is, $b_1 - b_2 \in \ker\beta = \operatorname{im}\alpha$. For any $x \in M$, it follows that $x \otimes b_1 - x \otimes b_2 = x \otimes (b_1 - b_2) \in \operatorname{im}(1 \otimes \alpha) = E$. Therefore we can define a function

$$\begin{aligned} M \times C &\xrightarrow{f} \frac{M \otimes_R B}{E} \\ (x,c) &\mapsto x \otimes b + E \end{aligned}$$

where b is an arbitrary element in $\beta^{-1}(c)$. The reader should verify that f is R-balanced. So there exists a homomorphism γ making the diagram

$$\begin{tikzcd}
M \times C \arrow[r, "\tau"] \arrow[dr, "f"'] & M \otimes_R C \arrow[d, "\gamma"] \\
 & \frac{M \otimes_R B}{E}
\end{tikzcd}$$

commutative. By construction, $\gamma = \bar{\beta}^{-1}$. □

DEFINITION 2.3.19. By Lemma 2.3.18 the functor $M \otimes_R (\cdot)$ is right exact. In case $M \otimes_R (\cdot)$ is also left exact, then we say M is a *flat* R-module.

EXAMPLE 2.3.20. Take $R = \mathbb{Z}$, $M = \mathbb{Z}/n$. The sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

is exact. In $M \otimes \mathbb{Q}$, $1 \otimes 1$ is equal to $1 \otimes n/n = n \otimes 1/n = 0 \otimes 0$. So tensoring the previous sequence with $M \otimes (\cdot)$,

$$0 \to \mathbb{Z}/n \to 0 \to 0 \to 0$$

is not exact. As a $\mathbb{Z}$-module, $\mathbb{Z}/n$ is not flat.

In Lemma 2.3.21 below, we show that the tensor product of two R-algebras is an R-algebra. In other words, tensor product defines a product on the category of R-algebras.

LEMMA 2.3.21. *If A and B are R-algebras, then $A \otimes_R B$ is an R-algebra with multiplication induced by $(x_1 \otimes y_1)(x_2 \otimes y_2) = x_1x_2 \otimes y_1y_2$.*

PROOF. Using Corollary 2.3.11 (1), the tensor product of R-modules is an R-module. Using Lemma 2.3.16, the "twist" map

$$\begin{aligned} \tau : A \otimes_R B &\to B \otimes_R A \\ x \otimes y &\mapsto y \otimes x \end{aligned}$$

is an R-module isomorphism. The reader should verify that multiplication in A and in B induce R-module homomorphisms

$$\begin{aligned} \mu : A \otimes_R A &\to A \\ x \otimes y &\mapsto xy \end{aligned}$$

and

$$\begin{aligned} \nu : B \otimes_R B &\to B \\ x \otimes y &\mapsto xy \end{aligned}$$

respectively. Consider the R-module homomorphisms

$$\begin{aligned} (A \otimes_R B) \otimes_R (A \otimes_R B) &\xrightarrow{\cong} A \otimes_R (B \otimes_R A) \otimes_R B \\ &\xrightarrow{1 \otimes \tau \otimes 1} A \otimes_R (A \otimes_R B) \otimes_R B \\ &\xrightarrow{\cong} (A \otimes_R A) \otimes_R (B \otimes_R B) \\ &\xrightarrow{\mu \otimes \nu} A \otimes_R B. \end{aligned} \tag{3.1}$$

Since it is defined by the composition of the homomorphisms in (3.1), the multiplication rule in $A \otimes_R B$ is well defined. The reader should verify that the associative and distributive laws hold. The multiplicative identity is $1 \otimes 1$. If $r \in R$, then $r \otimes 1 = 1 \otimes r$ in $A \otimes_R B$.

The reader should verify that $r \mapsto r \otimes 1$ defines a homomorphism from R to the center of $A \otimes_R B$. $\square$

LEMMA 2.3.22. *Let R be a commutative ring and let A and B be R-algebras. Let M be a left A-module and N a left B-module. Given $a \in A$, $b \in B$, $x \in M$, and $y \in N$, if $(a \otimes b)(x \otimes y)$ is defined to be $ax \otimes by$, then this makes $M \otimes_R N$ into a left $A \otimes_R B$-module.*

PROOF. The R-algebras A and B come with homomorphisms $\theta_1 : R \to A$ and $\theta_2 : R \to B$ satisfying $\operatorname{im}(\theta_1) \subseteq Z(A)$ and $\operatorname{im}(\theta_2) \subseteq Z(B)$. Therefore, A and B are both left R right R bimodules and by Example 2.3.9 we can view M as a left A right R bimodule and N as a left B left R bimodule. By Lemma 2.3.10, $M \otimes_R N$ is a left A-module and a left B-module. By Example 1.1.13, the left regular representations of A and B are R-algebra homomorphisms $\phi_1 : A \to \operatorname{Hom}_R(M \otimes_R N, M \otimes_R N)$ and $\phi_2 : B \to \operatorname{Hom}_R(M \otimes_R N, M \otimes_R N)$. Therefore $\phi_1(a)\phi_2(b)(x \otimes y) = ax \otimes by = \phi_2(b)\phi_1(a)(x \otimes y)$, which shows elements in the image of ϕ_1 commute with elements in the image of ϕ_2. By Exercise 2.3.6, there exists an R-algebra homomorphism $\gamma : A \otimes_R B \to \operatorname{Hom}_R(M \otimes_R N, M \otimes_R N)$ such that the diagram

$$\begin{tikzcd}
 & \operatorname{Hom}_R(M \otimes_R N, M \otimes_R N) & \\
A \arrow[ur, "\phi_1"] \arrow[r, "\rho_1"'] & A \otimes_R B \arrow[u, "\gamma"'] & B \arrow[ul, "\phi_2"'] \arrow[l, "\rho_2"]
\end{tikzcd}$$

commutes. By Lemma 1.1.10, this makes $M \otimes_R N$ into a left $A \otimes_R B$-module. Finally, left multiplication of $x \otimes y$ by $a \otimes b$ is equal to $ax \otimes by$, $\square$

In Theorem 2.3.23 below we show that given a homomorphism of rings $\phi : A \to B$, there is a change of base ring functor from the category of right A-modules to the category of right B-modules given by the tensor functor $(\cdot) \otimes_A B$.

THEOREM 2.3.23. *Let $\phi : A \to B$ be a homomorphism of rings. As in Example 2.3.9, ϕ makes B into a left A right A bimodule.*

(1) The assignment $M \mapsto M \otimes_A B$ defines a right exact covariant functor $\mathfrak{M}_A \to \mathfrak{M}_B$ which satisfies:
   (a) A is mapped to B.
   (b) Any direct sum $\bigoplus_{i \in I} M_i$ is mapped to the direct sum $\bigoplus_{i \in I} (M_i \otimes_A B)$.
   (c) The free module A^I is mapped to the free B-module B^I.
(2) If M is A-projective, then $M \otimes_A B$ is B-projective.
(3) If M is an A-generator, then $M \otimes_A B$ is a B-generator.
(4) If M is finitely generated over A, then $M \otimes_A B$ is finitely generated over B.
(5) If M is a flat A-module, then $M \otimes_A B$ is a flat B-module.

Left hand versions of (1) – (5) hold for the covariant functor ${}_A\mathfrak{M} \to {}_B\mathfrak{M}$ which is defined by $M \mapsto B \otimes_A M$.

PROOF. (1): Apply Lemmas 2.3.13, 2.3.15, 2.3.17, and 2.3.18.

(2): By Proposition 2.1.1, M is a direct summand of a free A-module. By (1), $M \otimes_A B$ is a direct summand of a free B-module.

(3): If $M^{(n)} \to A \to 0$ is an exact sequence of right A-modules, then by (1)

$$(M \otimes_A B)^{(n)} \to B \to 0$$

is an exact sequence of right B-modules. By Exercise 2.2.9 we are done.

(4): If $A^{(n)} \to M \to 0$ is an exact sequence of right A-modules, then by (1)

$$B^{(n)} \to M \otimes_A B \to 0$$

is an exact sequence of right B-modules. By Lemma 1.6.11 we are done.

(5): Is left to the reader. □

In Proposition 2.3.24 below, R is a ring and M and N are two-sided R-bimodules. Given that M and N both have a certain property, we ask whether the tensor product $M \otimes_R N$ also has that same property.

PROPOSITION 2.3.24. *Let R be a ring and let M and N be left R right R-bimodules.*

(1) If M and N are finitely generated as left R-modules, then $M \otimes_R N$ is finitely generated as a left R-module.

(2) If M and N are projective as left R-modules, then $M \otimes_R N$ is projective as a left R-module.

(3) If M and N are left R-generator modules, then $M \otimes_R N$ is a left R-generator module.

(4) If M and N are left R-progenerator modules, then $M \otimes_R N$ is a left R-progenerator module.

Right hand versions of (1) – (4) hold.

PROOF. (1): We are given exact sequences of left R-modules

$$R^{(m)} \xrightarrow{\alpha} M \to 0 \tag{3.2}$$

and

$$R^{(n)} \xrightarrow{\beta} N \to 0. \tag{3.3}$$

Tensor (3.2) with $(\cdot) \otimes_R N$ to get the exact sequence of left R-modules

$$R^{(m)} \otimes_R N \xrightarrow{\alpha \otimes 1} M \otimes_R N \to 0. \tag{3.4}$$

Tensor (3.3) with $R^{(m)} \otimes_R (\cdot)$ to get the exact sequence of left R-modules

$$R^{(m)} \otimes_R R^{(n)} \xrightarrow{1 \otimes \beta} R^{(m)} \otimes_R N \to 0. \tag{3.5}$$

The composition map $(\alpha \otimes 1) \circ (1 \otimes \beta)$ is onto.

(2): Start with dual bases $\{(f_i, m_i) \mid i \in I\}$ for M and $\{(g_j, n_j) \mid j \in J\}$ for N. Then $f_i \otimes g_j \in \operatorname{Hom}_R(M \otimes_R N, R)$. For a typical generator $x \otimes y$ of $M \otimes_R N$, the following equations

$$\begin{aligned}
\sum_{(i,j)} (f_i \otimes g_j)(x \otimes y)(m_i \otimes n_j) &= \sum_{(i,j)} (f_i(x) g_j(y)(m_i \otimes n_j) \\
&= \sum_{(i,j)} f_i(x) m_i \otimes g_j(y) n_j) \\
&= \sum_i \Big(f_i(x) m_i \otimes \big(\sum_j g_j(y) n_j\big)\Big) \\
&= \sum_i \big(f_i(x) m_i \otimes y \big) \\
&= \big(\sum_i f_i(x) m_i\big) \otimes y \\
&= x \otimes y
\end{aligned}$$

show that $\{(f_i \otimes g_j, m_i \otimes n_j) \mid (i,j) \in I \times J\}$ is a dual basis for $M \otimes_R N$.

(3): By Exercise 2.2.9, there are exact sequences

$$M^{(m)} \xrightarrow{\alpha} R \to 0 \tag{3.6}$$

and

$$N^{(n)} \xrightarrow{\beta} R \to 0. \tag{3.7}$$

Tensor (3.6) with $(\cdot) \otimes_R N^{(n)}$ to get the exact sequence

$$M^{(m)} \otimes_R N^{(n)} \xrightarrow{\alpha\otimes 1} R \otimes_R N^{(n)} \to 0. \tag{3.8}$$

Then the composition $(1 \otimes \beta) \circ (\alpha \otimes 1)$ maps $(M \otimes_R N)^{(mn)}$ onto R.

(4): Follows from (1), (2) and (3). □

In Proposition 2.3.25 below, R is a ring and M and N are two-sided R-bimodules. If the tensor product $M \otimes_R N$ has a certain property, we ask whether M and N also have that same property.

PROPOSITION 2.3.25. *Let R be a ring. Let M and N be left R right R-bimodules. Assume $M \otimes_R N$ is a left R-generator module. Then the following are true.*

(1) M and N are both left R-generator modules.
(2) If $M \otimes_R N$ is projective as a left R-module, then M and N are both projective as left R-modules.
(3) If $M \otimes_R N$ is finitely generated as a left R-module, then M and N are both finitely generated as left R-modules.
(4) If $M \otimes_R N$ is a left progenerator over R, then M and N are both left progenerators over R.

If $M \otimes_R N$ is a right R-generator module, then right hand versions of (1) – (4) hold for M and N.

PROOF. (1): By Exercise 2.2.9 there is a free R-module F_1 of finite rank and a homomorphism f_1 of left R-modules such that $f_1 : F_1 \otimes_R (M \otimes_R N) \to R$ is onto. By Lemma 1.6.11 there is a free R-module F_2 and a left R-module homomorphism f_2 such that $f_2 : F_2 \to M$ is onto. By Lemma 2.3.18,

$$F_2 \otimes_R N \xrightarrow{f_2\otimes 1} M \otimes_R N \to 0$$

is exact. For the same reason,

$$F_1 \otimes_R (F_2 \otimes_R N) \xrightarrow{1\otimes f_2\otimes 1} F_1 \otimes_R (M \otimes_R N) \to 0$$

is exact. Since $F_1 \otimes_R F_2$ is a free R-module, Lemma 2.3.14 and Lemma 2.3.15 show that $F_1 \otimes_R (F_2 \otimes_R N)$ is a direct sum of copies of N. Then $f_1 \circ (1 \otimes f_2 \otimes 1)$ maps a direct sum of copies of N onto R. Use Exercise 2.2.9 again to show N is a left R-module generator. The other case is left to the reader.

(2) and (3): By Part (1) and Exercise 2.2.9 there is a free R-module F of finite rank and a left R-module homomorphism f such that $N \otimes_R F \xrightarrow{f} R$ is onto. But f is split since R is projective over R. By Exercise 2.3.6,

$$M \otimes_R N \otimes_R F \xrightarrow{f\otimes 1} M \to 0$$

is split exact. If $M \otimes_R N$ is projective, then by Lemma 2.3.15 and Exercise 2.2.6, M is projective. If $M \otimes_R N$ is finitely generated, then so is M. The other cases are left to the reader. □

3.3. Exercises.

EXERCISE 2.3.1. Assume A is a $\mathbb{Z}$-module and $m > 0$. Prove that $A \otimes_{\mathbb{Z}} \mathbb{Z}/m \cong A/mA$.

EXERCISE 2.3.2. If $m > 0$, $n > 0$ and $d = \gcd(m,n)$, then $\mathbb{Z}/m \otimes_{\mathbb{Z}} \mathbb{Z}/n \cong \mathbb{Z}/d$.

EXERCISE 2.3.3. Let R be a ring, M a right R-module, N a left R-module. If M' is a submodule of M and N' is a submodule of N, then show that $M/M' \otimes_R N/N' \cong (M \otimes_R N)/C$ where C is the subgroup of $M \otimes_R N$ generated by all elements of the form $x' \otimes y$ and $x \otimes y'$ with $x \in M$, $x' \in M'$, $y \in N$ and $y' \in N'$.

EXERCISE 2.3.4. Let $B = \langle b \rangle$ be the cyclic group of order four, $A = \langle 2b \rangle$ the subgroup of order two and $\alpha : A \to B$ the homomorphism defined by $A \subseteq B$. Show that the groups $A \otimes_{\mathbb{Z}} A$ and $A \otimes_{\mathbb{Z}} B$ are both nonzero. Show that $1 \otimes \alpha : A \otimes_{\mathbb{Z}} A \to A \otimes_{\mathbb{Z}} B$ is the zero homomorphism.

EXERCISE 2.3.5. Let R be a ring and let R^I and R^J be free R-modules.

(1) Show that $R^I \otimes_R R^J$ is a free R-module.
(2) If A is a free R-module of rank m and B is a free R-module of rank n, then show that $A \otimes_R B$ is free of rank mn.

EXERCISE 2.3.6. Let

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{3.9}$$

be a short exact sequence of left R-modules. Given a right R-module M, consider the sequence

$$0 \to M \otimes_R A \xrightarrow{1\otimes\alpha} M \otimes_R B \xrightarrow{1\otimes\beta} M \otimes_R C \to 0. \tag{3.10}$$

Prove:

(1) If (3.9) is split exact, then (3.10) is split exact.
(2) If M is a free right R-module, then (3.10) is exact, hence M is flat.
(3) If M is a projective right R-module, then (3.10) is exact, hence M is flat.

EXERCISE 2.3.7. If R is any ring and M is an R-module, use Exercise 2.3.6 and Exercise 2.2.5 to show that M has a *flat resolution*.

EXERCISE 2.3.8. Let R be a ring and I a right ideal of R. Let B be a left R-module. Prove that there is an isomorphism of groups

$$R/I \otimes_R B \cong B/IB$$

where IB is the subgroup of B generated by $\{rx \mid r \in I, x \in B\}$.

EXERCISE 2.3.9. Prove that if R is a commutative ring with ideals I and J, then there is an isomorphism of R-modules

$$R/I \otimes_R R/J \cong R/(I+J).$$

EXERCISE 2.3.10. Let R be a commutative ring. Suppose A and B are R-algebras. Then A and B come with homomorphisms $\theta_1 : R \to A$ and $\theta_2 : R \to B$ satisfying $\operatorname{im}(\theta_1) \subseteq Z(A)$ and $\operatorname{im}(\theta_2) \subseteq Z(B)$.

(1) Show that there exist R-algebra homomorphisms $\rho_1 : A \to A \otimes_R B$ and $\rho_2 : B \to A \otimes_R B$ such that the diagram

(3.11)
$$\begin{tikzcd} & A \otimes_R B & \\ A \arrow[ur, "\rho_1"] & & B \arrow[ul, "\rho_2"'] \\ & R \arrow[ul, "\theta_1"] \arrow[ur, "\theta_2"'] & \end{tikzcd}$$

commutes. Show that $\mathrm{im}(\rho_1)$ commutes with $\mathrm{im}(\rho_2)$. That is, $\rho_1(x)\rho_2(y) = \rho_2(y)\rho_1(x)$ for all $x \in A$, $y \in B$.

(2) Suppose there exist R-algebra homomorphisms $\alpha : A \to C$ and $\beta : B \to C$ such that $\mathrm{im}(\alpha)$ commutes with $\mathrm{im}(\beta)$. Show that there exists a unique R-algebra homomorphism $\gamma : A \otimes_R B \to C$ such that the diagram

(3.12)
$$\begin{tikzcd} & C & \\ A \arrow[ur, "\alpha"] \arrow[r, "\rho_1"'] & A \otimes_R B \arrow[u, dashed, "\exists\gamma"'] & B \arrow[ul, "\beta"'] \arrow[l, "\rho_2"] \end{tikzcd}$$

commutes.

(3) Show that if there exists an R-algebra homomorphism $\gamma : A \otimes_R B \to C$, then there exist R-algebra homomorphisms $\alpha : A \to C$ and $\beta : B \to C$ such that the image of α commutes with the image of β and diagram (3.12) commutes.

EXERCISE 2.3.11. Let S be a commutative R-algebra. Show that there is a well defined homomorphism of R-algebras $\mu : S \otimes_R S \to S$ which maps a typical element $\sum x_i \otimes y_i$ in the tensor algebra to $\sum x_i y_i$ in S.

EXERCISE 2.3.12. Let R be a commutative ring and let A and B be R-algebras. Prove that $A \otimes_R B \cong B \otimes_R A$ as R-algebras.

EXERCISE 2.3.13. Let A be an R-algebra. Show that $A \otimes_R R[x] \cong A[x]$ as R-algebras.

EXERCISE 2.3.14. Let S and T be commutative R-algebras. Prove:

(1) If S and T are both finitely generated R-algebras, then $S \otimes_R T$ is a finitely generated R-algebra.
(2) If T is a finitely generated R-algebra, then $S \otimes_R T$ is a finitely generated S-algebra.

EXERCISE 2.3.15. Let R be a commutative ring. Prove that if I is an ideal in R, then $I \otimes_R R[x] \cong I[x]$ and $R[x]/I[x] \cong (R/I)[x]$.

EXERCISE 2.3.16. Let $\theta : R \to S$ be a homomorphism of rings. Let $M \in \mathfrak{M}_S$ and $N \in {}_S\mathfrak{M}$. Via θ, M can be viewed as a right R-module and N as a left R-module. Show that θ induces a well defined $\mathbb{Z}$-module epimorphism $M \otimes_R N \to M \otimes_S N$. (Note: The dual result, how a Hom group behaves when the ring in the middle is changed, is studied in Exercise 1.1.4.)

EXERCISE 2.3.17. Let $\theta : R \to S$ be a homomorphism of rings. Let $M \in \mathfrak{M}_R$ and $N \in {}_R\mathfrak{M}$, $M' \in \mathfrak{M}_S$ and $N' \in {}_S\mathfrak{M}$. Via θ, M' and N' are viewed as R-modules. In this context, let $f : M \to M'$ be a right R-module homomorphism and $g : N \to N'$ a left R-module homomorphism. Using Lemma 2.3.6 and Exercise 2.3.16, show that there is a well defined $\mathbb{Z}$-module homomorphism $M \otimes_R N \to M' \otimes_S N'$ which satisfies $x \otimes y \mapsto f(x) \otimes g(y)$.

EXERCISE 2.3.18. Let R be a commutative ring and S a commutative R-algebra. Let A be an S-algebra. Using Exercise 2.3.16, show that there is a well defined epimorphism of rings $A \otimes_R A \to A \otimes_S A$.

EXERCISE 2.3.19. Prove that if A is an R-algebra, then $A \otimes_R M_n(R) \cong M_n(A)$ as R-algebras.

EXERCISE 2.3.20. Let R be an integral domain and K the field of fractions of R. Show that $M \otimes_R K = 0$, if M is a torsion R-module (Definition 1.7.13).

EXERCISE 2.3.21. Let k be a field and $n > 1$ an integer. Let $T = k[x,y]$, $S = k[x^n, xy, y^n]$, and $R = k[x^n, y^n]$. For the tower of subrings $R \subseteq S \subseteq T$, prove:

(1) T is free over R of rank n^2.
(2) S is free over R of rank n.
(3) T is not free over S. (Hint: Consider the residue class rings $S/(x^n, xy, y^n)$ and $T/(x^n, xy, y^n)$.)

For more properties of the ring $k[x^n, xy, y^n]$, see Exercise 11.4.2.

4. Hom Groups

If R is a ring and M and N are R-modules, then $\operatorname{Hom}_R(M,N)$ is the set of R-module homomorphisms from M to N. Then $\operatorname{Hom}_R(M,N)$ is an additive group under point-wise addition:

$$(f+g)(x) = f(x) + g(x).$$

If R is commutative, then $\operatorname{Hom}_R(M,N)$ can be turned into a left R-module by defining $(rf)(x) = rf(x)$. If R is noncommutative, then $\operatorname{Hom}_R(M,N)$ cannot be turned into an R-module per se. If S is another ring and M or N is a bimodule over R and S, then we can turn $\operatorname{Hom}_R(M,N)$ into an S-module. Lemma 2.4.1 lists four such possibilities.

LEMMA 2.4.1. *Let R and S be rings.*

(1) If M is a left R right S bimodule and N is a left R-module, then $\operatorname{Hom}_R(M,N)$ is a left S-module, with the action of S given by $(sf)(m) = f(ms)$.
(2) If M is a left R-module and N is a left R right S bimodule, then $\operatorname{Hom}_R(M,N)$ is a right S-module, with the action of S given by $(fs)(m) = (f(m))s$.
(3) If M is a left R left S bimodule and N is a left R-module, then $\operatorname{Hom}_R(M,N)$ is a right S-module, with the action of S given by $(fs)(m) = f(sm)$.
(4) If M is a left R-module and N is a left R left S bimodule, then $\operatorname{Hom}_R(M,N)$ is a left S-module, with the action of S given by $(sf)(m) = s(f(m))$.

PROOF. Is left to the reader. □

Let R be a ring and M a left R-module. Then $\operatorname{Hom}_R(M,M)$ is a ring where multiplication is composition of functions:

$$(fg)(x) = f(g(x)).$$

By Example 1.1.14, the ring $S = \operatorname{Hom}_R(M,M)$ acts as a ring of functions on M and this makes M a left S-module. If R is commutative, then $S = \operatorname{Hom}_R(M,M)$ is an R-algebra. The next two results are corollaries to Lemma 2.2.1 (Nakayama's Lemma).

COROLLARY 2.4.2. *Let R be a commutative ring and M a finitely generated R-module. Let $f : M \to M$ be an R-module homomorphism such that f is onto. Then f is one-to-one.*

PROOF. Let $R[x]$ be the polynomial ring in one variable over R. We turn M into an $R[x]$-module using f. Given $m \in M$ and $p(x) \in R[x]$, define

$$p(x) \cdot m = p(f)(m).$$

Since M is finitely generated over R, M is finitely generated over $R[x]$. Let I be the ideal in $R[x]$ generated by x. Then $IM = M$ because f is onto. By Nakayama's Lemma 2.2.1, $I + \operatorname{annih}_{R[x]} M = R[x]$. For some $p(x)x \in I$, $1 - p(x)x \in \operatorname{annih}_{R[x]} M$. Then $(1 - p(x)x)M = 0$ which says for each $m \in M$, $m = (p(f)f)(m)$. Then $p(f)f$ is the identity function, so f is one-to-one. □

COROLLARY 2.4.3. *Let R be a commutative ring, M an R-module, N a finitely generated R-module, and $f \in \operatorname{Hom}_R(M,N)$. Then f is onto if and only if for each maximal ideal $\mathfrak{m}$ in R, the induced map $\bar{f} : M/\mathfrak{m}M \to N/\mathfrak{m}N$ is onto.*

PROOF. Let C denote the cokernel of f and let $\mathfrak{m}$ be an arbitrary maximal ideal of R. Since N is finitely generated, so is C. Tensor the exact sequence

$$M \xrightarrow{f} N \to C \to 0$$

with $(\cdot) \otimes_R R/\mathfrak{m}$ to get

$$M/\mathfrak{m}M \xrightarrow{\bar{f}} N/\mathfrak{m}N \to C/\mathfrak{m}C \to 0$$

which is exact since tensoring is right exact. If f is onto, then $C = 0$ so $\bar{f}$ is onto. Conversely if $\mathfrak{m}C = C$ for every $\mathfrak{m}$, then Corollary 2.2.2 (Corollary to Nakayama's Lemma) implies $C = 0$. □

4.1. Hom Functor.

LEMMA 2.4.4. *For a ring R and a left R-module M, the following are true.*

(1) $\operatorname{Hom}_R(M,\cdot)$ *is a covariant functor from ${}_R\mathfrak{M}$ to ${}_\mathbb{Z}\mathfrak{M}$ which sends a left R module N to the abelian group* $\operatorname{Hom}_R(M,N)$. *Given any R-module homomorphism $f : A \to B$, there is a homomorphism of groups*

$$\operatorname{Hom}_R(M,A) \xrightarrow{\mathrm{H}_f} \operatorname{Hom}_R(M,B)$$

which is defined by the assignment $g \mapsto fg$.

(2) $\operatorname{Hom}_R(\cdot,M)$ *is a contravariant functor from ${}_R\mathfrak{M}$ to ${}_\mathbb{Z}\mathfrak{M}$ which sends a left R module N to the abelian group* $\operatorname{Hom}_R(N,M)$. *Given any R-module homomorphism $f : A \to B$, there is a homomorphism of groups*

$$\operatorname{Hom}_R(B,M) \xrightarrow{\mathrm{H}_f} \operatorname{Hom}_R(A,M)$$

which is defined by the assignment $g \mapsto gf$.

PROOF. Is left to the reader. □

PROPOSITION 2.4.5. *Let R be a ring and M a left R-module.*

(1) $\operatorname{Hom}_R(M,\cdot)$ *is a left exact covariant functor from ${}_R\mathfrak{M}$ to ${}_\mathbb{Z}\mathfrak{M}$.*
(2) M is projective if and only if $\operatorname{Hom}_R(M,\cdot)$ *is an exact functor.*
(3) $\operatorname{Hom}_R(\cdot,M)$ *is a left exact contravariant functor from ${}_R\mathfrak{M}$ to ${}_\mathbb{Z}\mathfrak{M}$.*

PROOF. (1): Given an exact sequence

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{4.1}$$

in ${}_R\mathfrak{M}$, we prove that the corresponding sequence

$$0 \to \operatorname{Hom}_R(M,A) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_R(M,B) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_R(M,C) \tag{4.2}$$

in ${}_{\mathbb{Z}}\mathfrak{M}$ is exact.

Step 1: Show that H_α is one-to-one. Assume $g \in \operatorname{Hom}_R(M,A)$ and $\alpha g = 0$. Since α is one-to-one, then $g = 0$.

Step 2: Show $\operatorname{im}\mathrm{H}_\alpha \subseteq \ker \mathrm{H}_\beta$. Suppose $g \in \operatorname{Hom}_R(M,A)$. Then $\mathrm{H}_\beta\,\mathrm{H}_\alpha(g) = \beta\alpha g = 0$ since (4.1) is exact.

Step 3: Show $\operatorname{im}\mathrm{H}_\alpha \supseteq \ker \mathrm{H}_\beta$. Suppose $h \in \operatorname{Hom}_R(M,B)$ and $\mathrm{H}_\beta(h) = \beta h = 0$. Then $\operatorname{im}(h) \subseteq \ker(\beta) = \operatorname{im}(\alpha)$. Since α is one-to-one, there is an isomorphism of R-modules $\alpha^{-1} : \operatorname{im}(\alpha) \to A$. So the composition $g = \alpha^{-1} \circ h$ is an R-module homomorphism $g : M \to A$ and $\mathrm{H}_\alpha(g) = \alpha g = h$.

(2) and (3): Are left to the reader. $\square$

A partial converse to Proposition 2.4.5 (3) is

LEMMA 2.4.6. *Let R be a ring. The sequence of R-modules*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

is exact, if for all R-modules M

$$\operatorname{Hom}_R(C,M) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_R(B,M) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_R(A,M)$$

is an exact sequence of $\mathbb{Z}$-modules.

PROOF. Step 1: $\operatorname{im}\alpha \subseteq \ker\beta$. Suppose there exists $a \in A$ such that $\beta\alpha a \neq 0$. We take M to be the nonzero module C. By assumption,

$$\operatorname{Hom}_R(C,C) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_R(B,C) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_R(A,C)$$

is an exact sequence of $\mathbb{Z}$-modules. Let 1 denote the identity element in $\operatorname{Hom}_R(C,C)$. By evaluating at the element a, we see that $\mathrm{H}_\alpha\,\mathrm{H}_\beta(1) \neq 0$, a contradiction.

Step 2: $\operatorname{im}\alpha \supseteq \ker\beta$. Suppose there exists $b \in B$ such that $\beta b = 0$ and $b \notin \operatorname{im}\alpha$. By Proposition 2.4.5 (3), the exact sequence

$$A \xrightarrow{\alpha} B \xrightarrow{\pi} B/\operatorname{im}\alpha \to 0$$

gives rise to the exact sequence

$$0 \to \operatorname{Hom}_R(B/\operatorname{im}\alpha, B/\operatorname{im}\alpha) \xrightarrow{\mathrm{H}_\pi} \operatorname{Hom}_R(B, B/\operatorname{im}\alpha) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_R(A, B/\operatorname{im}\alpha).$$

The identity map $1 \in \operatorname{Hom}_R(B/\operatorname{im}\alpha, B/\operatorname{im}\alpha)$ maps to the nonzero map $\pi = \mathrm{H}_\pi(1)$. Since $\mathrm{H}_\alpha(\pi) = \pi\alpha = 0$, we see that $\pi \in \ker \mathrm{H}_\alpha$. If we take M to be the nonzero module $B/\operatorname{im}\alpha$, then by assumption,

$$\operatorname{Hom}_R(C, B/\operatorname{im}\alpha) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_R(B, B/\operatorname{im}\alpha) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_R(A, B/\operatorname{im}\alpha)$$

is an exact sequence of $\mathbb{Z}$-modules. So $\pi \in \operatorname{im}\mathrm{H}_\beta$. There exists $g \in \operatorname{Hom}_R(C, B/\operatorname{im}\alpha)$ such that $g\beta = \pi$. On the one hand we have $g\beta(b) = 0$. On the other hand we have $\pi(b) \neq 0$, a contradiction. $\square$

4.2. Various Identities Involving the Hom Functor.

LEMMA 2.4.7. *Let R be a ring and M a left R-module. Then the map $f \mapsto f(1)$ defines an R-module isomorphism $\phi : \operatorname{Hom}_R(R,M) \to M$.*

PROOF. By Lemma 2.4.1 (1), we make $\operatorname{Hom}_R(R,M)$ into a left R-module by the action $(rf)(x) = f(xr)$. The equations

$$\phi(f_1+f_2) = (f_1+f_2)(1) = f_1(1)+f_2(1) = \phi(f_1)+\phi(f_2)$$

and

$$\phi(rf) = (rf)(1) = f(1r) = f(r1) = rf(1) = r\phi(f)$$

show that ϕ is an R-module homomorphism. Given any $x \in M$, define $\rho_x : R \to M$ to be "right multiplication by x". That is, $\rho_x(a) = ax$ for any $a \in R$. Since M is a left R-module, it follows that $\rho_x \in \operatorname{Hom}_R(R,M)$. This defines a function $\rho : M \to \operatorname{Hom}_R(R,M)$ which is the inverse to ϕ. $\square$

PROPOSITION 2.4.8. *Let R be a ring. Let M, N, $\{M_i \mid i \in I\}$ and $\{N_j \mid j \in J\}$ be R-modules. There are isomorphisms*

(1)
$$\operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \cong \prod_{i\in I}\operatorname{Hom}_R(M_i,N)$$

(2)
$$\operatorname{Hom}_R\Big(M, \prod_{j\in J} N_j\Big) \cong \prod_{j\in J}\operatorname{Hom}_R(M,N_j)$$

of $\mathbb{Z}$-modules.

PROOF. (1): Let $\iota_j : M_j \to \bigoplus_{i\in I} M_i$ be the injection into coordinate j. Define

$$\phi : \operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \to \prod_{i\in I}\operatorname{Hom}_R(M_i,N)$$

by $\phi(f) = g$ where $g(i) = f\iota_i$. Clearly ϕ is a $\mathbb{Z}$-module homomorphism. Given any $g \in \prod_{i\in I}\operatorname{Hom}_R(M_i,N)$, by Exercise 1.6.15 there exists a unique f such that the diagram

$$\begin{tikzcd} M_j \arrow[r, "\iota_j"] \arrow[dr, "g(j)"'] & \bigoplus_{i\in I} M_i \arrow[d, dashed, "\exists! f"] \\ & N \end{tikzcd}$$

commutes for every $j \in I$. Therefore $\phi(f) = g$. This shows that ϕ is a one-to-one correspondence, completing (1).

(2): Is left to the reader. (Hint: instead of the injection maps, use projections. Use Exercise 1.6.14.) $\square$

COROLLARY 2.4.9. *(Hom Distributes over a Finite Direct Sum) Let R be a ring and say $\{M_1,\dots,M_m\}$ and $\{N_1,\dots,N_n\}$ are R-modules. There is an isomorphism of $\mathbb{Z}$-modules*

$$\operatorname{Hom}_R\Big(\bigoplus_{i=1}^{m} M_i, \bigoplus_{j=1}^{n} N_j\Big) \xrightarrow{\phi} \bigoplus_{(i,j)=(1,1)}^{(m,n)} \operatorname{Hom}_R(M_i,N_j)$$

given by $\phi(f) = g$ where $g(k,\ell) \in \operatorname{Hom}_R(M_k,N_\ell)$ is defined by $g(k,\ell) = \pi_\ell \circ f \circ \iota_k$. Here we use the notation $\iota_k : M_k \to \bigoplus M_i$ is the injection into the kth summand and $\pi_\ell : \bigoplus N_j \to N_\ell$ is the projection onto the ℓth summand.

4.3. Hom Tensor Relations. In this section we prove several identities involving Hom groups and the tensor product. We usually refer to these as "Hom Tensor Relations".

THEOREM 2.4.10. *(Adjoint Isomorphism) Let R and S be rings.*

(1) If $A \in {}_R\mathfrak{M}$, $B \in {}_S\mathfrak{M}_R$ and $C \in {}_S\mathfrak{M}$, then there is an isomorphism of $\mathbb{Z}$-modules

$$\operatorname{Hom}_S(B \otimes_R A, C) \xrightarrow{\psi} \operatorname{Hom}_R(A, \operatorname{Hom}_S(B, C))$$

defined by $\psi(f)(a) = f(\cdot \otimes a)$.

(2) If $A \in \mathfrak{M}_R$, $B \in {}_R\mathfrak{M}_S$ and $C \in \mathfrak{M}_S$, then there is an isomorphism of $\mathbb{Z}$-modules

$$\operatorname{Hom}_S(A \otimes_R B, C) \xrightarrow{\phi} \operatorname{Hom}_R(A, \operatorname{Hom}_S(B, C))$$

defined by $\phi(f)(a) = f(a \otimes \cdot)$.

In both cases, the isomorphism is natural in both variables A and C. The "Tensor-Hom" pair, $(B \otimes_R (\cdot), \operatorname{Hom}_S(B, \cdot))$, is an adjoint pair.

PROOF. (1): Make $B \otimes_R A$ into a left S-module by $s(b \otimes a) = sb \otimes a$. Make $\operatorname{Hom}_S(B,C)$ into a left R-module by $(rf)(b) = f(br)$. Let $f \in \operatorname{Hom}_S(B \otimes_R A, C)$. For any $a \in A$, define $f(\cdot \otimes a) : B \to C$ by $b \mapsto f(b \otimes a)$. The reader should verify that $a \mapsto f(\cdot \otimes a)$ is an R-module homomorphism $A \to \operatorname{Hom}_S(B,C)$. This map is additive in f so ψ is well defined. Conversely, say $g \in \operatorname{Hom}_R(A, \operatorname{Hom}_S(B,C))$. Define $B \times A \to C$ by $(b,a) \mapsto g(a)(b)$. The reader should verify that this map is balanced and commutes with the left S-action on B and C. Hence there is induced $\phi(g) \in \operatorname{Hom}_S(B \otimes_R A, C)$ and the reader should verify that ϕ is the inverse to ψ. The reader should verify that ψ is natural in both variables.

(2): is left to the reader. □

LEMMA 2.4.11. *Let R and S be rings. Let $A \in {}_R\mathfrak{M}$ be finitely generated and projective. For any $B \in {}_R\mathfrak{M}_S$ and $C \in \mathfrak{M}_S$ there is a natural isomorphism*

$$\operatorname{Hom}_S(B,C) \otimes_R A \xrightarrow{\alpha} \operatorname{Hom}_S(\operatorname{Hom}_R(A,B), C)$$

of abelian groups. On generators, the map is defined by $\alpha(f \otimes a)(g) = f(g(a))$.

PROOF. Note that $\operatorname{Hom}_S(B,C)$ is a right R-module by the action $(fr)(b) = f(rb)$ and $\operatorname{Hom}_R(A,B)$ is a right S-module by the action $(gs)(a) = g(a)s$. Given any (f,a) in $\operatorname{Hom}_S(B,C) \times A$, define $\phi(f,a) \in \operatorname{Hom}_S(\operatorname{Hom}_R(A,B),C)$ by $\phi(f,a)(g) = f(g(a))$. The reader should verify that ϕ is a well defined balanced map. Therefore α is a well defined group homomorphism. Also note that if $\psi : A \to A'$ is an R-module homomorphism, then the diagram

$$\begin{tikzcd}
\operatorname{Hom}_S(B,C) \otimes_R A \arrow[r, "\alpha"] \arrow[d, "1\otimes\psi"'] & \operatorname{Hom}_S(\operatorname{Hom}_R(A,B),C) \arrow[d, "\mathrm{H}(\mathrm{H}(\psi))"] \\
\operatorname{Hom}_S(B,C) \otimes_R A' \arrow[r, "\alpha"] & \operatorname{Hom}_S(\operatorname{Hom}_R(A',B),C)
\end{tikzcd}$$

commutes. If $A = R$, then by Lemma 2.4.7 we see that α is an isomorphism. If $A = R^n$ is finitely generated and free, then use Lemma 2.4.9 to show α is an isomorphism. If A is a direct summand of a free R-module of finite rank, then combine the above results to complete the proof. □

THEOREM 2.4.12. *Let R be a commutative ring and let A and B be R-algebras. Let M be a finitely generated projective A-module and N a finitely generated projective B-module. Then for any A-module M' and any B-module N', the mapping*

$$\operatorname{Hom}_A(M,M') \otimes_R \operatorname{Hom}_B(N,N') \xrightarrow{\psi} \operatorname{Hom}_{A \otimes_R B}(M \otimes_R N, M' \otimes_R N')$$

induced by $\psi(f\otimes g)(x\otimes y) = f(x)\otimes g(y)$ is an R-module isomorphism. If $M = M'$ and $N = N'$, then ψ is also a homomorphism of rings.

PROOF. By Lemma 2.3.22, $M\otimes_R N$ and $M'\otimes_R N'$ are $A\otimes_R B$-modules. Define ρ : $\operatorname{Hom}_A(M,M')\times\operatorname{Hom}_B(N,N')\to\operatorname{Hom}_{A\otimes_R B}(M\otimes_R N, M'\otimes_R N')$ by $\rho(f,g)(x\otimes y) = f(x)\otimes g(y)$. The equations

$$\begin{aligned}\rho(f_1+f_2,g)(x\otimes y) &= (f_1+f_2)(x)\otimes g(y)\\ &= (f_1(x)+f_2(x))\otimes g(y)\\ &= f_1(x)\otimes g(y)+f_2(x)\otimes g(y)\\ &= \rho(f_1,g)(x\otimes y)+\rho(f_2,g)(x\otimes y)\\ &= \big(\rho(f_1,g)+\rho(f_2,g)\big)(x\otimes y)\end{aligned}$$

and

$$\begin{aligned}\rho(fr,g)(x\otimes y) &= (fr)(x)\otimes g(y)\\ &= f(x)r\otimes g(y)\\ &= f(x)\otimes rg(y)\\ &= f(x)\otimes (rg)(y)\\ &= \rho(f,rg)(x\otimes y)\end{aligned}$$

show that ρ is R-balanced. Therefore ψ is well defined. Now we show that ψ is an isomorphism. The method of proof is to reduce to the case where M and N are free modules.

Case 1: Show that ψ is an isomorphism if $M = A$ and $N = B$. By Lemma 2.4.7, both sides are naturally isomorphic to $M'\otimes_R N'$.

Case 2: Show that ψ is an isomorphism if M is free of finite rank m over A and N is free of finite rank n over B. By Lemma 2.4.9, Lemma 2.3.15 and Case 1, both sides are naturally isomorphic to $(M'\otimes_R N')^{(mn)}$.

Case 3: The general case. By Proposition 2.1.1 (1), we can write $M\oplus L\cong F$ where F is a free A module of finite rank and $N\oplus K\cong G$ where G is a free B module of finite. Using Lemma 2.4.9 and Lemma 2.3.15

$$\operatorname{Hom}_A(F,M')\otimes_R\operatorname{Hom}_B(G,N') = \big(\operatorname{Hom}_A(M,M')\otimes_R\operatorname{Hom}_B(N,N')\big)\oplus H \tag{4.3}$$

is an internal direct sum of the left hand side for some submodule H. Likewise,

$$\operatorname{Hom}_{A\otimes_R B}(F\otimes_R G, M'\otimes_R N') = \operatorname{Hom}_{A\otimes_R B}(M\otimes_R N, M'\otimes_R N')\oplus H' \tag{4.4}$$

is an internal direct sum of the right hand side, for some submodule H'. By Case 2, the natural map Ψ is an isomorphism between the left hand sides of (4.3) and (4.4). The restriction of Ψ gives the desired isomorphism ψ. □

COROLLARY 2.4.13. *Let R be a commutative ring and N a finitely generated projective R-module. Let A be an R-algebra. Then*

$$A\otimes_R\operatorname{Hom}_R(N,N')\xrightarrow{\psi}\operatorname{Hom}_A(A\otimes_R N, A\otimes_R N')$$

is an R-module isomorphism for any R-module N'.

PROOF. Set $B = R$, $M = M' = A$. □

COROLLARY 2.4.14. *If R is commutative and M and N are finitely generated projective R-modules, then*

$$\operatorname{Hom}_R(M,M)\otimes_R\operatorname{Hom}_R(N,N)\xrightarrow{\psi}\operatorname{Hom}_R(M\otimes_R N, M\otimes_R N)$$

is an R-algebra isomorphism.

PROOF. Take $A = B = R$, $M = M'$ and $N = N'$. $\square$

THEOREM 2.4.15. *Let A and B be rings. Let L be a finitely generated and projective left A-module. Let M be a left A right B bimodule. Let N be a left B-module. Then*

$$\operatorname{Hom}_A(L,M) \otimes_B N \xrightarrow{\psi} \operatorname{Hom}_A(L, M \otimes_B N)$$

is a $\mathbb{Z}$-module isomorphism, where $\psi(f \otimes y)(x) = f(x) \otimes y$ for all $y \in N$ and $x \in L$.

PROOF. By Lemma 2.4.1, $\operatorname{Hom}_A(L,M)$ is a right B-module by the action $(fb)(x) = f(x)b$. The reader should verify that ψ is balanced, hence well defined.

Case 1: Show that ψ is an isomorphism if $L = A$. By Lemma 2.4.7, both sides are naturally isomorphic to $M \otimes_B N$.

Case 2: Show that ψ is an isomorphism if L is free of rank n over A. By Lemma 2.4.9, Lemma 2.3.15 and Case 1, both sides are naturally isomorphic to $(M \otimes_R N)^{(n)}$.

Case 3: The general case. By Proposition 2.1.1 (1), we can write $L \oplus K \cong F$ where F is a free A module of rank n. Using Lemma 2.4.9 and Lemma 2.3.15

$$\operatorname{Hom}_A(F,M) \otimes_B N = \operatorname{Hom}_A(L,M) \otimes_R N \oplus H \tag{4.5}$$

is an internal direct sum of the left hand side for some submodule H. Likewise,

$$\operatorname{Hom}_A(F, M \otimes_B N) = \operatorname{Hom}_A(L, M \otimes_R N) \oplus H' \tag{4.6}$$

is an internal direct sum of the right hand side, for some submodule H'. By Case 2, the natural map Ψ is an isomorphism between the left hand sides of (4.5) and (4.6). The restriction of Ψ gives the desired isomorphism ψ. $\square$

4.4. Exercises.

EXERCISE 2.4.1. Let R be a ring and M a left R-module. The functor $\operatorname{Hom}_R(M,-)$ from the category of left R-modules to the category of $\mathbb{Z}$-modules is said to be *faithful* in case for every R-module homomorphism $\beta : A \to B$, if $\beta \neq 0$, then there exists $h \in \operatorname{Hom}_R(M,A)$ such that $\beta h \neq 0$. This exercise outlines a proof that M is an R-generator if and only if the functor $\operatorname{Hom}_R(M,-)$ is faithful. (This idea comes from [**10**, Proposition 1.1(a), p. 52].)

(1) For any left R-module A, set $H = \operatorname{Hom}_R(M,A)$. Let M^H denote the direct sum of copies of M over the index set H. Show that there is an R-module homomorphism
$$\alpha : M^H \to A$$
defined by $\alpha(f) = \sum_{h \in H} h(f(h))$.

(2) Show that if $\operatorname{Hom}_R(M,-)$ is faithful, then for any left R-module A, the map α defined in Part (1) is surjective. Conclude that M is an R-generator. (Hint: Let $\beta : A \to B$ be the cokernel of α. Show that the composition $M \xrightarrow{h} A \xrightarrow{\beta} B$ is the zero map for all $h \in H$.)

(3) Prove that if M is an R-generator, then $\operatorname{Hom}_R(M,-)$ is faithful. (Hint: Use Exercise 2.2.9.

EXERCISE 2.4.2. Let R be any ring and $\phi : A \to B$ a homomorphism of left R-modules. Prove that the following are equivalent.

(1) ϕ has a left inverse. That is, there exists an R-module homomorphism $\psi : B \to A$ such that $\psi\phi = 1_A$.

(2) For every left R-module M, the sequence

$$\operatorname{Hom}_R(B,M) \xrightarrow{\mathrm{H}_\phi} \operatorname{Hom}_R(A,M) \to 0$$

is exact.

(3) The sequence

$$\operatorname{Hom}_R(B,A) \xrightarrow{\mathrm{H}_\phi} \operatorname{Hom}_R(A,A) \to 0$$

is exact.

See Exercise 2.4.9 for the dual result on the splitting of $A \to B \to 0$.

EXERCISE 2.4.3. Let R be any ring and $\phi : A \to B$ a homomorphism of left R-modules. Prove that the following are equivalent.

(1) ϕ is an isomorphism.
(2) For every R-module M, $\mathrm{H}_\phi : \operatorname{Hom}_R(B,M) \to \operatorname{Hom}_R(A,M)$ is an isomorphism.

EXERCISE 2.4.4. Let A be an R-algebra that is finitely generated as an R-module. Suppose x and y are elements of A satisfying $xy = 1$. Prove that $yx = 1$. (Hints: Let $\rho_y : A \to A$ be defined by "right multiplication by y". That is, $\rho_y(a) = ay$. Show that ρ_y is onto. Conclude that ρ_y is one-to-one and use this to prove $yx = 1$.)

EXERCISE 2.4.5. Let R be a ring, M a left R-module, and N a right R-module. Prove the following:

(1) $M^* = \operatorname{Hom}_R(M,R)$ is a right R-module by the formula given in Lemma 2.4.1 (2).
(2) $N^* = \operatorname{Hom}_R(N,R)$ is a left R-module by the rule $(rf)(x) = rf(x)$.
(3) The left R-module $M^{**} = \operatorname{Hom}_R(M^*,R)$ is called the *double dual of M*. For $m \in M$, let $\varphi_m : M^* \to R$ be the "evaluation at m" map. That is, if $f \in M^*$, then $\varphi_m(f) = f(m)$. Prove that $\varphi_m \in M^{**}$, and that the assignment $m \mapsto \varphi_m$ defines a homomorphism of left R-modules $M \to M^{**}$.

EXERCISE 2.4.6. Let R be a ring. We say a left R-module M is *reflexive* in case the homomorphism $M \to M^{**}$ of Exercise 2.4.5 is an isomorphism. Prove the following:

(1) If $M_1, \dots, M_n$ are left R-modules, then the direct sum $\bigoplus_{i=1}^n M_i$ is reflexive if and only if each M_i is reflexive.
(2) A finitely generated free R-module is reflexive.
(3) A finitely generated projective R-module is reflexive.
(4) Let R be a commutative ring. If P is a finitely generated projective R-module and M is a reflexive R-module, then $P \otimes_R M$ is reflexive.

EXERCISE 2.4.7. Let A be a finite abelian group. Prove that $\operatorname{Hom}_{\mathbb{Z}}(A,\mathbb{Z}) = (0)$. Conclude that A is not a reflexive $\mathbb{Z}$-module.

EXERCISE 2.4.8. Let R be a PID and A a finitely generated torsion R-module. Prove that $\operatorname{Hom}_R(A,R) = (0)$. Conclude that A is not a reflexive R-module.

EXERCISE 2.4.9. Let R be any ring and $\phi : A \to B$ a homomorphism of left R-modules. Prove that the following are equivalent.

(1) ϕ has a right inverse. That is, there exists an R-module homomorphism $\psi : B \to A$ such that $\phi\psi = 1_B$.
(2) For every left R-module M, the sequence

$$\operatorname{Hom}_R(M,A) \xrightarrow{\mathrm{H}_\phi} \operatorname{Hom}_R(M,B) \to 0$$

is exact.

(3) The sequence

$$\operatorname{Hom}_R(B,A) \xrightarrow{\mathrm{H}_\phi} \operatorname{Hom}_R(B,B) \to 0$$

is exact.

See Exercise 2.4.2 for the dual result on the splitting of $0 \to A \to B$.

EXERCISE 2.4.10. Let R be a ring. Show that there exists an isomorphism of rings $\operatorname{Hom}_R(R,R) \cong R^o$, where R is viewed as a left R-module and R^o denotes the opposite ring.

5. Some Homological Algebra

5.1. The Five Lemma.

THEOREM 2.5.1. *(The Five Lemma) Let R be any ring and*

$$\begin{tikzcd}
A_1 \arrow[r, "f_1"] \arrow[d, "\alpha_1"] & A_2 \arrow[r, "f_2"] \arrow[d, "\alpha_2"] & A_3 \arrow[r, "f_3"] \arrow[d, "\alpha_3"] & A_4 \arrow[r, "f_4"] \arrow[d, "\alpha_4"] & A_5 \arrow[d, "\alpha_5"] \\
B_1 \arrow[r, "g_1"] & B_2 \arrow[r, "g_2"] & B_3 \arrow[r, "g_3"] & B_4 \arrow[r, "g_4"] & B_5
\end{tikzcd}$$

a commutative diagram of R-modules with exact rows.

(1) If α_2 and α_4 are onto and α_5 is one-to-one, then α_3 is onto.
(2) If α_2 and α_4 are one-to-one and α_1 is onto , then α_3 is one-to-one.

PROOF. (1) Let $b_3 \in B_3$. Since α_4 is onto there is $a_4 \in A_4$ such that $\alpha_4(a_4) = g_3(b_3)$. The second row is exact and α_5 is one-to-one and the diagram commutes, so $f_4(a_4) = 0$. The top row is exact, so there exists $a_3 \in A_3$ such that $f_3(a_3) = a_4$. The diagram commutes, so $g_3(b_3 - \alpha_3(a_3)) = 0$. The bottom row is exact, so there exists $b_2 \in B_2$ such that $g_2(b_2) = b_3 - \alpha_3(a_3)$. Since α_2 is onto, there is $a_2 \in A_2$ such that $\alpha_2(a_2) = b_2$. The diagram commutes, so $\alpha_3(f_2(a_2) + a_3) = b_3 - \alpha_3(a_3) + \alpha_3(a_3) = b_3$.

(2) Is left to the reader. $\square$

5.2. The Snake Lemma. We now prove what is perhaps the most fundamental tool in homological algebra, the so-called Snake Lemma.

THEOREM 2.5.2. *(The Snake Lemma) Let R be any ring and*

$$\begin{tikzcd}
 & A_1 \arrow[r, "f_1"] \arrow[d, "\alpha"'] & A_2 \arrow[r, "f_2"] \arrow[d, "\beta"'] & A_3 \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & B_1 \arrow[r, "g_1"] & B_2 \arrow[r, "g_2"] & B_3 &
\end{tikzcd}$$

a commutative diagram of R-modules with exact rows. Then there is an exact sequence

$$\ker\alpha \xrightarrow{f_1^*} \ker\beta \xrightarrow{f_2^*} \ker\gamma \xrightarrow{\partial} \operatorname{coker}\alpha \xrightarrow{g_1^*} \operatorname{coker}\beta \xrightarrow{g_2^*} \operatorname{coker}\gamma.$$

If f_1 is one-to-one, then f_1^* is one-to-one. If g_2 is onto, then g_2^* is onto.

PROOF. The proof is a series of small steps.

Step 1: There is an exact sequence

$$\ker\alpha \xrightarrow{f_1^*} \ker\beta \xrightarrow{f_2^*} \ker\gamma$$

where the maps are the restriction maps of f_1 and f_2 to submodules. If f_1 is one-to-one, then f_1^* is one-to-one. These are routine diagram chasing arguments.

Step 2: Construct the exact sequence

$$\operatorname{coker}\alpha \xrightarrow{g_1^*} \operatorname{coker}\beta \xrightarrow{g_2^*} \operatorname{coker}\gamma.$$

Since $g_1(\alpha(A_1) = \beta(f_1(A_1)$, it follows from Theorem 1.1.12 that g_1^* is well-defined. Likewise, since $g_2(\beta(A_2) = \gamma(f_2(A_2)$, it follows that g_2^* is well-defined. Since $g_2g_1 = 0$ it follows that $g_2^*g_1^* = 0$. Suppose $x \in B_2$ and $g_2(x) \in \operatorname{im}(\gamma)$. Then there is $y \in A_3$ and $\gamma(y) = g_2(x)$. Since f_2 is onto, there is $z \in A_2$ such that $f_2(z) = y$. We have $\gamma(f_2(z)) = g_2(\beta(z)) = g_2(x)$. Then $x - \beta(z) \in \ker(g_2) = \operatorname{im}(g_1)$. There exists $w \in B_1$ such that $g_1(w) = x - \beta(z)$. Then $x \equiv g_1(w) \pmod{\operatorname{im}\beta}$ which proves $\operatorname{im} g_1^* = \ker g_2^*$. If g_2 is onto, then it is easy to see that g_2^* is onto.

Step 3: Define the connecting homomorphism $\partial : \ker\gamma \to \operatorname{coker}\alpha$ by the formula

$$\partial(x) = g_1^{-1}\beta f_2^{-1}(x) \pmod{\operatorname{im}\alpha}.$$

Step 3.1: Check that ∂ is well defined. First notice that

$$g_2(\beta(f_2^{-1}(x))) = \gamma(f_2(f_2^{-1}(x))) = \gamma(x) = 0$$

since $x \in \ker\gamma$. Therefore, $\beta(f_2^{-1}(x)) \in \operatorname{im} g_1$. Now pick $y \in f_2^{-1}(x)$. Then

$$\begin{aligned} f_2^{-1}(x) &= y + \operatorname{im} f_1 \\ \beta(f_2^{-1}(x)) &= \beta(y) + \beta(\operatorname{im} f_1) \\ \beta(f_2^{-1}(x)) &= \beta(y) + g_1(\operatorname{im}\alpha) \\ g_1^{-1}(\beta(f_2^{-1}(x))) &= g_1^{-1}(\beta(y)) + \operatorname{im}\alpha. \end{aligned}$$

So $\partial(x) \equiv g_1^{-1}(\beta(y)) \pmod{\operatorname{im}\alpha}$, hence ∂ is well defined.

Step 3.2: Construct the complex

$$\ker\beta \xrightarrow{f_2^*} \ker\gamma \xrightarrow{\partial} \operatorname{coker}\alpha \xrightarrow{g_1^*} \operatorname{coker}\beta.$$

The proof follows directly from the definition of ∂.

Step 3.3: Prove exactness at $\ker\gamma$. Suppose $\partial(x) = 0$. That is, $g_1^{-1}(\beta(f_2^{-1}(x))) \in \operatorname{im}\alpha$. Pick $y \in A_2$ such that $f_2(y) = x$. Then for some $z \in A_1$,

$$\beta(y) = g_1\alpha(z) = \beta f_1(z).$$

Hence $y - f_1(z) \in \ker\beta$ and $f_2(y - f_1(z)) = f_2(y) - f_2f_1(z) = f_2(y) = x$. So $x \in \operatorname{im} f_2^*$.

Step 3.4: Prove exactness at $\operatorname{coker}\alpha$. Suppose $x \in B_1$ and $g_1(x) \in \operatorname{im}\beta$. Then $g_1(x) = \beta(y)$ for some $y \in A_2$. Then $\gamma(f_2(y)) = g_2(\beta(y)) = g_2(g_1(x)) = 0$. So $f_2(y) \in \ker\gamma$ and $\partial(f_2(y)) \equiv x \pmod{\operatorname{im}\alpha}$. □

5.3. The Product Lemma. The following lemma is another fundamental tool in homological algebra. It is called the Product Lemma in [**11**], [**38**], and [**13**]. Sometimes it is called the Kernel-Cokernel Sequence.

THEOREM 2.5.3. *If R is any ring and*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

a sequence of R-module homomorphisms, then there exists an exact sequence

$$0 \to \ker f \xrightarrow{\alpha_1} \ker(gf) \xrightarrow{\alpha_2} \ker g \xrightarrow{\alpha_3} \operatorname{coker} f \xrightarrow{\alpha_4} \operatorname{coker}(gf) \xrightarrow{\alpha_5} \operatorname{coker} g \to 0$$

where α_3 is the natural map $B \to \operatorname{coker} f$ restricted to $\ker g$.

PROOF. The proof consists of a sequence of five steps. Each homomorphism α_i is defined, and exactness proved at each term in the sequence.

Step 1: Exactness at $\ker f$. The map α_1 is defined to be the set inclusion homomorphism, which is well defined because $\ker f \subseteq \ker(gf)$. Being the set inclusion map, α_1 is one-to-one.

Step 2: Exactness at $\ker(gf)$. The map α_2 is f restricted to $\ker f$. If $x \in \ker f$, then $gf(x) = g(f(x)) = g(0) = 0$, which imples $\alpha_2\alpha_1 = 0$. Let $x \in \ker(gf)$ and assume $\alpha_2(x) = f(x) = 0$. Then $x \in \ker f$. This proves $\operatorname{im}\alpha_1 = \ker\alpha_2$.

Step 3: Exactness at $\ker g$. The map α_3 is the natural map $\bar{f} : B \to \operatorname{coker} f$ restricted to $\ker g$. If $x \in \ker(gf)$, then $\alpha_3\alpha_2(x) = \bar{f}f(x) = 0$. Hence $\alpha_3\alpha_2 = 0$. Let $y \in \ker g$ and assume $\bar{f}(y) = 0$. Then $y \in \operatorname{im} f$, so there exists $x \in A$ such that $y = f(x)$. Therefore $0 = g(y) = gf(x)$, which implies $x \in \ker(gf)$. Hence $y \in \operatorname{im}\alpha_2$. This proves $\operatorname{im}\alpha_2 = \ker\alpha_3$.

Step 4: Exactness at $\operatorname{coker} f$. To define the map α_4, consider the following commutative diagram.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "gf"'] & B \arrow[r, "\bar{f}"] \arrow[d, "g"] & \operatorname{coker} f \arrow[r] \arrow[dd, dashed, "\exists\alpha_4"] & 0 \\
 & C \arrow[dr, "\overline{gf}"'] & & \\
 & & \operatorname{coker}(gf) \arrow[dr] & \\
 & & & 0
\end{tikzcd}$$

A typical $y \in \operatorname{im} f = \ker\bar{f}$ can be written $y = f(x)$ for some $x \in A$. Then $g(y) \in \operatorname{im}(gf)$, and it follows that $\overline{gf}(g(y)) = 0$. By Theorem 1.1.12, α_4 is well defined. If $y \in \ker g$, then $\alpha_4\bar{f}(y) = \overline{gf}(g(y)) = 0$. Therefore $\alpha_3\alpha_4 = 0$. To see that $\operatorname{im}\alpha_3 = \ker\alpha_4$, let $y \in B$ and assume $\alpha_4\bar{f}(y) = 0$. Then $0 = \alpha_4\bar{f}(y) = \overline{gf}g(y)$. Thus $g(y) \in \operatorname{im} gf$, hence $g(y) = gf(x)$ for some $x \in A$. We have $y - f(x) \in \ker g$. Since $\bar{f}(y - f(x)) = \bar{f}(y)$ we see that $\bar{f}(y) \in \operatorname{im}\alpha_3$.

Step 5: Exactness at $\operatorname{coker}(gf)$. To define the map α_5, consider the following commutative diagram.

$$\begin{tikzcd}
A \arrow[r, "gf"] & C \arrow[r, "\overline{gf}"] \arrow[dr, "\bar{g}"'] & \operatorname{coker}(gf) \arrow[r] \arrow[d, dashed, "\exists\alpha_5"] & 0 \\
 & & \operatorname{coker} g &
\end{tikzcd}$$

Let $z \in \ker\overline{gf} = \operatorname{im}(gf)$. Then $z = gf(x)$ for some $x \in A$, hence $z \in \operatorname{im} g = \ker\bar{g}$. Therefore $\bar{g}(z) = \bar{g}gf(x) = 0$. By Theorem 1.1.12, α_5 is well defined. Let $y \in B$. Then $\alpha_4\bar{f}(y) = \overline{gf}g(y)$ and $\alpha_5\alpha_4\bar{f}(y) = \alpha_5\overline{gf}g(y) = \bar{g}g(y) = 0$. Therefore $\alpha_5\alpha_4 = 0$. Given $z \in C$, if $0 = \alpha_5\overline{gf}(z) = \bar{g}(z)$, then $z \in \operatorname{im} g$. So $z = g(y)$ for some $y \in B$. Thus $\overline{gf}(z) = \alpha_4\bar{f}(y)$ is in $\operatorname{im}\alpha_4$. This shows $\operatorname{im}\alpha_4 = \ker\alpha_5$. Given $z \in C$ we have $\bar{g}(z) = \alpha_5\overline{gf}(z)$ is in $\operatorname{im}\alpha_5$. This shows α_5 is onto. $\square$

5.4. Exercise.

EXERCISE 2.5.1. In the context of Theorem 2.5.3, let

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} \\ A_1 & \xrightarrow{f_1} & B_1 & \xrightarrow{g_1} & C_1 \end{array}$$

be a commutative diagram of R-modules. Show that there exist homomorphisms $\gamma_1,\dots,\gamma_6$ connecting the six term exact sequence for gf and the six term exact sequence for $g_1 f_1$ such that the diagram

$$\begin{array}{ccccccccccc} \ker f & \xrightarrow{\alpha_1} & \ker gf & \xrightarrow{\alpha_2} & \ker g & \xrightarrow{\alpha_3} & \operatorname{coker} f & \xrightarrow{\alpha_4} & \operatorname{coker} gf & \xrightarrow{\alpha_5} & \operatorname{coker} g \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_4} & & \downarrow{\scriptstyle \gamma_5} & & \downarrow{\scriptstyle \gamma_6} \\ \ker f_1 & \xrightarrow{\alpha_1} & \ker g_1 f_1 & \xrightarrow{\alpha_2} & \ker g_1 & \xrightarrow{\alpha_3} & \operatorname{coker} f_1 & \xrightarrow{\alpha_4} & \operatorname{coker} g_1 f_1 & \xrightarrow{\alpha_5} & \operatorname{coker} g_1 \end{array}$$

commutes.

EXERCISE 2.5.2. Let $Z = \operatorname{Max}(\mathbb{Z})$ denote the set of maximal ideals in $\mathbb{Z}$. Then each $\mathfrak{m} \in Z$ is a principal ideal $p\mathbb{Z}$ for some positive prime $p \in \mathbb{Z}$. In other words, Z is parametrized by the set of prime numbers. For each $\mathfrak{m} \in Z$, the residue ring $\mathbb{Z}/\mathfrak{m}$ is a finite field whose order is a prime number. Let $P = \prod_{\mathfrak{m}\in Z} \mathbb{Z}/\mathfrak{m}$ be the direct product of the finite prime fields. Then P is a ring and there is a natural homomorphism $\theta : \mathbb{Z} \to P$. As in Example 1.1.13, the left regular representation $\lambda : P \to \operatorname{Hom}_{\mathbb{Z}}(P,P)$ is defined by $\alpha \mapsto \ell_\alpha$. The following steps outline a proof that λ is an isomorphism of rings.

(1) Let $W \subseteq Z$ and assume W is infinite. Show that $\theta : \mathbb{Z} \to \prod_{\mathfrak{m}\in W} \mathbb{Z}/\mathfrak{m}$ is one-to-one. Hence the ring $\prod_{\mathfrak{m}\in W} \mathbb{Z}/\mathfrak{m}$ (and in particular P) is a faithful $\mathbb{Z}$-algebra and has characteristic zero.
(2) Let p be a prime number, $\pi_p : P \to \mathbb{Z}/p$ the projection map, and $\iota_p : \mathbb{Z}/p \to P$ the injection map. Show that

$$0 \to \mathbb{Z}/p \xrightarrow{\iota_p} P \xrightarrow{\ell_p} P \xrightarrow{\pi_p} \mathbb{Z}/p \to 0$$

is an exact sequence of $\mathbb{Z}$-modules.
(3) Let $h : P \to P$ be a $\mathbb{Z}$-module homomorphism. Show that h restricts to $\mathbb{Z}$-module homomorphisms $h : \ker \pi_p \to \ker \pi_p$ and $h : \operatorname{im} \iota_p \to \operatorname{im} \iota_p$.
(4) Let h be as in (3). Show that there exists $\alpha \in P$ such that h is equal to ℓ_α.
(5) Conclude that $\lambda : P \to \operatorname{Hom}_{\mathbb{Z}}(P,P)$ is an isomorphism of rings.

EXERCISE 2.5.3. In this exercise we continue to use the notation introduced in Exercise 2.5.2. Let $S = \bigoplus_{\mathfrak{m}\in Z} \mathbb{Z}/\mathfrak{m}$ be the direct sum of the finite prime fields. The following steps outline a proof that the endomorphism rings $\operatorname{Hom}_{\mathbb{Z}}(S,S)$ and $\operatorname{Hom}_{\mathbb{Z}}(P,P)$ are equal.

(1) Show that S is an ideal in the ring P.
(2) Show that if $h : P \to P$ is a $\mathbb{Z}$-module homomorphism, then h restricts to a $\mathbb{Z}$-module homomorphism $h : S \to S$.
(3) Show that every $h \in \operatorname{Hom}_{\mathbb{Z}}(S,S)$ is equal to ℓ_α for some $\alpha \in P$.
(4) Show that $\operatorname{Hom}_{\mathbb{Z}}(P,P) \cong \operatorname{Hom}_{\mathbb{Z}}(S,S)$ by the restriction map of (2).

For a continuation of this example, see Example 2.6.7.

EXERCISE 2.5.4. Let k be a field, A a k-algebra, and M a left A-module. Prove that if $\dim_k(M) = 1$, then A contains a two-sided ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \cong k$. (Hint: Consider the left regular representation $\lambda : A \to \operatorname{Hom}_k(M,M)$.)

EXERCISE 2.5.5. Let R be a ring, and M an R-module with submodules S and T.

(1) Prove that if ϕ is the subtraction mapping $(x,y) \mapsto x-y$, and ψ is the diagonal $z \mapsto (z,z)$, then there are exact sequences of R-modules

$$0 \to M \xrightarrow{\psi} M \oplus M \xrightarrow{\phi} M \to 0$$

and

$$0 \to S \cap T \xrightarrow{\psi} S \oplus T \xrightarrow{\phi} S+T \to 0.$$

(2) Combine the exact sequences of (1) and apply Theorem 2.5.2 to prove that

$$0 \to S \cap T \to M \xrightarrow{\psi} M/S \oplus M/T \xrightarrow{\phi} M/(S+T) \to 0$$

is an exact sequence of R-modules.

6. Injective Modules

Throughout this section, R will be an arbitrary ring. Unless otherwise specified, an R-module is a left R-module.

DEFINITION 2.6.1. Let R be a ring and E an R-module. Then E is *injective* if for any diagram of R-modules

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & A \arrow[u, "\phi"] \arrow[r, "\alpha"] & B \arrow[ul, dashed, "\exists\psi"'] \end{tikzcd}$$

with the bottom row exact, there exists an R-module homomorphism $\psi : B \to E$ such that $\psi\alpha = \phi$.

THEOREM 2.6.2. *An R-module E is injective if and only if the functor* $\operatorname{Hom}_R(\cdot, E)$ *is exact.*

PROOF. Is left to the reader. $\square$

PROPOSITION 2.6.3. *If $\{E_i \mid i \in I\}$ is a family of R-modules, then the direct product $\prod_{i \in I} E_i$ is injective if and only if each E_i is injective.*

PROOF. Assume each E_i is injective. For each $i \in I$, let $\pi_i : \prod_i E_i \to E_i$ be the projection onto coordinate i. In the following diagram , assume that we are given α and ϕ and that α is one-to-one.

$$\begin{tikzcd} & \prod_i E_i \arrow[r, "\pi_i"] & E_i \\ 0 \arrow[r] & A \arrow[u, "\phi"] \arrow[r, "\alpha"] & B \arrow[u, dashed, "\exists\psi_i"'] \end{tikzcd}$$

For each i there exists $\psi_i : B \to E_i$ such that $\psi_i\alpha = \pi_i\phi$. Define $\psi : B \to \prod_i E_i$ to be the product of the ψ_i. That is, for any $x \in B$, $\psi(x)(i) = \psi_i(x)$. The reader should verify that $\psi\alpha = \phi$. The converse is left to the reader. $\square$

LEMMA 2.6.4. *An R-module E is injective if and only if for every left ideal I of R, every homomorphism $I \to E$ can be extended to an R-module homomorphism $R \to E$.*

PROOF. Suppose E is injective and $\alpha : I \to R$ is the set inclusion map. Then any R-homomorphism $\phi : I \to E$ can be extended to $\psi : R \to E$.

Conversely suppose any homomorphism $I \to E$ can be extended to R if I is a left ideal of R. Let

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & A \arrow[u, "\phi"] \arrow[r, "\alpha"] & B \end{tikzcd}$$

be a diagram of R-modules with the bottom row exact. We need to find an R-module homomorphism $\psi : B \to E$ such that $\psi\alpha = \phi$. Consider the set $\mathscr{S}$ of all R-module homomorphisms $\sigma : C \to E$ such that $\alpha(A) \subseteq C \subseteq B$ and $\sigma\alpha = \phi$. Then $\mathscr{S}$ is nonempty because $\phi : A \to E$ is in $\mathscr{S}$. Put a partial ordering on $\mathscr{S}$ by saying $\sigma_1 : C_1 \to E$ is less than or equal to $\sigma_2 : C_2 \to E$ if $C_1 \subseteq C_2$ and σ_2 is an extension of σ_1. By Zorn's Lemma, Proposition 1.2.4, $\mathscr{S}$ contains a maximal member, $\psi : M \to E$. To finish the proof, it is enough to show $M = B$.

Suppose $M \neq B$ and let $b \in B - M$. The proof is by contradiction. Let $I = \{r \in R \mid rb \in M\}$. Then I is a left ideal of R. Define an R-module homomorphism $\sigma : I \to E$ by $\sigma(r) = \psi(rb)$. By hypothesis, there exists $\tau : R \to E$ such that τ is an extension of σ. To arrive at a contradiction, we show that there exists a homomorphism $\psi_1 : M + Rb \to E$ which is an extension of ψ. Define ψ_1 in the following way. If $m + rb \in M + Rb$, define $\psi_1(m + rb) = \psi(m) + r\tau(1)$. To see that ψ_1 is well defined, assume that in $M + Rb$ there is an element expressed in two ways: $m + rb = m_1 + r_1 b$. Subtracting gives $m - m_1 = (r_1 - r)b$ which is in M. Therefore $r_1 - r$ is in I. From $\psi(m - m_1) = \psi((r_1 - r)b) = \sigma(r_1 - r) = \tau(r_1 - r) = (r_1 - r)\tau(1)$, it follows that $\psi(m) - \psi(m_1) = r_1\tau(1) - r\tau(1)$. Therefore $\psi(m) + r\tau(1) = \psi(m_1) + r_1\tau(1)$ and we have shown that ψ_1 is well defined. This is a contradiction because ψ_1 is an extension of ψ and ψ is maximal. $\square$

DEFINITION 2.6.5. An abelian group A is said to be *divisible* in case for every nonzero integer n and every $a \in A$ there exists $x \in A$ such that $nx = a$.

EXAMPLE 2.6.6. Let n be a nonzero integer and $a \in \mathbb{Q}$. Set $x = a/n \in \mathbb{Q}$. Then $nx = a$, which shows the additive group $\mathbb{Q}$ is divisible.

EXAMPLE 2.6.7. Let $Z = \operatorname{Max}(\mathbb{Z})$ denote the set of maximal ideals in $\mathbb{Z}$. Then each $\mathfrak{m} \in Z$ is a principal ideal $p\mathbb{Z}$ for some positive prime $p \in \mathbb{Z}$. Let

$$P = \prod_{\mathfrak{m} \in Z} \mathbb{Z}/\mathfrak{m}$$

$$S = \bigoplus_{\mathfrak{m} \in Z} \mathbb{Z}/\mathfrak{m}$$

be the direct product and the direct sum of the prime fields $\mathbb{Z}/\mathfrak{m}$. By Exercises 2.5.2 and 2.5.3, S is an ideal in the ring P. In this example we show that the quotient P/S is a divisible abelian group. Let $\alpha \in \mathbb{Z}$ be a positive integer. Let $V(\alpha) = \{\mathfrak{m} \in Z \mid \alpha \in \mathfrak{m}\}$ and $U(\alpha) = \{\mathfrak{m} \in Z \mid \alpha \notin \mathfrak{m}\}$. Then $Z = V(\alpha) \cup U(\alpha)$ is a disjoint union. By The Fundamental Theorem of Arithmetic, $V(\alpha)$ is a finite set. If we set $P_0 = \prod_{\mathfrak{m} \in V(\alpha)} \mathbb{Z}/\mathfrak{m}$ and $P_1 = \prod_{\mathfrak{m} \in U(\alpha)} \mathbb{Z}/\mathfrak{m}$, then $P = P_0 \oplus P_1$ is the internal direct sum of the ideals. Let e_0 and e_1 be the idempotent generators of P_0 and P_1 respectively. The reader should verify that in the ring P_0, αe_0 is equal to 0 and in the ring P_1, αe_1 is invertible. Then $\alpha P = P_1$ and $P \otimes_{\mathbb{Z}} \mathbb{Z}/\alpha = P/\alpha P \cong P_0$. Notice that $P_0 \subseteq S$ and $S \otimes_{\mathbb{Z}} \mathbb{Z}/\alpha = S/\alpha S \cong P_0$. Consider the exact sequence

$$0 \to S \to P \to P/S \to 0.$$

By Lemma 2.3.18, $(P/S) \otimes_{\mathbb{Z}} \mathbb{Z}/\alpha = 0$. This proves P/S is a divisible abelian group. For a continuation of this example, see Exercise 3.1.20.

LEMMA 2.6.8. *An abelian group A is divisible if and only if A is an injective $\mathbb{Z}$-module.*

PROOF. Assume A is an injective $\mathbb{Z}$-module. Let $n \in \mathbb{Z} - (0)$ and $a \in A$. Let $\phi : \mathbb{Z}n \to A$ be the map induced by $n \mapsto a$. By Lemma 2.6.4, ϕ can be extended to a homomorphism $\psi : \mathbb{Z} \to E$. In this case, $a = \phi(n) = \psi(n) = n\psi(1)$ so a is divisible by n.

Conversely, assume A is divisible. A typical ideal of $\mathbb{Z}$ is $I = \mathbb{Z}n$. Suppose $\sigma : I \to A$ is a homomorphism. By Lemma 2.6.4, it is enough to construct an extension $\tau : \mathbb{Z} \to A$ of σ. If $n = 0$, then simply take $\tau = 0$. Otherwise solve $nx = \sigma(n)$ for x and define $\tau(1) = x$. $\square$

LEMMA 2.6.9. *If A is an abelian group, then A is isomorphic to a subgroup of a divisible abelian group.*

PROOF. The $\mathbb{Z}$-module A is the homomorphic image of a free $\mathbb{Z}$-module, $\sigma : \mathbb{Z}^I \to A$, for some index set I. Then $A \cong \mathbb{Z}^I/K$ where $K \subseteq \mathbb{Z}^I$ is the kernel of σ. Since $\mathbb{Z} \subseteq \mathbb{Q}$, there is a chain of subgroups $K \subseteq \mathbb{Z}^I \subseteq \mathbb{Q}^I$. This means $\mathbb{Z}^I/K$ is isomorphic to a subgroup of $\mathbb{Q}^I/K$. By Example 2.6.6, $\mathbb{Q}$ is divisible and by Exercises 2.6.1 and 2.6.2, $\mathbb{Q}^I/K$ is divisible. $\square$

LEMMA 2.6.10. *Let A be a divisible abelian group and R a ring. Then $\operatorname{Hom}_{\mathbb{Z}}(R,A)$ is an injective left R-module.*

PROOF. Since $R \in {}_{\mathbb{Z}}\mathfrak{M}_R$, we make $\operatorname{Hom}_{\mathbb{Z}}(R,A)$ into a left R-module by $(rf)(x) = f(xr)$. If M is any left R-module, then by the Adjoint Isomorphism (Theorem 2.4.10) there is a $\mathbb{Z}$-module isomorphism $\operatorname{Hom}_{\mathbb{Z}}(R \otimes_R M, A) \to \operatorname{Hom}_R(M, \operatorname{Hom}_{\mathbb{Z}}(R,A))$. To prove the lemma, we show that the contravariant functor $\operatorname{Hom}_R(\cdot, \operatorname{Hom}_{\mathbb{Z}}(R,A))$ is right exact and apply Theorem 2.6.2. Let $0 \to M \to N$ be an exact sequence of R-modules. The diagram

$$\begin{tikzcd}
\operatorname{Hom}_{\mathbb{Z}}(N,A) \arrow[r] \arrow[d, "\cong"'] & \operatorname{Hom}_{\mathbb{Z}}(M,A) \arrow[r] \arrow[d, "\cong"'] & 0 \\
\operatorname{Hom}_R(N, \operatorname{Hom}_{\mathbb{Z}}(R,A)) \arrow[r] & \operatorname{Hom}_R(M, \operatorname{Hom}_{\mathbb{Z}}(R,A)) \arrow[r] & 0
\end{tikzcd}$$

commutes. The top row is exact because by Lemma 2.6.8 and Theorem 2.6.2, the contravariant functor $\operatorname{Hom}_{\mathbb{Z}}(\cdot, A)$ is right exact. The vertical maps are the adjoint isomorphisms, so the bottom row is exact. $\square$

PROPOSITION 2.6.11. *Every left R-module M is isomorphic to a submodule of an injective R-module.*

PROOF. By Lemma 2.4.7 there is an R-module isomorphism $M \cong \operatorname{Hom}_R(R,M)$ given by $m \mapsto \rho_m$, where ρ_m is "right multiplication by m". Every R-homomorphism is a $\mathbb{Z}$-homomorphism, so $\operatorname{Hom}_R(R,M) \subseteq \operatorname{Hom}_{\mathbb{Z}}(R,M)$. By Lemma 2.6.9, there is a one-to-one homomorphism of abelian groups $\sigma : M \to D$ for some divisible abelian group D. By Proposition 2.4.5, there is an exact sequence

$$0 \to \operatorname{Hom}_{\mathbb{Z}}(R,M) \to \operatorname{Hom}_{\mathbb{Z}}(R,D).$$

Combining the above, the composite map

$$M \cong \operatorname{Hom}_R(R,M) \subseteq \operatorname{Hom}_{\mathbb{Z}}(R,M) \to \operatorname{Hom}_{\mathbb{Z}}(R,D)$$

is one-to-one and is given by $m \mapsto \sigma\rho_m$. This is an R-module homomorphism since the left R-module action on $\operatorname{Hom}_{\mathbb{Z}}(R,D)$ is given by $(rf)(x) = f(xr)$. By Lemma 2.6.10, we are done. $\square$

PROPOSITION 2.6.12. *Let R be a ring and E an R-module. The following are equivalent.*

(1) *E is injective.*
(2) *Every short exact sequence of R-modules $0 \to E \to A \to B \to 0$ is split exact.*
(3) *E is a direct summand of any R-module of which it is a submodule.*

PROOF. (1) implies (2): Let $\phi : E \to E$ be the identity map on E. By Definition 2.6.1 there exists $\psi : A \to E$ such that ψ is the desired splitting map.

(2) implies (3): Suppose that E is a submodule of M. The sequence $0 \to E \to M \to M/E \to 0$ is exact. By (2) there is a splitting map $\psi : M \to E$ such that for any $x \in E$ we have $\psi(x) = x$. If $K = \ker \psi$, then $M = E \oplus K$.

(3) implies (1): By Proposition 2.6.11, there is an injective R-module I such that E is a submodule of I. By (3), $I = E \oplus K$ for some submodule K. By Proposition 2.6.3, E is injective. □

6.1. Exercises.

EXERCISE 2.6.1. Prove that if A is a divisible abelian group and $B \subseteq A$ is a subgroup, then A/B is divisible.

EXERCISE 2.6.2. Prove that for any family of divisible abelian groups $\{A_i \mid i \in I\}$, the direct sum $\bigoplus_{i \in I} M_i$ is divisible.

EXERCISE 2.6.3. Let A be a divisible abelian group. Prove that if B is a subgroup of A which is a direct summand of A, then B is divisible.

EXERCISE 2.6.4. Let R be any ring and M an R-module. Suppose there is an infinite exact sequence

$$0 \to M \to E^0 \to E^1 \to E^2 \to \cdots \to E^n \to E^{n+1} \to \cdots \tag{6.1}$$

of R-modules. If each E^i is an injective R-module, then we say (6.1) is an *injective resolution* of M. Use Proposition 2.6.11 and induction to show that an injective resolution exists for any R and any M. We say that the category ${}_R\mathfrak{M}$ *has enough injectives*.

EXERCISE 2.6.5. Prove that if D is a division ring, then any nonzero vector space over D is an injective D-module.

EXERCISE 2.6.6. Let p be a prime number and A an abelian group. We say that A is *p-divisible*, if for every $n \geq 0$ and for every $x \in A$, there exists $y \in A$ such that $p^n y = x$. Prove that a p-divisible p-group is divisible.

6.2. Injective Modules and Flat Modules. Throughout this section, R is an arbitrary ring.

THEOREM 2.6.13. *Let R and S be arbitrary rings. Let $M \in {}_S\mathfrak{M}_R$ and assume M is a flat right R-module. Let I be a left injective S-module. Then $\operatorname{Hom}_S(M,I)$ is an injective left R-module.*

PROOF. Notice that $\operatorname{Hom}_S(M,I)$ is a left R-module by the action $(rf)(x) = f(xr)$. By the hypothesis on M and I, the functors $M \otimes_R (\cdot)$ and $\operatorname{Hom}_S(\cdot, I)$ are both exact. The composite functor $\operatorname{Hom}_S(M \otimes_R (\cdot), I)$ is also exact. By Theorem 2.4.10, this functor is naturally isomorphic to $\operatorname{Hom}_R(\cdot, \operatorname{Hom}_S(M,I))$, which is also exact. By Theorem 2.6.2, $\operatorname{Hom}_S(M,I)$ is injective. □

DEFINITION 2.6.14. A module C is a *cogenerator* for ${}_R\mathfrak{M}$ if for every module M and every nonzero $x \in M$ there exists $f \in \operatorname{Hom}_R(M,C)$ such that $f(x) \neq 0$.

LEMMA 2.6.15. *The $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is a cogenerator for ${}_{\mathbb{Z}}\mathfrak{M}$.*

PROOF. By Example 2.6.6 and Exercise 2.6.1, $\mathbb{Q}/\mathbb{Z}$ is a divisible abelian group. By Lemma 2.6.8, $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module. Let M be a $\mathbb{Z}$-module and let x be a nonzero element of M. To define a map $f : \mathbb{Z}m \to \mathbb{Q}/\mathbb{Z}$, it is enough to specify the image of the generator m. If d is the order of m, then

$$f(m) = \begin{cases} \frac{1}{2} + \mathbb{Z} & \text{if } d = \infty \\ \frac{1}{d} + \mathbb{Z} & \text{if } d < \infty \end{cases}$$

produces a well defined map f. Also $f(m) \neq 0$ and since $\mathbb{Q}/\mathbb{Z}$ is injective, f can be extended to $\operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. $\square$

DEFINITION 2.6.16. Let M be a right R-module. The R-module $\operatorname{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$ is called the *character module* of M. The character module of M is a left R-module by the action $rf(x) = f(xr)$ where $r \in R$, $f \in \operatorname{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$ and $x \in M$.

LEMMA 2.6.17. *The sequence of right R-modules*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is exact if and only if the sequence of character modules

$$0 \to \operatorname{Hom}_{\mathbb{Z}}(C,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_{\mathbb{Z}}(B,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_{\mathbb{Z}}(A,\mathbb{Q}/\mathbb{Z}) \to 0$$

is exact.

PROOF. Assume the original sequence is exact. By Theorem 2.6.2, the second sequence is exact. Conversely, it is enough to assume

$$\operatorname{Hom}_{\mathbb{Z}}(C,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_{\mathbb{Z}}(B,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_{\mathbb{Z}}(A,\mathbb{Q}/\mathbb{Z}) \tag{6.2}$$

is exact and prove that

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

is exact.

Step 1: Show that $\operatorname{im}\alpha \subseteq \ker\beta$. For contradiction's sake, assume $a \in A$ and $\beta\alpha(a) \neq 0$. By Lemma 2.6.15, there is $f \in \operatorname{Hom}_{\mathbb{Z}}(C,\mathbb{Q}/\mathbb{Z})$ such that $f\beta\alpha(a) \neq 0$. Therefore $\mathrm{H}_\alpha \mathrm{H}_\beta(f) \neq 0$ which is a contradiction.

Step 2: Show that $\operatorname{im}\alpha \supseteq \ker\beta$. For contradiction's sake, assume $b \in B$ and $\beta(b) = 0$ and $b \notin \operatorname{im}\alpha(a)$. Then $b + \operatorname{im}\alpha$ is a nonzero element of $B/\operatorname{im}\alpha$. The exact sequence

$$A \xrightarrow{\alpha} B \xrightarrow{\pi} B/\operatorname{im}\alpha$$

gives rise to the exact sequence

$$\operatorname{Hom}_{\mathbb{Z}}(B/\operatorname{im}\alpha,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\pi} \operatorname{Hom}_{\mathbb{Z}}(B,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_{\mathbb{Z}}(A,\mathbb{Q}/\mathbb{Z}).$$

By Lemma 2.6.15, there is $g \in \operatorname{Hom}_{\mathbb{Z}}(B/\operatorname{im}\alpha,\mathbb{Q}/\mathbb{Z})$ such that $g(b+\operatorname{im}\alpha) \neq 0$. Let $f = \mathrm{H}_\pi(g)$. Then $\mathrm{H}_\alpha(f) = 0$ and exactness of (6.2) implies $f = \mathrm{H}_\beta(h)$ for some $h \in \operatorname{Hom}_{\mathbb{Z}}(C,\mathbb{Q}/\mathbb{Z})$. On the one hand, $f(b) = g\pi(b) \neq 0$. On the other hand, $f(b) = h\beta(b) = h(0) = 0$. This is a contradiction. $\square$

THEOREM 2.6.18. *Let R be any ring and M a right R-module. Then M is flat if and only if the character module* $\operatorname{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$ *is an injective left R-module.*

PROOF. View M as a left $\mathbb{Z}$-right R-bimodule. Since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, if M is flat, apply Theorem 2.6.13 to see that $\operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is an injective left R-module.

Conversely assume $\operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is an injective left R-module. By Theorem 2.6.2, the functor $\operatorname{Hom}_R(\cdot, \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}))$ is exact. By Theorem 2.4.10, the isomorphic functor $\operatorname{Hom}_{\mathbb{Z}}(M \otimes_R (\cdot), \mathbb{Q}/\mathbb{Z})$ is also exact. Suppose $0 \to A \to B$ is an exact sequence of left R-modules. The sequence

$$\operatorname{Hom}_{\mathbb{Z}}(M \otimes_R B, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}_{\mathbb{Z}}(M \otimes_R A, \mathbb{Q}/\mathbb{Z}) \to 0$$

is an exact sequence of $\mathbb{Z}$-modules. By Lemma 2.6.17, $0 \to M \otimes_R A \to M \otimes_R B$ is an exact sequence of $\mathbb{Z}$-modules. This proves M is flat. $\square$

For another proof of Theorem 2.6.19, see Corollary 3.7.7. For a stronger version when R is a local ring, see Corollary 3.7.5.

THEOREM 2.6.19. *The R-module M is finitely generated projective over R if and only if M is flat and of finite presentation over R.*

PROOF. If M is finitely generated and projective, then M is flat by Exercise 2.3.6 and of finite presentation by Corollary 2.1.8.

Assume M is flat and of finite presentation over R. Then M is finitely generated, so by Proposition 2.4.5 it is enough to show that $\operatorname{Hom}_R(M, \cdot)$ is right exact. Let $A \to B \to 0$ be an exact sequence of R-modules. It is enough to show that $\operatorname{Hom}_R(M,A) \to \operatorname{Hom}_R(M,B) \to 0$ is exact. By Lemma 2.6.17, it is enough to show that

$$0 \to \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,B), \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,A), \mathbb{Q}/\mathbb{Z}) \tag{6.3}$$

is exact. Since M is of finite presentation, there exist free R-modules F_1 and F_0 of finite rank, and an exact sequence

$$F_1 \to F_0 \to M \to 0. \tag{6.4}$$

Suppose $B \in {}_R\mathfrak{M}_{\mathbb{Z}}$. Suppose $E \in \mathfrak{M}_{\mathbb{Z}}$ is injective. Consider the diagram

$$\begin{tikzcd}
\operatorname{Hom}_{\mathbb{Z}}(B,E) \otimes_R F_1 \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_{\mathbb{Z}}(B,E) \otimes_R F_0 \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_{\mathbb{Z}}(B,E) \otimes_R M \to 0 \arrow[d, "\alpha"] \\
\operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(F_1,B),E) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(F_0,B),E) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,B),E) \to 0
\end{tikzcd}$$

The top row is obtained by tensoring (6.4) with $\operatorname{Hom}_{\mathbb{Z}}(B,E)$, hence it is exact. The bottom row is exact because it comes from (6.4) by first applying the left exact contravariant functor $\operatorname{Hom}_R(\cdot, B), E)$ followed by the exact contravariant functor $\operatorname{Hom}_{\mathbb{Z}}(\cdot, E)$. The vertical maps come from the proof of Lemma 2.4.11, so the diagram commutes. The two left-most vertical maps are isomorphisms, by Lemma 2.4.11. The Five Lemma (Theorem 2.5.1) says that the third vertical map is an isomorphism. The isomorphism is natural in B which says we can apply this result to the exact sequence $A \to B \to 0$ and get a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(B, \mathbb{Q}/\mathbb{Z}) \otimes_R M \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \otimes_R M \arrow[d, "\alpha"] \\
0 \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,B), \mathbb{Q}/\mathbb{Z}) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,A), \mathbb{Q}/\mathbb{Z})
\end{tikzcd}$$

where the vertical arrows are isomorphisms. The top row is obtained from the exact sequence $A \to B \to 0$ by first applying the exact contravariant functor $\operatorname{Hom}_{\mathbb{Z}}(\cdot, \mathbb{Q}/\mathbb{Z})$ followed by the exact functor $(\cdot) \otimes_R M$. Therefore, the top row is exact, which implies the bottom row is exact. The bottom row is (6.3), so we are done. $\square$

7. Direct Limits and Inverse Limits

7.1. The Direct Limit.

DEFINITION 2.7.1. An index set I is called a *directed set* in case there is a reflexive, transitive binary relation, denoted $\leq$, on I such that for any two elements $i, j \in I$, there is an element $k \in I$ with $i \leq k$ and $j \leq k$. Let I be a directed set and $\mathfrak{C}$ a category. Usually $\mathfrak{C}$ will be a category of R-modules for some ring R. At other times, $\mathfrak{C}$ will be a category of R-algebras for some commutative ring R. Suppose that for each $i \in I$ there is an object $A_i \in \mathfrak{C}$ and for each pair $i, j \in I$ such that $i \leq j$ there is a $\mathfrak{C}$-morphism $\phi^i_j : A_i \to A_j$ such that the following are satisfied.

(1) For each $i \in I$, $\phi^i_i : A_i \to A_i$ is the identity on A_i, and
(2) for all $i, j, k \in I$ with $i \leq j \leq k$, the diagram

$$\begin{tikzcd} A_i \arrow[rr, "\phi^i_k"] \arrow[dr, "\phi^i_j"'] & & A_k \\ & A_j \arrow[ur, "\phi^j_k"'] & \end{tikzcd}$$

commutes.

Then the collection of objects and morphisms $\{A_i, \phi^i_j\}$ is called a *directed system* in $\mathfrak{C}$ with index set I.

DEFINITION 2.7.2. Let $\{A_i, \phi^i_j\}$ be a directed system in $\mathfrak{C}$ for a directed index set I. The *direct limit* of this system, denoted $\varinjlim A_i$, is an object in $\mathfrak{C}$ together with a set of morphisms $\alpha_i : A_i \to \varinjlim A_i$ indexed by I such that the following are satisfied.

(1) For all $i \leq j$, $\alpha_i = \alpha_j \phi^i_j$, and
(2) $\varinjlim A_i$ satisfies the universal mapping property. Namely, if X is an object in $\mathfrak{C}$ and $f_i : A_i \to X$ is a set of morphisms indexed by I such that for all $i \leq j$, $f_i = f_j \phi^i_j$, then there exists a unique morphism $\beta : \varinjlim A_i \to X$ making the diagram

$$\begin{tikzcd} \varinjlim A_i \arrow[rr, dashed, "\exists!\beta"] & & X \\ & A_i \arrow[ul, "\alpha_i"'] \arrow[ur, "f_i"] \arrow[d, "\phi^i_j"] & \\ & A_j \arrow[uul, "\alpha_j"] \arrow[uur, "f_j"'] & \end{tikzcd}$$

commute for all $i \leq j$ in I.

PROPOSITION 2.7.3. *Let R be a ring. If $\{A_i, \phi^i_j\}$ is a directed system of R-modules for a directed index set I, then the direct limit $\varinjlim A_i$ exists. The direct limit is unique up to isomorphism.*

PROOF. Let $U = \bigcup_i A_i$ be the disjoint union of the modules. Define a binary relation $\sim$ on U in the following way. For any $x \in A_i$ and $y \in A_j$, we say x and y are related and write $x \sim y$ in case there exists $k \in I$ such that $i \leq k$ and $j \leq k$ and $\phi^i_k(x) = \phi^j_k(y)$. Clearly

$\sim$ is reflexive and symmetric. Assume $x \in A_i$, $y \in A_j$ and $z \in A_k$ and there exists m and n such that $i \leq m$, $j \leq m$, $j \leq n$, $k \leq n$, and $\phi^i_m(x) = \phi^j_m(y)$ and $\phi^j_n(y) = \phi^k_n(z)$. Since I is directed, there exists p such that $m \leq p$ and $n \leq p$. It follows that $\phi^i_p(x) = \phi^j_p(y) = \phi^k_p(z)$, so $\sim$ is transitive. Denote the equivalence class of $x \in U$ by $[x]$ and let $L = U/\sim$ be the set of all equivalence classes. Turn L into an R-module in the following way. If $r \in R$ and $x \in U$, define $r[x] = [rx]$. If $x \in A_i$ and $y \in A_j$ and k is such that $i \leq k$ and $j \leq k$, then define $[x]+[y] = [\phi^i_k(x) + \phi^j_k(y)]$. For each $i \in I$, let $\alpha_i : A_i \to L$ be the assignment $x \mapsto [x]$. It is clear that α_i is R-linear. If $i \leq j$ and $x \in A_i$, then $x \sim \phi^i_j(x)$, which says $\alpha_i = \alpha_j \phi^i_j$.

To see that L satisfies the universal mapping property, let X be an R-module and $f_i : A_i \to X$ a set of morphisms indexed by I such that for all $i \leq j$, $f_i = f_j \phi^i_j$. Suppose $x \in A_i$ and $y \in A_j$ are related. Then there exists $k \in I$ such that $i \leq k$, $j \leq k$ and $\phi^i_k(x) = \phi^j_k(y)$. Then $f_i(x) = f_k(\phi^i_k(x)) = f_k(\phi^j_k(y)) = f_j(y)$, so the assignment $[x] \mapsto f_i(x)$ induces a well defined R-module homomorphism $\beta : L \to X$. The R-module L satisfies Definition 2.7.2, so $L = \varinjlim A_i$.

Mimic the uniqueness part of the proof of Theorem 2.3.3 to prove that the direct limit is unique. $\square$

COROLLARY 2.7.4. *Let R be a commutative ring. If $\{A_i, \phi^i_j\}$ is a directed system of R-algebras for a directed index set I, then the direct limit $\varinjlim A_i$ exists.*

PROOF. The proof is left to the reader. $\square$

LEMMA 2.7.5. *Let R be a ring and $\{A_i, \phi^i_j\}$ a directed system of R-modules for a directed index set I. Suppose for some $i \in I$ and $x \in A_i$ that $[x] = 0$ in the direct limit $\varinjlim A_i$. Then there exists $k \geq i$ such that $\phi^i_k(x) = 0$ in A_k.*

PROOF. This follows straight from the construction in Proposition 2.7.3. Namely, $x \sim 0$ if and only if there exists $k \geq i$ such that $\phi^i_k(x) = 0$ in A_k. $\square$

Let R be a ring and I a directed index set. Suppose $\{A_i, \phi^i_j\}$ and $\{B_i, \psi^i_j\}$ are two directed systems of R-modules. A *morphism* from $\{A_i, \phi^i_j\}$ to $\{B_i, \psi^i_j\}$ is a set of R-module homomorphisms $\alpha = \{\alpha_i : A_i \to B_j\}_{i \in I}$ indexed by I such that the diagram

$$\begin{tikzcd} A_i \arrow[r, "\alpha_i"] \arrow[d, "\phi^i_j"'] & B_i \arrow[d, "\psi^i_j"] \\ A_j \arrow[r, "\alpha_j"] & B_j \end{tikzcd}$$

commutes whenever $i \leq j$. Define $f_i : A_i \to \varinjlim B_i$ by composing α_i with the structure map $B_i \to \varinjlim B_i$. The universal mapping property guarantees a unique R-module homomorphism $\vec{\alpha} : \varinjlim A_i \to \varinjlim B_i$.

THEOREM 2.7.6. *Let R be a ring, I a directed index set, and*

$$\{A_i, \phi^i_j\} \xrightarrow{\alpha} \{B_i, \psi^i_j\} \xrightarrow{\beta} \{C_i, \rho^i_j\}$$

a sequence of morphisms of directed systems of R-modules such that

$$0 \to A_i \xrightarrow{\alpha_i} B_i \xrightarrow{\beta_i} C_i \to 0$$

is exact for every $i \in I$. Then

$$0 \to \varinjlim A_i \xrightarrow{\vec{\alpha}} \varinjlim B_i \xrightarrow{\vec{\beta}} \varinjlim C_i \to 0$$

is an exact sequence of R-modules.

PROOF. The proof is a series of four small steps. We incorporate the notation of Proposition 2.7.3.

Step 1: $\vec{\beta}$ is onto. Given $[x] \in \varinjlim C_i$, there exists $i \in I$ such that $x \in C_i$. Since $\beta_i : B_i \to C_i$ is onto, there exists $b \in B_i$ such that $x = \beta_i(b)$. Then $[x] = \vec{\beta}[b]$.

Step 2: $\operatorname{im}\vec{\alpha} \subseteq \ker\vec{\beta}$. Given $[x] \in \varinjlim A_i$ there exists $i \in I$ such that $x \in A_i$. Then $\vec{\beta}\vec{\alpha}[x] = [\beta_i\alpha_i(x)] = [0]$.

Step 3: $\ker\vec{\beta} \subseteq \operatorname{im}\vec{\alpha}$. Given $[x] \in \ker\vec{\beta}$ there exists $i \in I$ such that $x \in B_i$. By Lemma 2.7.5 there exists $j > i$ such that $\rho^i_j\beta_i(x) = 0$. Since β is a morphism, $\beta_j\psi^i_j(x) = 0$. Therefore $\psi^i_j(x) \in \ker\beta_j = \operatorname{im}\alpha_j$, so $[x] \in \operatorname{im}\alpha$.

Step 4: $\vec{\alpha}$ is one-to-one. Given $[x] \in \ker\vec{\alpha}$, there exists $i \in I$ such that $x \in A_i$ and $[\alpha_i(x)] = 0$. By Lemma 2.7.5 there exists $j > i$ such that $\psi^i_j\alpha_i(x) = 0$. Since α is a morphism, $\alpha_j\phi^i_j(x) = 0$. Since α_j is one-to-one, it follows that $\phi^i_j(x) = 0$, hence $[x] = 0$. □

COROLLARY 2.7.7. *In the context of Theorem 2.7.6,*

$$\varinjlim (A_i \oplus B_i) \cong \left(\varinjlim A_i\right) \oplus \left(\varinjlim B_i\right)$$

7.1.1. *Tensor Product of Direct Limits.* Let $\{R_i, \theta^i_j\}$ be a directed system of rings for a directed index set I. Each R_i can be viewed as a $\mathbb{Z}$-algebra, hence the direct limit $R = \varinjlim R_i$ exists, by Corollary 2.7.4. For the same index set I, let $\{M_i, \phi^i_j\}$ and $\{N_i, \psi^i_j\}$ be directed systems of $\mathbb{Z}$-modules such that each M_i is a right R_i-module and each N_i is a left R_i-module. For each $i \le j$, M_j and N_j are R_i-modules via $\theta^i_j : R_i \to R_j$. In this context, we also assume that the transition homomorphisms ϕ^i_j and ψ^i_j are R_i-linear:

$$\phi^i_j(ax) = \theta^i_j(a)\phi^i_j(x)$$
$$\psi^i_j(ax) = \theta^i_j(a)\phi^i_j(x)$$

for all $a \in R_i$, $x \in M_i$ and $y \in N_i$. By Exercise 2.3.17 there are $\mathbb{Z}$-module homomorphisms

$$\tau^i_j : M_i \otimes_{R_i} N_i \to M_j \otimes_{R_j} N_j$$

such that $\{M_i \otimes_{R_i} N_i, \tau^i_j\}$ is a directed system for I. Let $M = \varinjlim M_i$, $N = \varinjlim N_i$.

PROPOSITION 2.7.8. *In the above context,* $\varinjlim M_i \otimes_{R_i} N_i = M \otimes_R N$.

PROOF. By Exercise 2.3.17 there are $\mathbb{Z}$-module homomorphisms

$$\alpha_i : M_i \otimes_{R_i} N_i \to M \otimes_R N$$

such that $\alpha_i = \alpha_j\tau^i_j$. We show that $M \otimes_R N$ satisfies the universal mapping property of Definition 2.7.2. Suppose we are given $\mathbb{Z}$-module homomorphisms

$$f_i : M_i \otimes_{R_i} N_i \to X$$

such that $f_i = f_j\tau^i_j$. Suppose $(x,y) \in M \times N$. Then for some $i \in I$, (x,y) comes from $M_i \times N_i$. The reader should verify that $(x,y) \mapsto f_i(x \otimes y)$ defines an R-balanced map $M \times N \to X$. This induces $\beta : M \otimes_R N \to X$. By Theorem 2.3.3, β is unique and satisfies $\beta\alpha_i = f_i$. □

7.1.2. *Direct Limits and Adjoint Pairs.*

THEOREM 2.7.9. *Let $F : \mathfrak{A} \to \mathfrak{C}$ and $G : \mathfrak{C} \to \mathfrak{A}$ be covariant functors and assume (F,G) is an adjoint pair. Let $\{A_i, \phi^i_j\}$ be a directed system in $\mathfrak{A}$ for a directed index set I and assume the direct limit $\varinjlim A_i$ exists. Then $\{FA_i, F\phi^i_j\}$ is a directed system in $\mathfrak{C}$ for the directed index set I and $\varinjlim FA_i \cong F(\varinjlim A_i)$.*

PROOF. Because F is a functor, $\{FA_i, F\phi^i_j\}$ is a directed system in $\mathfrak{C}$ for I. The proof reduces to showing $F(\varinjlim A_i)$ satisfies the universal mapping property of Definition 2.7.2. Assume we are given a commutative diagram

$$\begin{tikzcd}
F(\varinjlim A_i) & & X \\
& FA_i \arrow[ul, "F\alpha_i"'] \arrow[ur, "f_i"] \arrow[d, "F\phi^i_j"] & \\
& FA_j \arrow[uul, "F\alpha_j"] \arrow[uur, "f_j"'] &
\end{tikzcd}$$

in $\mathfrak{C}$, where the left half comes from the definition of $\varinjlim A_i$. To finish the proof we must show that there is a unique $\beta : F(\varinjlim A_i) \to X$ which commutes with the rest of the diagram. Since (F,G) is an adjoint pair, there is a natural bijection

$$\psi : \operatorname{Hom}_{\mathfrak{C}}(FA, X) \to \operatorname{Hom}_{\mathfrak{A}}(A, GX)$$

for any $A \in \mathfrak{A}$. Applying ψ to the right half of the diagram, we get a commutative diagram

$$\begin{tikzcd}
\varinjlim A_i \arrow[rr, dashed, "\theta"] & & GX \\
& A_i \arrow[ul, "\alpha_i"'] \arrow[ur, "\psi f_i"] \arrow[d, "\phi^i_j"] & \\
& A_j \arrow[uul, "\alpha_j"] \arrow[uur, "\psi f_j"'] &
\end{tikzcd}$$

in $\mathfrak{A}$. By definition of $\varinjlim A_i$, the morphism θ exists and is unique. Let $\beta = \psi^{-1}(\theta)$. Then $\beta : F(\varinjlim A_i) \to X$. Because ψ (and ψ^{-1}) is natural in the A variable, β makes the first diagram commutative. Because ψ is a bijection, β is unique. $\square$

COROLLARY 2.7.10. *Let R be a ring and $\{A_i, \phi^i_j\}$ a directed system of left R-modules for a directed index set I. If M is a right R-module, then*

$$M \otimes_R \varinjlim A_i \cong \varinjlim (M \otimes_R A_i).$$

PROOF. This follows from Proposition 2.7.8. We give a second proof based on Theorem 2.7.9. View M as a left $\mathbb{Z}$ right R bimodule. By Theorem 2.4.10, Tensor-Hom, $(M \otimes_R (\cdot), \operatorname{Hom}_{\mathbb{Z}}(M, \cdot))$, is an adjoint pair. $\square$

7.2. The Inverse Limit.

DEFINITION 2.7.11. Let $\mathfrak{C}$ be a category. Usually $\mathfrak{C}$ will be a category of modules or a category of algebras over a commutative ring. At other times, $\mathfrak{C}$ will be a category of topological groups. Let I be an index set with a reflexive, transitive binary relation, denoted $\leq$. (Do not assume I is a directed set.) Suppose that for each $i \in I$ there is an object $A_i \in \mathfrak{C}$ and for each pair $i, j \in I$ such that $i \leq j$ there is a $\mathfrak{C}$-morphism $\phi_i^j : A_j \to A_i$ such that the following are satisfied.

(1) For each $i \in I$, $\phi_i^i : A_i \to A_i$ is the identity on A_i, and
(2) for all $i, j, k \in I$ with $i \leq j \leq k$, the diagram

$$\begin{tikzcd} A_k \arrow[rr, "\phi_i^k"] \arrow[dr, "\phi_j^k"'] & & A_i \\ & A_j \arrow[ur, "\phi_i^j"'] & \end{tikzcd}$$

commutes.

Then the collection of objects and morphisms $\{A_i, \phi_i^j\}$ is called an *inverse system* in $\mathfrak{C}$ with index set I.

DEFINITION 2.7.12. Let $\{A_i, \phi_i^j\}$ be an inverse system in $\mathfrak{C}$ for an index set I. The *inverse limit* of this system, denoted $\varprojlim A_i$, is an object in $\mathfrak{C}$ together with a set of morphisms $\alpha_i : \varprojlim A_i \to A_i$ indexed by I such that the following are satisfied.

(1) For all $i \leq j$, $\alpha_i = \phi_i^j \alpha_j$, and
(2) $\varprojlim A_i$ satisfies the universal mapping property. Namely, if X is an object in $\mathfrak{C}$ and $f_i : X \to A_i$ is a set of morphisms indexed by I such that for all $i \leq j$, $f_i = \phi_i^j f_j$, then there exists a unique morphism $\beta : X \to \varprojlim A_i$ making the diagram

$$\begin{tikzcd} \varprojlim A_i \arrow[dr, "\alpha_i"] \arrow[ddr, "\alpha_j"'] & & X \arrow[ll, dashed, "\beta"'] \arrow[dl, "f_i"'] \arrow[ddl, "f_j"] \\ & A_i & \\ & A_j \arrow[u, "\phi_i^j"'] & \end{tikzcd}$$

commute for all $i \leq j$ in I.

PROPOSITION 2.7.13. *Let R be a ring. If $\{A_i, \phi_i^j\}$ is an inverse system of R-modules for an index set I, then the inverse limit $\varprojlim A_i$ exists. The inverse limit is unique up to isomorphism.*

PROOF. Let L be the set of all $f \in \prod A_i$ such that $f(i) = \phi_i^j f(j)$ whenever $i \leq j$. The reader should verify that L is an R-submodule of $\prod A_i$. Let $\pi_i : \prod A_i \to A_i$ be the projection onto the i-th factor. Let α_i be the restriction of π_i to L. The reader should verify that $\alpha_i = \phi_i^j \alpha_j$.

To see that L satisfies the universal mapping property, let X be an R-module and $f_i : X \to A_i$ a set of morphisms indexed by I such that for all $i \leq j$, $f_i = \phi_i^j f_j$. Define an R-module homomorphism $\beta : X \to \prod A_i$ by the rule $\beta(x)(i) = f_i(x)$ for all $x \in X$. If $i \leq j$, then $\beta(x)(i) = f_i(x) = \phi_i^j f_j(x) = \phi_i^j \beta(x)(j)$, so the image of β is contained in L. The R-module L satisfies Definition 2.7.12, so $L = \varprojlim A_i$.

Mimic the uniqueness part of the proof of Theorem 2.3.3 to prove that the inverse limit is unique. □

COROLLARY 2.7.14. *Let R be a commutative ring. If $\{A_i, \phi_i^j\}$ is an inverse system of R-algebras for an index set I, then the inverse limit $\varprojlim A_i$ exists.*

PROOF. The proof is left to the reader. □

THEOREM 2.7.15. *Let $F : \mathfrak{A} \to \mathfrak{C}$ and $G : \mathfrak{C} \to \mathfrak{A}$ be covariant functors and assume (F, G) is an adjoint pair. Let $\{C_i, \psi_i^j\}$ be an inverse system in $\mathfrak{C}$ for an index set I and assume the inverse limit $\varprojlim C_i$ exists. Then $\{GC_i, G\psi_i^j\}$ is an inverse system in $\mathfrak{A}$ for the index set I and $\varprojlim GC_i \cong G(\varprojlim C_i)$.*

PROOF. The proof is left to the reader. (Hint: Follow the proof of Theorem 2.7.9. Start with the appropriate diagram in $\mathfrak{A}$. Use the adjoint isomorphism ψ to get the commutative diagram in $\mathfrak{C}$ which can be completed.) □

COROLLARY 2.7.16. *Let R be a ring and $\{A_i, \phi_i^j\}$ an inverse system of left R-modules for an index set I. If M is a left R-module, then*

$$\mathrm{Hom}_R(M, \varprojlim A_i) \cong \varprojlim \mathrm{Hom}_R(M, A_i).$$

PROOF. We view M as a left R right $\mathbb{Z}$ bimodule. By Theorem 2.4.10, Tensor-Hom, $(M \otimes_{\mathbb{Z}} (\cdot), \mathrm{Hom}_R(M, \cdot))$, is an adjoint pair. □

EXAMPLE 2.7.17. Let A be a ring. Suppose $f_1 : M_1 \to M_3$ and $f_2 : M_2 \to M_3$ are homomorphisms of left A-modules. Then the *pullback* (or *fiber product*) is defined to be $M = \{(x_1, x_2) \in M_1 \oplus M_2 \mid f_1(x_1) = f_2(x_2)\}$. Notice that M is the kernel of the A-module homomorphism $M_1 \oplus M_2 \to M_3$ defined by $(x_1, x_2) \mapsto f_1(x_1) - f_2(x_2)$, hence M is a left A-module. If h_1 and h_2 are induced by the coordinate projections, then

$$\begin{tikzcd} M \arrow[r, "h_2"] \arrow[d, "h_1"'] & M_2 \arrow[d, "f_2"] \\ M_1 \arrow[r, "f_1"] & M_3 \end{tikzcd} \tag{7.1}$$

is a commutative diagram of A-modules. An important feature of the pullback is that it can be interpreted as an inverse limit. For the index set, take $I = \{1, 2, 3\}$ with the ordering $1 < 3$, $2 < 3$. The reader should verify that if f_1, f_2 are the transition homomorphisms, then $\{M_1, M_2, M_3\}$ is an inverse system and the inverse limit $\varprojlim M_i$ is isomorphic to the pullback M of (7.1). In particular, the pullback M satisfies the universal mapping property. That is, if N is an R-module and there exist h_1' and h_2' such that $f_1 h_1' = f_2 h_2'$, then there exists a unique morphism $\beta : N \to M$ such that the diagram

$$\begin{tikzcd}
N \arrow[dr, dashed, "\exists\beta"'] \arrow[drr, bend left, "h'_2"] \arrow[ddr, bend right, "h'_1"'] & & \\
& M \arrow[r, "h_2"'] \arrow[d, "h_1"] & M_2 \arrow[d, "f_2"] \\
& M_1 \arrow[r, "f_1"'] & M_3
\end{tikzcd}$$

commutes. A commutative square of R-modules such as (7.1) is called a *cartesian square* (or *fiber product diagram*, or *pullback diagram*), if M is isomorphic to the pullback $\varprojlim M_i$. Let A_1, A_2, A_3 be rings. If $f_1 : A_1 \to A_3$ and $f_2 : A_2 \to A_3$ are homomorphisms, then the inverse limit $A = \varprojlim A_i$ with respect to the index set $I = \{1,2,3\}$ is a ring. As above, A can be identified with the pullback $A = \{(x_1,x_2) \in A_1 \oplus A_2 \mid f_1(x_1) = f_2(x_2)\}$.

7.3. Inverse Systems Indexed by Nonnegative Integers. For the index set $\mathbb{Z}_{\geq 0} = \{0,1,2,\dots\}$, the notation simplifies. Let R be any ring and $\{A_i, \phi_i^j\}$ an inverse system of R-modules for the index set $\{0,1,2,\dots\}$. Simply write ϕ_{i+1} for ϕ_i^{i+1}. Then for any $j > i$ we can multiply to get $\phi_i^j = \phi_{i+1}\phi_{i+2}\cdots\phi_j$. Using this notation, and Proposition 2.7.13, the inverse limit $\varprojlim A_i$ can be identified with the set of all sequences $(x_0,x_1,x_2,\dots)$ in $\prod_{n=0}^{\infty} A_n$ such that $x_n = \phi_{n+1}x_{n+1}$ for all $n \geq 0$. Define

$$d : \prod_{n=0}^{\infty} A_n \longrightarrow \prod_{n=0}^{\infty} A_n$$

by $d(x_0,x_1,x_2,\dots) = (x_0 - \phi_1 x_1,\ x_1 - \phi_2 x_2,\ x_2 - \phi_3 x_3,\ \dots,\ x_n - \phi_{n+1}x_{n+1},\ \dots)$.

LEMMA 2.7.18. *Let R be any ring and $\{A_i, \phi_{i+1}\}$ an inverse system of R-modules for the index set $\{0,1,2,\dots\}$. If $\phi_{n+1} : A_{n+1} \to A_n$ is onto for each $n \geq 0$, then there is an exact sequence*

$$0 \to \varprojlim A_n \to \prod_{n=0}^{\infty} A_n \xrightarrow{d} \prod_{n=0}^{\infty} A_n \to 0$$

where d is defined in the previous paragraph.

PROOF. It follows at once that $\ker d = \varprojlim A_n$. Let $(y_0,y_1,y_2,\dots) \in \prod A_n$. To show that d is surjective, it is enough to solve the equations

$$\begin{aligned}
x_0 - \phi_1 x_1 &= y_0 \\
x_1 - \phi_2 x_2 &= y_1 \\
&\vdots \\
x_n - \phi_{n+1}x_{n+1} &= y_n
\end{aligned}$$

for $(x_0,x_1,x_2,\dots)$. This is possible because each ϕ_{n+1} is surjective. Simply take $x_0 = 0$, $x_1 = (\phi_1)^{-1}(-y_0)$, and recursively, $x_{n+1} = (\phi_{n+1})^{-1}(x_n - y_n)$. $\square$

Let R be a ring and suppose $\{A_i, \phi_{i+1}\}$ and $\{B_i, \psi_{i+1}\}$ are two inverse systems of R-modules indexed by $I = \{0,1,2,3,\dots\}$. A *morphism* from $\{A_i, \phi_{i+1}\}$ to $\{B_i, \psi_{i+1}\}$ is a sequence of R-module homomorphisms $\alpha = \{\alpha_i : A_i \to B_j\}_{i\geq 0}$ such that the diagram

$$\begin{tikzcd} A_{i+1} \arrow[r, "\alpha_{i+1}"] \arrow[d, "\phi_{i+1}"'] & B_{i+1} \arrow[d, "\psi_{i+1}"] \\ A_i \arrow[r, "\alpha_i"] & B_i \end{tikzcd}$$

commutes whenever $i \geq 0$. Define $f_i : \varprojlim A_i \to B_i$ by composing the structure map $\varprojlim A_i \to A_i$ with α_i. The universal mapping property guarantees a unique R-module homomorphism $\overleftarrow{\alpha} : \varprojlim A_i \to \varprojlim B_i$.

PROPOSITION 2.7.19. *Let R be a ring, and*

$$\{A_i, \phi_{i+1}\} \xrightarrow{\alpha} \{B_i, \psi_{i+1}\} \xrightarrow{\beta} \{C_i, \rho_{i+1}\}$$

a sequence of morphisms of inverse systems of R-modules indexed by $\{0,1,2,3,\dots\}$ such that

(1) $0 \to A_i \xrightarrow{\alpha_i} B_i \xrightarrow{\beta_i} C_i \to 0$ *is exact for every $i \geq 0$, and*
(2) $\phi_{i+1} : A_{i+1} \to A_i$ *is onto for every $i \geq 0$.*

Then

$$0 \to \varprojlim A_i \xrightarrow{\overleftarrow{\alpha}} \varprojlim B_i \xrightarrow{\overleftarrow{\beta}} \varprojlim C_i \to 0$$

is an exact sequence of R-modules.

PROOF. The diagram

$$\begin{tikzcd} 0 \arrow[r] & \prod A_n \arrow[r, "\alpha"] \arrow[d, "d"] & \prod B_n \arrow[r, "\beta"] \arrow[d, "d"] & \prod C_n \arrow[r] \arrow[d, "d"] & 0 \\ 0 \arrow[r] & \prod A_n \arrow[r, "\alpha"] & \prod B_n \arrow[r, "\beta"] & \prod C_n \arrow[r] & 0 \end{tikzcd}$$

commutes and the rows are exact. By Lemma 2.7.18, the leftmost vertical map is onto. The rest of the proof follows from Theorem 2.5.2 and Lemma 2.7.18. □

7.3.1. *The I-adic completion of a module.*

DEFINITION 2.7.20. Let R be a commutative ring, I an ideal in R and M an R-module. Then for all integers $n \geq 1$, I^n denotes the ideal generated by all products of the form $x_1x_2\cdots x_n$ where each x_i is in I. The chain of ideals $R \supseteq I^1 \supseteq I^2 \supseteq I^3 \supseteq \dots$ gives rise to the chain of submodules $M \supseteq I^1M \supseteq I^2M \supseteq I^3M \supseteq \dots$. Then $I^{i+1}M \subseteq I^iM$ so there is a natural projection $\phi_{i+1} : M/I^{i+1}M \to M/I^iM$. The set of R-modules and homomorphisms $\{M/I^iM, \phi_{i+1}\}$ is an inverse system indexed by $\{1,2,3,4,\dots\}$. The inverse limit of this system $\hat{M} = \varprojlim M/I^iM$ is called the *I-adic completion* of M. For each i, let $\eta_i : M \to M/I^iM$ be the natural projection. Clearly $\eta_i = \phi_{i+1}\eta_{i+1}$ so by Definition 2.7.12, there is a unique $\beta : M \to \hat{M}$ such that the diagram

$$\begin{tikzcd}
\hat{M} \arrow[dr] \arrow[ddr] & & M \arrow[ll, "\beta"'] \arrow[dl, "\eta_i"] \arrow[ddl, "\eta_{i+1}"] \\
& M/I^iM & \\
& M/I^{i+1}M \arrow[u, "\phi_{i+1}"] &
\end{tikzcd}$$

commutes.

PROPOSITION 2.7.21. *Let I be an ideal in the commutative ring R. Let M be an R-module and $\hat{M}$ the I-adic completion of M. The natural map $\beta : M \to \hat{M}$ is one-to-one if and only if $\cap I^n M = 0$.*

PROOF. Let $x \in M$. Notice that

$$\ker(\beta) = \{x \in M \mid x \in I^n M \ (\forall n > 0)\} = \bigcap I^n M.$$

Therefore β is one-to-one if and only if $\cap I^n M = 0$. $\square$

PROPOSITION 2.7.22. *Let I be an ideal in the commutative ring R and $\hat{R}$ the I-adic completion of R. Let M be an R-module and $\hat{M}$ the I-adic completion of M. Then $\hat{M}$ is an $\hat{R}$-module.*

PROOF. By Corollary 2.7.14, $\hat{R}$ is a commutative ring. For each i, let $\alpha_i : \hat{R} \to R/I^i$ and $\beta_i : \hat{M} \to M/I^iM$ be the natural maps. Then

$$\alpha_i \otimes \beta_i : \hat{R} \otimes_{\mathbb{Z}} \hat{M} \to R/I^i \otimes_{\mathbb{Z}} M/I^iM$$

is a well defined R-module homomorphism. Since M/I^iM is a module over R/I^i, let

$$\mu_i : R/I^i \otimes_{\mathbb{Z}} M/I^iM \to M/I^iM$$

be the multiplication map defined by $x \otimes y \mapsto xy$. So the maps $f_i = \mu_i \circ (\alpha_i \otimes \beta_i)$ and the universal mapping property give a product map $\hat{R} \otimes \hat{M} \to \hat{M}$ which turns $\hat{M}$ into an $\hat{R}$-module. $\square$

7.4. Exercises.

EXERCISE 2.7.1. Let R be an arbitrary ring. Let I be an index set, $X = \{x_i\}_{i \in I}$ a set of indeterminates indexed by I. Let J be the set of all finite subsets of I, ordered by set inclusion. For each $\alpha \in J$, let $X_\alpha = \{x_j \mid j \in \alpha\}$. Show how to make the set of polynomial rings $\{R[X_\alpha]\}_{\alpha \in J}$ into a directed system of rings. Define $R[X] = \varinjlim R[X_\alpha]$ as the direct limit. Let $\sigma : R \to S$ be a homomorphism of commutative rings. Show that σ extends to a homomorphism on the polynomial rings $\bar{\sigma} : R[X] \to S[X]$. If $f : X \to S$ is a function, show that there is a unique homomorphism $\bar{\sigma} : R[X] \to S$ such that $\bar{\sigma}[x] = f(x)$ for every $x \in X$..

EXERCISE 2.7.2. Suppose $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$ is a chain of submodules of the R-module A. Show how to make $\{A_i\}$ into a directed system and prove that $\varinjlim A_i = \bigcup_i A_i$.

EXERCISE 2.7.3. Let A be an R-module. Let S be the set of all subsets of A which are finitely generated R-submodules of A. Let S be ordered by $\subseteq$. For $\alpha \in S$, let A_α denote the R-submodule of A whose underlying set is α. Show how to make $\{A_\alpha\}$ into a directed system and prove that $A = \varinjlim A_\alpha$.

EXERCISE 2.7.4. Let R be a commutative ring and A an R-algebra. Show that $A = \varinjlim A_\alpha$ where A_α runs over the set of all finitely generated R-subalgebras of A.

EXERCISE 2.7.5. Let R be a commutative ring, A an R-algebra and $f \in A$. Show that $A = \varinjlim A_\alpha$ where A_α runs over all finitely generated R-subalgebras of A such that $R[f] \subseteq A_\alpha \subseteq A$.

EXERCISE 2.7.6. Let R be a ring and $\{M_i \mid i \in I\}$ a family of R-modules where I is an indexing set. Let $S = \bigoplus M_i$ be the direct sum. Let J be the set of all finite subsets of I, ordered by set inclusion. For each $\alpha \in J$, let $S_\alpha = \bigoplus_{i\in\alpha} M_i$ be the direct sum over the finite index set α. Show how to make $\{S_\alpha\}$ into a directed system and prove that $\varinjlim S_\alpha \cong S$.

EXERCISE 2.7.7. Let A be a commutative ring and $R = A[x]$ the polynomial ring in one variable with coefficients in A. Let $I = Rx$ be the ideal in R generated by x. Show that the I-adic completion of R is isomorphic to the power series ring $A[[x]]$ in one variable over A. (Hint: Show that $A[[x]]$ satisfies properties (1) and (2) of Definition 2.7.12.)

EXERCISE 2.7.8. Let R be any ring and $\{A_i, \phi^i_j\}$ a directed system of flat R-modules for a directed index set I. Show that the direct limit $\varinjlim A_i$ is a flat R-module.

EXERCISE 2.7.9. Let $\{R_i, \theta^i_j\}$ be a directed system of rings for a directed index set I. Let $R = \varinjlim R_i$ be the direct limit. As in Proposition 2.7.8, let $\{M_i, \phi^i_j\}$ be a directed system of $\mathbb{Z}$-modules for the same index set I such that each M_i is a left R_i-module and the transition homomorphisms ϕ^i_j are R_i-module homomorphisms. If each M_i is a flat R_i-module, show that $M = \varinjlim M_i$ is a flat R-module. (Hint: $\{R \otimes_{R_i} M_i, 1 \otimes \phi^i_j\}$ is a directed system of flat R-modules.)

EXERCISE 2.7.10. Let R be any ring and A an R-module. Show that if every finitely generated submodule of A is flat, then A is flat.

EXERCISE 2.7.11. Let R be a ring and $\{M_i, \phi^i_j\}$ a directed system of R-modules for a directed index set I. Let $\Xi = \{(x,y) \in I \times I \mid x \le y\}$. Let $\iota_i : M_i \to \bigoplus_{k\in I} M_k$ be the injection map into coordinate i. Given $(i,j) \in \Xi$, define $\delta_{ij} : M_i \to \bigoplus_{k\in I} M_k$ by $\delta_{ij}(x) = \iota_j \phi^i_j(x) - \iota_i(x)$. By Exercise 1.6.15, there exists $\delta : \bigoplus_{(i,j)\in\Xi} M_i \to \bigoplus_{k\in I} M_k$. Define L to be the cokernel of δ. There is a natural projection $\eta : \bigoplus_{k\in I} M_k \to L$. Define $\alpha_i = \eta\iota_i : M_i \to L$.

(1) Prove that $\alpha_i = \alpha_j \phi^i_j$ for all $i \le j$.
(2) Prove that L satisfies the universal mapping property of Definition 2.7.2, hence $L \cong \varinjlim M_i$.
(3) Prove that there is an exact sequence of R-modules

$$\bigoplus_{(i,j)\in\Xi} M_i \xrightarrow{\delta} \bigoplus_{k\in I} M_k \to \varinjlim M_i \to 0$$

EXERCISE 2.7.12. Let R be a ring and $\{M_i, \phi^j_i\}$ an inverse system of R-modules for an index set I. Let $\Xi = \{(x,y) \in I \times I \mid x \le y\}$. Let $\pi_i : \prod_{k\in I} M_k \to M_i$ be the projection map onto coordinate i. Given $(i,j) \in \Xi$, define $d_{ij} : \prod_{k\in I} M_k \to M_i$ by $d_{ij}(x) = \phi^j_i \pi_j(x) - \pi_i(x)$.

By Exercise 1.6.14, there exists $d : \prod_{k\in I} M_k \to \prod_{(i,j)\in\Xi} M_i$. Use Proposition 2.7.13 to prove that there is an exact sequence of R-modules

$$0 \to \varprojlim M_i \to \prod_{k\in I} M_k \xrightarrow{d} \prod_{(i,j)\in\Xi} M_i$$

EXERCISE 2.7.13. Let R be a ring and $\{A_i, \phi^i_j\}$ a directed system of R-modules for a directed index set I. Show that if M is any R-module, then there is an isomorphism

$$\operatorname{Hom}_R(\varinjlim A_i, M) \cong \varprojlim \operatorname{Hom}_R(A_i, M)$$

of $\mathbb{Z}$-modules. (Hint: Start with the exact sequence of Exercise 2.7.11 (3). Apply the functor $\operatorname{Hom}_R(\cdot, M)$. Use Proposition 2.4.8 and Exercise 2.7.12.)

EXERCISE 2.7.14. Let I be any index set ordered by the relation $x \le y$ if and only if $x = y$. For any family of R-modules $\{M_i \mid i \in I\}$ indexed by I, prove the following.

(1) I is a directed index set and if 1_{M_i} is the identity map on M_i, then $\{M_i, 1_{M_i}\}$ is both a directed system of R-modules, and an inverse system of R-modules.
(2) The direct limit $\varinjlim M_i$ exists and is equal to the direct sum $\bigoplus_{i\in I} M_i$.
(3) The inverse limit $\varprojlim M_i$ exists and is equal to the product $\prod_{i\in I} M_i$.

EXERCISE 2.7.15. Let $\mathfrak{C}_1$, $\mathfrak{C}_2$ be categories of modules and $\mathfrak{F} : \mathfrak{C}_1 \to \mathfrak{C}_2$ a left exact functor which commutes with arbitrary products. That is, $\mathfrak{F}(\prod_{k\in I} M_k) = \prod_{k\in I} \mathfrak{F}(M_k)$, for any family of objects in $\mathfrak{C}_1$. Prove that $\mathfrak{F}$ commutes with inverse limits. That is, $\mathfrak{F}\left(\varprojlim M_k\right) = \varprojlim \mathfrak{F}(M_k)$ for any inverse system in $\mathfrak{C}_1$.

EXERCISE 2.7.16. Let R be a commutative ring and $\mathfrak{p} \in \operatorname{Spec} R$. Show how to make $\{R[\alpha^{-1}] \mid \alpha \in R - \mathfrak{p}\}$ into a directed system and prove that the local ring of R at $\mathfrak{p}$ is equal to the direct limit: $R_{\mathfrak{p}} = \varinjlim R_\alpha$.

EXERCISE 2.7.17. (Local to Global Property for Idempotents) Let R be a commutative ring and $\mathfrak{p} \in \operatorname{Spec} R$. Let A be an R-algebra and e an idempotent in $A_{\mathfrak{p}}$. Show that there exists $\alpha \in R - \mathfrak{p}$ and an idempotent e_0 in $A_\alpha = A \otimes_R R[\alpha^{-1}]$ such that e is equal to the image of e_0 under the natural map $A_\alpha \to A_{\mathfrak{p}}$.

EXERCISE 2.7.18. Let R be a ring and $\{A_i, \phi^i_j\}$ a directed system of R-modules for a directed index set I. Let P be a finitely generated projective R-module.

(1) Show that $\operatorname{Hom}_R(P, \varinjlim A_i) \cong \varinjlim \operatorname{Hom}_R(P, A_i)$. (Hint: As in Theorem 2.4.12, reduce to the case where P is free.)
(2) Show that $\operatorname{Hom}_R(P, \bigoplus_i A_i) \cong \bigoplus_i \operatorname{Hom}_R(P, A_i)$.

EXERCISE 2.7.19. Let R be a commutative ring and $\{A_i, \phi^i_j\}$ a directed system of R-algebras for a directed index set I. Show that an idempotent in $\varinjlim A_i$ comes from an idempotent in A_i, for some $i \in I$. In other words, if $e \in \varinjlim A_i$ and $e^2 = e$, then for some $i \in I$, there exists $e_i \in A_i$ such that $e_i^2 = e_i$ and if $\alpha_i : A_i \to \varinjlim A_i$ is the natural map, then $\alpha_i(e_i) = e$.

EXERCISE 2.7.20. Let R be a commutative ring. Let I and J be ideals in R and assume there exists $m > 0$ such that $I^m \subseteq J$. Prove that the natural homomorphisms $R/I^{mi} \to R/J^i$ induce a homomorphism of rings $\varprojlim R/I^k \to \varprojlim R/J^k$. See Exercise 7.1.5 for an application of this result.

EXERCISE 2.7.21. In the context of the pullback diagram (7.1), prove the following:

(1) $\ker h_1 \cong \ker f_2$ and $\ker h_2 \cong \ker f_1$.

(2) If f_2 is onto, then h_1 is onto. If f_1 is onto, then h_2 is onto.

EXERCISE 2.7.22. Let A be a ring and let I and J be two-sided ideals in A. Show that

$$\begin{tikzcd} \frac{A}{I\cap J} \arrow[r, "h_2"] \arrow[d, "h_1"'] & \frac{A}{J} \arrow[d, "f_2"] \\ \frac{A}{I} \arrow[r, "f_1"] & \frac{A}{I+J} \end{tikzcd}$$

is a cartesian square of rings, where all of the homomorphisms are the natural maps.

EXERCISE 2.7.23. Let B be a ring and I a two-sided ideal of B. Assume $A \subseteq B$ is a subring such that $I \subseteq A$. Show that

$$\begin{tikzcd} A \arrow[r] \arrow[d, "h_1"'] & B \arrow[d, "f_2"] \\ \frac{A}{I} \arrow[r, "f_1"] & \frac{B}{I} \end{tikzcd}$$

is a cartesian square of rings, where all of the homomorphisms are the natural maps.

8. The Morita Theorems

8.1. The Functors. We begin by establishing some notation that will be in effect throughout this section. For any ring R and any left R-module M, set

$$M^* = \operatorname{Hom}_R(M,R)$$

and

$$S = \operatorname{Hom}_R(M,M).$$

Since R is a left R right R bimodule, by Lemma 2.4.1 (2), M^* is a right R-module under the operation $(fr)(m) = f(m)r$. Since S is a ring of R-module endomorphisms of M, M is a left S-module by $sm = s(m)$. This follows from Example 1.1.14. Under this operation M is a left R left S bimodule. By Lemma 2.4.1 (3), we make M^* a right S-module by $(fs)(m) = f\big(s(m)\big)$, which is just composition of functions. The reader should verify that M^* is in fact a right R right S bimodule. It follows that we can form $M^* \otimes_R M$ and $M^* \otimes_S M$. By Lemma 2.3.10, $M^* \otimes_R M$ is a left S right S bimodule by virtue of M being a left R left S bimodule and M^* being a right R right S bimodule. Similarly $M^* \otimes_S M$ is a left R right R bimodule.

Define

$$M^* \otimes_R M \xrightarrow{\theta_R} S = \operatorname{Hom}_R(M,M)$$

by the rule $\theta_R(f \otimes m)(x) = f(x)m$. The reader should check that θ_R is both a left and a right S-module homomorphism. Define

$$M^* \otimes_S M \xrightarrow{\theta_S} R$$

by the rule $\theta_S(f \otimes m) = f(m)$. The reader should verify that θ_S is a right and left R-module homomorphism whose image is the trace ideal $\mathfrak{T}_R(M)$.

LEMMA 2.8.1. *In the above context,*

(1) *θ_R is onto if and only if M is finitely generated and projective. If θ_R is onto, it is one-to-one.*
(2) *θ_S is onto if and only if M is a generator. If θ_S is onto, it is one-to-one.*

PROOF. (1): Suppose θ_R is onto. Then there exist $f_i \in M^*$ and $m_i \in M$ such that the identity map $1 : M \to M$ is equal to $\theta_R(\sum_{i=1}^n f_i \otimes m_i)$. That is, for every $x \in M$, $x = \sum_{i=1}^n f_i(x)m_i$. Then $\{(f_i, m_i)\}$ is a finite dual basis for M. By the Dual Basis Lemma 2.1.10, we are done. Conversely, if a finite dual basis exists, then $1 : M \to M$ is in the image of θ_R. Since θ_R is an S-module homomorphism, θ_R is onto.

Now assume θ_R is onto. Then M has a dual basis $f_1, \dots, f_n \in M^*$, $m_1, \dots, m_n \in M$. Assume $\alpha = \sum_j h_j \otimes n_j \in M^* \otimes_R M$ and $\theta_R(\alpha) = 0$. That is, $\sum_j h_j(x)n_j = 0$ for every x in M. Then

$$
\begin{aligned}
\alpha &= \sum_j h_j \otimes n_j \\
&= \sum_j \big[h_j \otimes \big(\sum_i f_i(n_j)m_i\big)\big] \\
&= \sum_{i,j} h_j \otimes f_i(n_j)m_i \\
&= \sum_{i,j} \big(h_j \cdot f_i(n_j)\big) \otimes m_i \\
&= \sum_i \big[\big(\sum_j h_j \cdot f_i(n_j)\big) \otimes m_i\big] \\
&= \sum_i 0 \otimes m_i \\
&= 0,
\end{aligned}
$$

because for each i and for each $x \in M$,

$$
\begin{aligned}
\Big[\sum_j h_j \cdot f_i(n_j)\Big](x) &= \sum_j h_j(x) f_i(n_j) \\
&= \sum_j f_i\big(h_j(x)n_j\big) \\
&= f_i\big(\sum_j h_j(x)n_j\big) \\
&= f_i(0) \\
&= 0.
\end{aligned}
$$

(2): Because the image of θ_S equals $\mathfrak{T}_R(M)$, the trace ideal of M, it is clear that θ_S is onto if and only if M is an R-generator (Definition 2.1.12).

Suppose θ_S is onto. Assume $\sum_j h_j \otimes n_j \in \ker \theta_S$. That is, $\sum_j h_j(n_j) = 0$. Since θ_S is onto, there exist $f_1, \dots, f_n$ in M^*, $m_1, \dots, m_n$ in M with $\sum_i f_i(m_i) = 1 \in R$. Notice that for every i and every $x \in M$,

$$
\begin{aligned}
\sum_j h_j \cdot \theta_R(f_i \otimes n_j)(x) &= \sum_j h_j\big(f_i(x)n_j\big) \\
&= f_i(x) \sum_j h_j(n_j) \\
&= 0.
\end{aligned}
$$

Hence

$$\begin{aligned}
\sum_j h_j \otimes n_j &= \sum_j h_j \otimes \big(\sum_i f_i(m_i)\big) n_j \\
&= \sum_j h_j \otimes \big(\sum_i f_i(m_i) n_j\big) \\
&= \sum_j h_j \otimes \big(\sum_i \theta_R(f_i \otimes n_j)(m_i)\big) \\
&= \sum_{i,j} h_j \otimes \theta_R(f_i \otimes n_j)(m_i) \\
&= \sum_i \big(\sum_j h_j \cdot \theta_R(f_i \otimes n_j)\big) \otimes (m_i) \\
&= \sum_i 0 \otimes m_i \\
&= 0.
\end{aligned}$$

Therefore, θ_S is one-to-one. □

8.2. The Morita Theorems. Let R be any ring and M a left R-progenerator. Set $S = \operatorname{Hom}_R(M,M)$ and $M^* = \operatorname{Hom}_R(M,R)$. As in Section 2.8.1, M is a left R left S bimodule. A slight variation of Lemma 2.3.17 (2) shows that $(\cdot) \otimes_R M$ defines a covariant functor from $\mathfrak{M}_R$ to ${}_S\mathfrak{M}$. Likewise, M^* is a right R right S bimodule, hence $M^* \otimes_S (\cdot)$ defines a covariant functor from ${}_S\mathfrak{M}$ to $\mathfrak{M}_R$. The following is the crucial theorem.

THEOREM 2.8.2. *In the above context, the functors*

$$(\cdot) \otimes_R M : \mathfrak{M}_R \to {}_S\mathfrak{M}$$

and

$$M^* \otimes_S (\cdot) : {}_S\mathfrak{M} \to \mathfrak{M}_R$$

are inverse equivalences. We say that the categories $\mathfrak{M}_R$ and ${}_S\mathfrak{M}$ are Morita equivalent.

PROOF. Let L be any right R-module. Then, by the basic properties of the tensor product and Lemma 2.8.1 (2), we have

$$\begin{aligned}
M^* \otimes_S (L \otimes_R M) &\cong M^* \otimes_S (M \otimes_{R^o} L) \\
&\cong (M^* \otimes_S M) \otimes_{R^o} L \\
&\cong R \otimes_{R^o} L \\
&\cong L \otimes_R R \\
&\cong L
\end{aligned}$$

where the composite isomorphism is given by $f \otimes (l \otimes m) \mapsto l \cdot \theta_S(f \otimes m) = l \cdot f(m)$. This isomorphism allows one to verify that $(\,) \otimes_R M$ followed by $M^* \otimes_S (\,)$ is naturally equivalent to the identity functor on $\mathfrak{M}_R$. Likewise, for any left S-module N, the isomorphism of Lemma 2.8.1 (1) implies that

$$\begin{aligned}
(M^* \otimes_S N) \otimes_R M &\cong (N \otimes_{S^o} M^*) \otimes_R M \\
&\cong N \otimes_{S^o} (M^* \otimes_R M) \\
&\cong N \otimes_{S^o} S \\
&\cong S \otimes_S N \\
&\cong N
\end{aligned}$$

under the map $(f \otimes n) \otimes m \mapsto \theta_R(f \otimes m) \cdot n$. Again this gives us that $M^* \otimes_S (\,)$ followed by $(\,) \otimes_R M$ is naturally equivalent to the identity on ${}_S\mathfrak{M}$. $\square$

COROLLARY 2.8.3. *In the setting of Theorem 2.8.2, we have*

(1) $R \cong \operatorname{Hom}_S(M,M)$ *(as rings) where r in R maps to "left multiplication by r".*
(2) $M^* \cong \operatorname{Hom}_S(M,S)$ *(as right S-modules) where f in M^* maps to the homomorphism $\theta_R\big(f \otimes (\,)\big)$.*
(3) $M \cong \operatorname{Hom}_R(M^*,R) = M^{**}$ *(as left R-modules) where m in M maps to the element in M^{**} which is "evaluation at m".*
(4) $S^o \cong \operatorname{Hom}_R(M^*,M^*)$ *(as rings) where s in S^o maps to "right multiplication by s".*
(5) *M is an S-progenerator.*
(6) *M^* is an R-progenerator.*
(7) *M^* is an S-progenerator.*

PROOF. The fully faithful part of Proposition 1.4.6 applied to the functor $(\,) \otimes_R M$ says that for any two right R-modules A and B, the assignment

$$\operatorname{Hom}_R(A,B) \to \operatorname{Hom}_S(A \otimes_R M, B \otimes_R M) \tag{8.1}$$

is a one-to-one correspondence. Under this equivalence, the right R-module R corresponds to the left S-module $R \otimes_R M \cong M$ and the right R-module M^* corresponds to the left S-module $M^* \otimes_R M \cong S$. For (1), use (8.1) with $A = B = R$. For (2), use (8.1) with $A = R$ and $B = M^*$. In each case, the reader should verify that the composite isomorphisms are the correct maps.

The fully faithful part of Proposition 1.4.6 applied to the functor $M^* \otimes_S (\,) : {}_S\mathfrak{M} \to \mathfrak{M}_R$ says that for any two left S-modules C and D, the assignment

$$\operatorname{Hom}_S(C,D) \to \operatorname{Hom}_R(M^* \otimes_S C, M^* \otimes_S D) \tag{8.2}$$

is a one-to-one correspondence. By Lemma 2.4.7, M is isomorphic to $\operatorname{Hom}_S(S,M)$. By (8.2) with $C = S$ and $D = M$, we get $\operatorname{Hom}_S(S,M) \cong \operatorname{Hom}_R(M^*,R) = M^{**}$, which is (3). For (4), use (8.2) with $C = D = S$. Since $M^* \otimes_S S \cong M^*$, we get the isomorphism of rings $\operatorname{Hom}_S(S,S) \cong \operatorname{Hom}_R(M^*,M^*)$. By Exercise 2.4.10, $S^o \cong \operatorname{Hom}_S(S,S)$ as rings. In each case, the reader should verify that the composite isomorphisms are the correct maps.

(5): Because M is an R-progenerator, we have $\theta_S : M^* \otimes_S M \cong R$ and $\theta_R : M^* \otimes_R M \cong S$. By (1) and (2) above, this gives rise to isomorphisms

$$\theta_S : \operatorname{Hom}_S(M,S) \otimes_S M \cong \operatorname{Hom}_S(M,M)$$

and

$$\theta_R : \operatorname{Hom}_S(M,S) \otimes_{\operatorname{Hom}_S(M,M)} M \cong S.$$

By Lemma 2.8.1 with R and S interchanged, it follows that M is an S-progenerator.

(6): Again using $M^* \otimes_S M \cong R$ and $M^* \otimes_R M \cong S$ and this time substituting (3) and (4), we obtain

$$\begin{aligned} R &\cong M^* \otimes_S M \\ &\cong M^* \otimes_S \operatorname{Hom}_R(M^*,R) \\ &\cong \operatorname{Hom}_R(M^*,R) \otimes_{S^o} M^* \\ &\cong \operatorname{Hom}_R(M^*,R) \otimes_{\operatorname{Hom}_R(M^*,M^*)} M^* \end{aligned} \tag{8.3}$$

and

$$\begin{aligned}\operatorname{Hom}_{R^o}(M^*,R^o)\otimes_{R^o}M^* &\cong M^*\otimes_R \operatorname{Hom}_R(M^*,R)\\ &\cong M^*\otimes_R M\\ &\cong S \qquad (8.4)\\ &\cong \operatorname{Hom}_R(M^*,M^*)\\ &\cong \operatorname{Hom}_{R^o}(M^*,M^*)\end{aligned}$$

where the last isomorphism in the second string is set identity and M^* is considered as a left R^o-module since it is a right R-module. By Lemma 2.8.1 with M^* in place of M, we see that M^* is an R-generator by (8.3) and a finitely generated and projective left R^o-module by (8.4). This implies that M^* is a right R-progenerator.

(7): By (5), M is an S-progenerator. Apply (6) to the S-module M to get $\operatorname{Hom}_S(M,S)$ is an S-progenerator. By (2), $\operatorname{Hom}_S(M,S)\cong M^*$. □

COROLLARY 2.8.4. *Let R, M and S be as in Theorem 2.8.2. For any two-sided ideal* $\mathfrak{a}$ *of R,* $M^*\otimes_R(\mathfrak{a}\otimes_R M)$ *is naturally isomorphic to the two-sided ideal of S consisting of all elements of the form*

$$\sum_i \theta_R(f_i\otimes\alpha_i m_i)\ ,\ f_i\in M^*\ ,\ \alpha_i\in\mathfrak{a}\ ,\ m_i\in M.$$

For any two-sided ideal $\mathfrak{b}$ *of S,* $M^*\otimes_S(\mathfrak{b}\otimes_S M)$ *is naturally isomorphic to the two-sided ideal of R consisting of all elements of the form*

$$\sum_i \theta_S\big(f_i\otimes\beta_i(n_i)\big)=\sum_i f_i\big(\beta_i(n_i)\big)\ ,f_i\in M^*\ ,\beta_i\in\mathfrak{b}\ ,n_i\in M.$$

These correspondences are inverses of each other and establish a one-to-one, order preserving correspondence between the two-sided ideals of R and the two-sided ideals of S.

PROOF. Since M and M^* are both R-projective, they are flat. The exact sequence $0\to\mathfrak{a}\to R$ yields the exact sequence

$$0\to M^*\otimes_R(\mathfrak{a}\otimes_R M)\to M^*\otimes_R(R\otimes_R M)\cong M^*\otimes_R M\cong S\ .$$

We consider $M^*\otimes_R(\mathfrak{a}\otimes_R M)$ as a subset of $M^*\otimes_R(R\otimes_R M)$. By θ_R, $M^*\otimes_R(R\otimes_R M)$ is isomorphic to S. This maps this submodule $M^*\otimes_R(\mathfrak{a}\otimes_R M)$ onto the ideal of S made up of elements of the form $\sum_i\theta_R(f_i\otimes\alpha_i m_i)$.

Likewise, M and M^* are S-projective. The exact sequence $0\to\mathfrak{b}\to S$ yields the exact sequence

$$0\to M^*\otimes_S(\mathfrak{b}\otimes_S M)\to M^*\otimes_S M\cong R\ .$$

We view $M^*\otimes_S(\mathfrak{b}\otimes_S M)$ as the ideal of R made up of elements looking like $\sum_i f_i\big(\beta_i(n_i)\big)$. The reader should verify that the correspondences are inverses of each other. □

REMARK 2.8.5. In the setting of Theorem 2.8.2, the categories $\mathfrak{M}_R$ and ${}_S\mathfrak{M}$ are equivalent. Under this equivalence, the free R-module R corresponds to the left S-module M, which is not necessarily a free S-module. The free S-module S corresponds to the right R-module M^*, which is not necessarily a free R-module. In Corollary 2.8.6 below, we show that finitely generated R-modules correspond to finitely generated S-modules, projective R-modules correspond to projective S-modules, and R-generator modules correspond to S-generator modules.

COROLLARY 2.8.6. *In the setting of Theorem 2.8.2, let L be a right R-module and* $L\otimes_R M$ *its corresponding left S-module.*

(1) L is finitely generated over R if and only if $L \otimes_R M$ is finitely generated over S.
(2) L is R-projective if and only if $L \otimes_R M$ is S-projective.
(3) L is an R-generator if and only if $L \otimes_R M$ is an S-generator.

PROOF. Use Lemma 1.6.11 to write L as the homomorphic image of a free R-module

$$R^I \to L \to 0 \tag{8.5}$$

where I is an index set. Tensor (8.5) with $(\cdot) \otimes_R M$ to get the exact sequence

$$M^I \to L \otimes_R M \to 0 \tag{8.6}$$

of S-modules. By Corollary 2.8.3 (5), M is finitely generated and projective as an S-module. For each biconditional, we prove only one direction. Each converse follows by categorical equivalence.

(1): If L is finitely generated over R, we may assume I is a finite set. In (8.6), $M^I = \bigoplus_{i \in I} M$ is a finite sum of finitely generated modules and is finitely generated. So $L \otimes_R M$ is finitely generated.

(2): If L is projective, by Proposition 2.1.1, (8.5) splits. It follows that (8.6) also splits. Use Exercise 2.2.6 to show that the S-modules M^I and $L \otimes_R M$ are projective.

(3): Let L be an R-generator. Let $\delta : C \to D$ be a nonzero homomorphism of left S-modules. By Exercise 2.4.1 (3), to show that $L \otimes_R M$ is an S-generator it suffices to show that there exists an S-module homomorphism $f : L \otimes_R M \to C$ such that $\delta \circ f$ is nonzero. By Proposition 1.4.6, $1 \otimes \delta : M^* \otimes_S C \to M^* \otimes_S D$ is a nonzero homomorphism of right R-modules. Since L is an R-generator, by Exercise 2.4.1 (4), there exists an R-module homomorphism $\alpha : L \to M^* \otimes_S C$ such that $(1 \otimes \delta) \circ \alpha$ is nonzero. Again by Proposition 1.4.6, $\delta \circ (\alpha \otimes 1)$ is nonzero. □

EXAMPLE 2.8.7. Let R be a ring and $M_n(R)$ the ring of n-by-n matrices over R. It is an exercise using multiplication by elementary matrices to show that if I is an ideal in $M_n(R)$, then $I = M_n(J)$ for some ideal J in R (see [**19**, Exercise 3.2.34]). The reader should verify that this is a special case of Corollary 2.8.4. (Hint: Ideals in $M_n(R)$ correspond to ideals in $M_n(R)^o \cong M_n(R^o) \cong \mathrm{Hom}_R(F,F)$, where F is a free left R-module with rank n.)

EXAMPLE 2.8.8. An important special case of Example 2.8.7 is when $R = D$ is a division ring. Then D has no proper two-sided ideal. A left D-progenerator is a finitely generated D-vector space, say V. By Corollary 2.8.4, the endomorphism ring $\mathrm{Hom}_D(V,V)$ has no proper two-sided ideal. In the Wedderburn-Artin Theorem (Theorem 4.4.5) below, we prove the converse of this fact. That is, we show that if R is an artinian ring with no proper two-sided ideal, then R is isomorphic to a ring of the form $\mathrm{Hom}_D(V,V)$ for some division ring D.

8.3. Exercises.

EXERCISE 2.8.1. Let R be any ring and let M be a left R-progenerator. Set $S = \mathrm{Hom}_R(M,M)$. Show that

$$(\;) \otimes_R M : \mathfrak{M}_R \to {}_S\mathfrak{M}$$

and

$$\mathrm{Hom}_S(M,\;) : {}_S\mathfrak{M} \to \mathfrak{M}_R$$

are inverse equivalences, establishing $\mathfrak{M}_R \sim {}_S\mathfrak{M}$. (Hint: Use Corollary 2.8.3 (2) and Theorem 2.4.15.)

EXERCISE 2.8.2. Let R be any ring. A left R-module M is said to be *faithfully flat* if M is flat and M has the property that $N \otimes_R M = 0$ implies $N = 0$. Show that a left R-progenerator is faithfully flat.

CHAPTER 3

Modules over Commutative Rings

This chapter is a study of the theory of modules over commutative rings. In Chapter 2, modules were studied over general rings. So in this sense, the present chapter marks for us the beginning of Commutative Algebra. Like the material in Chapter 2, the material in this chapter is fundamental and will be applied in all of the following chapters.

The localization of a commutative ring R at a multiplicative subset W is a ring, denoted $W^{-1}R$, together with a natural homomorphism $R \to W^{-1}R$. This construction generalizes the familiar construction of the ring of quotients of an integral domain. As a set, $W^{-1}R$ is the set of equivalence classes of fractions $\{r/w \mid r \in R, w \in W\}$, modulo an appropriate equivalence relation. The localization of an R-module M at W is defined in a similar way. The "localization at W" functor from the category of R-modules to the category of $W^{-1}R$-modules, which is defined by $M \mapsto W^{-1}M$, is exact. Localization plays a central role throughout this chapter. The terminology for localization comes from the fact that in the set of all prime ideals of R, the prime ideals of $W^{-1}R$ make up a subset (see Exercise 3.3.9).

Section 3.1.1 contains some fundamental lemmas on homological algebra. These "Local to Global" lemmas are motivated by the question: "If a homomorphism of R-modules $\varphi : M \to N$ becomes an isomorphism upon localization at W, is φ an isomorphism?"

The fundamental theorems on the decomposition of a ring into an internal direct sum of ideals are Theorem 1.1.8 and Proposition 1.1.9. In Lemma 3.2.4, necessary and sufficient conditions are derived such that a left ideal I in a ring R is a module direct summand of R. This is one of the few results in this chapter that does not require the ring R to be commutative.

The set of all prime ideals in a commutative ring R is called the prime spectrum of R and is denoted $\operatorname{Spec} R$. We define a topology on $\operatorname{Spec} R$, the Zariski topology, and show that the assignment $R \mapsto \operatorname{Spec} R$ is a contravariant functor from the category of commutative rings to the category of topological spaces. If $\theta : R \to S$ is a homomorphism of rings, then $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is the corresponding continuous function. If W is a multiplicative subset of R, then $\operatorname{Spec} W^{-1}R \to \operatorname{Spec} R$ is one-to-one. As mentioned above, the term "localization" refers to localization to a smaller subset of $\operatorname{Spec} R$.

A local ring is a commutative ring R that has exactly one maximal ideal. If R is a commutative ring and P is a prime ideal of R, then the set $R - P$ is a multiplicative set. The localization of R at $R - P$ is denoted R_P and is a local ring with maximal ideal PR_P. In Section 3.4 we show that if M is a finitely generated projective R-module, then M_P is a free R_P-module of finite rank. Moreover, there exists an element $\alpha \in R - P$ such that M_α is a free R_α-module of finite rank. If $U(\alpha)$ denotes the image of the natural map $\operatorname{Spec} R_\alpha \to \operatorname{Spec} R$, then $U(\alpha)$ is an open subset in the Zariski topology. We show that there is a finite set $\{\alpha_1, \dots, \alpha_n\}$ such that $\{U(\alpha_1), \dots, U(\alpha_n)\}$ is an open cover of $\operatorname{Spec} R$ and M_{α_i} is free of finite rank over R_{α_i}. We say that a finitely generated projective module is locally free of finite rank. In Section 3.6 we prove the converse.

If M is a module over commutative ring R, then M is flat if the functor $M \otimes_R (\cdot)$ is both left and right exact. If M is flat and if $M \otimes_R N = 0$ implies $N = 0$, then M is called faithfully flat. As an R-module, $W^{-1}R$, the localization of R at a multiplicative set W, is generally flat but not faithfully flat. We study faithfully flat modules and algebras over commutative rings in Section 3.5 and flat modules and algebras in Section 3.7. If S is an R-algebra, we derive a number of very important necessary conditions and sufficient conditions in order for S to be a faithfully flat R-module.

1. Localization of Modules and Rings

In this section we define the localization of a module over a commutative ring. This definition is a generalization of the construction of the quotient field of an integral domain. Let R be a commutative ring and W a subset of R that satisfies

(1) $1 \in W$, and
(2) if x and y are in W, then $xy \in W$.

In this case, we say that W is a *multiplicative subset of* R.

EXAMPLE 3.1.1. Here are some typical examples of multiplicative sets.

(1) If P is a prime ideal in R, then Proposition 1.5.4 says that $R - P$ is a multiplicative subset of R.
(2) If R is an integral domain, then $W = R - (0)$ is a multiplicative subset of R.
(3) If $f \in R$, then $\{1, f, f^2, f^3, \dots\}$ is a multiplicative subset of R.
(4) The set of all $x \in R$ such that x is not a zero divisor is a multiplicative subset of R.

Suppose W is a multiplicative subset of R. Define a relation on $R \times W$ by $(r, v) \sim (s, w)$ if and only if there exists $q \in W$ such that $q(rw - sv) = 0$. Clearly $\sim$ is reflexive and symmetric. Let us show that it is transitive. Suppose $(r, u) \sim (s, v)$ and $(s, v) \sim (t, w)$. There exist $e, f \in W$ such that $e(rv - su) = 0$ and $f(sw - tv) = 0$. Multiply the first by fw and the second by eu to get $fwe(rv - su) = 0$ and $euf(sw - tv) = 0$. Subtracting, we have $rfwev - sfweu + seufw - teufv = evf(rw - tu) = 0$. Since $evf \in W$, this shows $(r, u) \sim (t, w)$. Therefore $\sim$ is an equivalence relation on $R \times W$. The set of equivalence classes is denoted $W^{-1}R$ and the equivalence class containing (r, w) is denoted by the fraction r/w.

LEMMA 3.1.2. *Let R be a commutative ring and W a multiplicative subset of R. Then $W^{-1}R$ is a commutative ring under the addition and multiplication operations*
$$\frac{r}{v} + \frac{s}{w} = \frac{rw + sv}{vw}, \quad \frac{r}{v}\frac{s}{w} = \frac{rs}{vw}.$$
The additive identity is $0/1$, the multiplicative identity is $1/1$. The map $\theta : R \to W^{-1}R$ defined by $r \mapsto r/1$ is a homomorphism of rings. The image of W under θ is a subset of the group of units of $W^{-1}R$.

PROOF. Assume $\frac{r}{v} = \frac{r_1}{v_1}$ and $\frac{s}{w} = \frac{s_1}{w_1}$. Then there exist α and β in W such that
$$\alpha(rv_1 - r_1 v) = 0 \tag{1.1}$$
$$\beta(sw_1 - s_1 w) = 0. \tag{1.2}$$
Multiply (1.1) by βww_1 and (1.2) by αvv_1 to get the identities
$$\alpha\beta rv_1 ww_1 - \alpha\beta r_1 vww_1 = 0$$
$$\alpha\beta sw_1 vv_1 - \alpha\beta s_1 wvv_1 = 0.$$

Adding the left-hand sides we derive

$$\alpha\beta\left((rw+sv)v_1w_1-(r_1w_1+s_1v_1)vw\right)=0.$$

This is the center equation in:

$$\frac{r}{v}+\frac{s}{w}=\frac{rw+sv}{vw}=\frac{r_1w_1+s_1v_1}{v_1w_1}=\frac{r_1}{v_1}+\frac{s_1}{w_1}.$$

Hence, addition of fractions is well defined. Multiply (1.1) by βsw_1 and (1.2) by $\alpha r_1 v$ to get the identities

$$\alpha\beta\left(rsv_1w_1-r_1vsw_1\right)=0$$
$$\alpha\beta\left(sw_1r_1v-s_1wr_1v\right)=0.$$

Adding the left-hand sides we derive

$$\alpha\beta\left(rsv_1w_1-r_1s_1vw\right)=0.$$

This is the center equation in:

$$\frac{r}{v}\frac{s}{w}=\frac{rs}{vw}=\frac{r_1s_1}{v_1w_1}=\frac{r_1}{v_1}\frac{s_1}{w_1}.$$

Hence, multiplication of fractions is well defined. It is routine to check that the associative and distributive laws hold and that $W^{-1}R$ is a commutative ring. The rest of the proof is left to the reader. □

DEFINITION 3.1.3. As in Lemma 3.1.2, let R be a commutative ring and W a multiplicative subset of R. The ring $W^{-1}R$ is called the *localization* of R at W. It comes with the natural map $\theta : R \to W^{-1}R$. If W is the set of all elements of R that are not zero divisors, then $W^{-1}R$ is called the *total ring of quotients* of R. If R is an integral domain and $W = R-(0)$, then $W^{-1}R$ is called the *quotient field*, or *field of fractions* of R.

The notion of localization is now extended to R-modules and R-algebras. Let M be an R-module and W a multiplicative subset of R. Define a relation on $M\times W$ by $(m_1,w_1)\sim(m_2,w_2)$ if and only if there exists $w\in W$ such that $w(w_2m_1-w_1m_2)=0$. The same argument used in Lemma 3.1.2 shows that $\sim$ is an equivalence relation on $M\times W$. The set of equivalence classes is denoted $W^{-1}M$ and the equivalence class containing (m,w) is denoted by the fraction m/w. We call $W^{-1}M$ the *localization of M at W*.

LEMMA 3.1.4. *Let R be a commutative ring, W a multiplicative set in R, and M an R-module.*

(1) *$W^{-1}M$ is a Z-module under the addition rule*
$$\frac{m_1}{w_1}+\frac{m_2}{w_2}=\frac{w_2m_1+w_1m_2}{w_1w_2}.$$
(2) *$W^{-1}M$ is an R-module under the multiplication rule*
$$r\frac{m}{w}=\frac{rm}{w}.$$
(3) *The assignment $m\mapsto m/1$ defines an R-module homomorphism $\sigma : M\to W^{-1}M$. The kernel of σ is equal to the the set of all $m\in M$ such that $wm=0$ for some w in W.*
(4) *If M is an R-algebra, the multiplication rule*
$$\frac{m_1}{w_1}\frac{m_2}{w_2}=\frac{m_1m_2}{w_1w_2}$$
makes $W^{-1}M$ into an R-algebra.

(5) *$W^{-1}M$ is a $W^{-1}R$-module under the multiplication rule*

$$\frac{r}{w_1}\frac{m}{w_2} = \frac{rm}{w_1 w_2}.$$

(6) *The assignment $\phi(m/w) = 1/w \otimes m$ defines a $W^{-1}R$-module isomorphism*

$$W^{-1}M \xrightarrow{\phi} W^{-1}R \otimes_R M.$$

PROOF. The proof is left to the reader. Notice that in (6) the inverse of ϕ is given by $a \otimes b \mapsto ab$. $\square$

EXAMPLE 3.1.5. Given a prime ideal P in R, let $W = R - P = \{x \in R \mid x \notin P\}$. As remarked in Example 3.1.1 (1), $R - P$ is a multiplicative set. The R-algebra $W^{-1}R$ is usually written R_P and if M is an R-module, we write M_P for the localization $W^{-1}M$. The ideal generated by P in R_P is $PR_P = \{x/y \in R_P \mid x \in P, y \notin P\}$. If $x/y \notin PR_P$, then $x \notin P$ so $y/x \in R_P$ is the multiplicative inverse of x/y. Since the complement of PR_P consists of units, the ideal PR_P contains every nonunit. So PR_P is the unique maximal ideal of R_P. As in Exercise 1.1.11, a local ring is a commutative ring that has a unique maximal ideal. Hence R_P is a local ring with maximal ideal PR_P, which is sometimes called the *local ring of R at P*. The factor ring R_P/PR_P is a field, which is sometimes called the *residue field* of R_P. The factor ring R/P is an integral domain and by Exercise 3.1.6, R_P/PR_P is isomorphic to the quotient field of R/P.

THEOREM 3.1.6. *(Universal Mapping Property) Let R be a commutative ring, W a multiplicative subset of R, and $W^{-1}R$ the localization. If S is a commutative ring and $f : R \to S$ a homomorphism such that $f(W) \subseteq \text{Units}(S)$, then there exists a unique homomorphism $\bar{f} : W^{-1}R \to S$*

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\theta"'] & & S \\ & W^{-1}R \arrow[ur, dashed, "\exists \bar{f}"'] & \end{tikzcd}$$

such that $f = \bar{f}\theta$.

PROOF. First we show the existence of $\bar{f}$. Assume $x_1/y_1 = x_2/y_2$. Then there exists $y \in W$ such that $y(x_1y_2 - x_2y_1) = 0$. Applying f, we get $f(y)(f(x_1)f(y_2) - f(x_2)f(y_1)) = 0$. Since $f(W) \subseteq \text{Units}(S)$ we get $f(x_1)f(y_1)^{-1} = f(x_2)f(y_2)^{-1}$. The reader should verify that $\bar{f}(x/y) = f(x)f(y)^{-1}$ defines a homomorphism of rings.

Now we prove the uniqueness of $\bar{f}$. Suppose $g : W^{-1}R \to S$ is another such homomorphism. Then for each $y \in W$, $f(y) = g\theta(y) = g(y/1)$ is a unit in S. Then $g(1/y) = g(y/1)^{-1}$ for each $y \in W$. Now $g(x/y) = g(\theta(x))g(\theta(y))^{-1} = f(x)f(y)^{-1} = \bar{f}(x/y)$. $\square$

Lemma 3.1.7 below shows that a localization of a commutative ring R is a flat R-module. In general, a localization $W^{-1}R$ is not projective (see Exercise 2.2.8).

LEMMA 3.1.7. *$W^{-1}R$ is a flat R-module.*

PROOF. Given an R-module monomorphism

$$0 \to A \xrightarrow{f} B$$

we need to show that

$$0 \to A \otimes_R W^{-1}R \xrightarrow{f \otimes 1} B \otimes_R W^{-1}R$$

is exact. Equivalently, by Lemma 3.1.4, we show

$$0 \to W^{-1}A \xrightarrow{f_W} W^{-1}B$$

is exact, where $f_W(a/w) = f(a)/w$. If $f(a)/w = 0$ in $W^{-1}B$, then there exists $y \in W$ such that $yf(a) = 0$. Then $f(ya) = 0$. Since f is one-to-one, $ya = 0$ in A. Then $a/w = 0$ in $W^{-1}A$. □

EXAMPLE 3.1.8. Let k be a field of characteristic different from 2. Let x be an indeterminate and $f(x) = x^2 - 1$. Let $R = k[x]/(f(x))$. The Chinese Remainder Theorem, Theorem 1.1.7, says $R \cong k[x]/(x-1) \oplus k[x]/(x+1)$. In R are the two idempotents $e_1 = (1+x)/2$ and $e_2 = (1-x)/2$. Notice that $e_1e_2 = 0$, $e_1 + e_2 = 1$, $e_i^2 = e_i$. Then $\{1, e_1\}$ is a multiplicative set. Consider the localization $R[e_1^{-1}]$ which is an R-algebra, hence comes with a structure homomorphism $\theta : R \to R[e_1^{-1}]$. Note that $\ker\theta = \{a \in R \mid a/1 = 0\} = \{a \in R \mid ae_1 = 0\} = Re_2$. Then the sequence

$$0 \to Re_2 \to R \xrightarrow{\theta} R[e_1^{-1}]$$

is exact. Since $e_1^2 = e_1$, multiplying by e_1/e_1 shows that an arbitrary element of $R[e_1^{-1}]$ can be represented in the form a/e_1. But an element $a \in R$ can be written $a = ae_1 + ae_2$ so every element of $R[e_1^{-1}]$ can be written $a/e_1 = (ae_1)/e_1 \in \theta(Re_1)$. That is, θ is onto and $R[e_1^{-1}] \cong R/Re_2$.

1.1. Local to Global Lemmas. Let R be a commutative ring and $\varphi : M \to N$ a homomorphism of R-modules. Suppose there is a multiplicative set $W \subseteq R$ such that the localization $\varphi_W : M_W \to N_W$ is one-to-one, or onto, or both. The results of this section are motivated by the question of whether φ is one-to-one, or onto, or both. Generally the answer is no, but we derive sufficient conditions such that the answer is yes for the localization at a subset of W of the form $\{1, w, w^2, ...\} \subseteq W$. In Section 3.3 we will see that in the Zariski topology on the set of all prime ideals of R, the set of prime ideals of the ring R_w is an open neighborhood of the set of prime ideals of R_W. This explains the terminology.

PROPOSITION 3.1.9. *Let R be a commutative ring and M an R-module. If $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ of R, then $M = (0)$.*

PROOF. Let $x \in M$. We show that $x = 0$. Assume $x \neq 0$. Look at $\operatorname{annih}_R(x) = \{y \in R \mid yx = 0\}$. Since $1 \notin \operatorname{annih}_R(x)$, there exists a maximal ideal $\mathfrak{m} \supseteq \operatorname{annih}_R(x)$. Since $x/1 = 0/1$ in $M_{\mathfrak{m}}$, there exists $y \notin \mathfrak{m}$ such that $yx = 0$. This is a contradiction. □

LEMMA 3.1.10. *Let R be a commutative ring, M a finitely generated R-module, and $W \subseteq R$ a multiplicative subset. Then $W^{-1}M = 0$ if and only if there exists $w \in W$ such that $wM = 0$.*

PROOF. If $wM = 0$, then clearly $W^{-1}M = 0$. Conversely, assume $W^{-1}M = 0$. Pick a generating set $\{m_1, \dots, m_n\}$ for M over R. Since each $m_i/1 = 0/1$ in M_W, there exist $w_1, \dots, w_n$ in W such that $w_im_i = 0$ for each i. Set $w = w_1w_2 \cdots w_n$. This w works. □

In the following, we write M_α instead of $M[\alpha^{-1}]$ for the localization of an R-module at the multiplicative set $\{1, \alpha, \alpha^2, \dots\}$.

LEMMA 3.1.11. *Let R be a commutative ring and $\varphi : M \to N$ a homomorphism of R-modules. Let $W \subseteq R$ be a multiplicative subset and $\varphi_W : M \otimes_R W^{-1}R \to N \otimes_R W^{-1}R$.*

(1) If φ_W is one-to-one and $\ker\varphi$ is a finitely generated R-module, then there exists $\alpha \in W$ such that $\varphi_\alpha : M_\alpha \to N_\alpha$ is one-to-one.

(2) *If φ_W is onto and* $\operatorname{coker}\varphi$ *is a finitely generated R-module, then there exists $\beta \in W$ such that $\varphi_\beta : M_\beta \to N_\beta$ is onto.*
(3) *If φ_W is an isomorphism and both* $\ker\varphi$ *and* $\operatorname{coker}\varphi$ *are finitely generated R-modules, then there exists $w \in W$ such that $\varphi_w : M_w \to N_w$ is an isomorphism.*

PROOF. Start with the exact sequence of R-modules

$$0 \to \ker(\varphi) \to M \xrightarrow{\varphi} N \to \operatorname{coker}(\varphi) \to 0. \tag{1.3}$$

Tensoring (1.3) with $(\cdot) \otimes_R R[W^{-1}]$ we get

$$0 \to W^{-1}\ker(\varphi) \to W^{-1}M \xrightarrow{\varphi_W} W^{-1}N \to W^{-1}\operatorname{coker}(\varphi) \to 0 \tag{1.4}$$

which is exact, by Lemma 3.1.7.

(1): If φ_W is one-to-one, then by Lemma 3.1.10 there is $\alpha \in W$ such that $\alpha(\ker(\varphi)) = 0$. Therefore, $\ker(\varphi) \otimes_R R[\alpha^{-1}] = 0$, and φ_α is one-to-one.

(2): If φ_W is onto, then by Lemma 3.1.10 there is $\beta \in W$ such that $\beta(\operatorname{coker}(\varphi)) = 0$. Therefore, $\operatorname{coker}(\varphi) \otimes_R R[\beta^{-1}] = 0$, and φ_β is onto.

(3): Let α be as in (1) and β as in (2). If we set $w = \alpha\beta$, then φ_w is an isomorphism of R_w-modules. □

LEMMA 3.1.12. *Let R be a commutative ring. Let A and B be commutative R-algebras and $\varphi : A \to B$ an R-algebra homomorphism. Assume* $\ker\varphi$ *is a finitely generated ideal of A, and B is a finitely generated A-algebra. If $W \subseteq R$ is a multiplicative subset and $\varphi \otimes 1 : A \otimes_R W^{-1}R \to B \otimes_R W^{-1}R$ is an isomorphism of $W^{-1}R$-algebras, then there exists $w \in W$ such that $\varphi_w : A_w \to B_w$ is an isomorphism of R_w-algebras.*

PROOF. Suppose $\ker\varphi = Ax_1 + \cdots + Ax_n$. By Lemma 3.1.10 there is $\alpha \in W$ such that $\alpha(Rx_1 + \cdots + Rx_n) = 0$. Therefore, $\alpha \ker\varphi = 0$. Suppose the A-algebra B is generated by $y_1, \dots, y_m$. By Lemma 3.1.10 there is $\beta \in W$ such that $\beta(Ry_1 + \cdots + Ry_m) \subseteq \varphi(A)$. If we set $w = \alpha\beta$, then $\varphi_w : A_w \to B_w$ is an isomorphism of R_w-algebras. □

LEMMA 3.1.13. *Let R be any ring and*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

an exact sequence of R-modules.

(1) *If B is finitely generated, then C is finitely generated.*
(2) *If A and C are finitely generated, then B is finitely generated.*
(3) *If B is finitely generated and C is of finite presentation, then A is finitely generated.*

PROOF. (1) and (2): Left to the reader.

(3): Consider the commutative diagram

$$\begin{tikzcd}
 & R^{(n)} \arrow[r, "\phi"] \arrow[d, dashed, "\exists\rho"] & R^{(n)} \arrow[r, "\psi"] \arrow[d, dashed, "\exists\eta"] & C \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & C \arrow[r] & 0
\end{tikzcd} \tag{1.5}$$

where the top row exists because C is of finite presentation. The homomorphism η exists by Proposition 2.1.1 (3) because $R^{(n)}$ is projective. Now $\beta\eta\phi = \psi\phi = 0$ so $\operatorname{im}\eta\phi \subseteq \ker\beta = \operatorname{im}\alpha$. Again, since $R^{(n)}$ is projective there exists ρ making the diagram commute. Since B is finitely generated, so is $\operatorname{coker}\eta$ by Part (1). The Snake Lemma 2.5.2 applied to

(1.5) says that $\operatorname{coker}\rho \cong \operatorname{coker}\eta$ so $\operatorname{coker}\rho$ is finitely generated. Because $\operatorname{im}\rho$ is finitely generated, the exact sequence

$$0 \to \operatorname{im}\rho \to A \to \operatorname{coker}\rho \to 0$$

and Part (2) show that A is finitely generated. □

LEMMA 3.1.14. *Let R be a commutative ring and M an R-module of finite presentation. Let $\mathfrak{p} \in \operatorname{Spec} R$ and assume $M_\mathfrak{p} = M \otimes_R R_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module. Then there exists $\alpha \in R - \mathfrak{p}$ such that M_α is a free R_α-module.*

PROOF. Since M is finitely generated, we know that $M_\mathfrak{p}$ is free of finite rank. Pick a basis $\{m_1/\alpha_1, \dots, m_n/\alpha_n\}$ for $M_\mathfrak{p}$ over $R_\mathfrak{p}$. Since $\{1/\alpha_1, \dots, 1/\alpha_n\}$ are units in $R_\mathfrak{p}$, it follows that $\{m_1/1, \dots, m_n/1\}$ is a basis for $M_\mathfrak{p}$ over $R_\mathfrak{p}$. Define $\varphi : R^n \to M$ by $(x_1, \dots, x_n) \mapsto \sum_{i=1}^n x_i m_i$, and consider the exact sequence of R-modules

$$0 \to \ker\varphi \to R^n \xrightarrow{\varphi} M \to \operatorname{coker}\varphi \to 0. \tag{1.6}$$

Tensoring (1.6) with $(\cdot) \otimes_R R_\mathfrak{p}$, we get

$$0 \to (\ker\varphi)_\mathfrak{p} \to R^n_\mathfrak{p} \xrightarrow{\varphi_\mathfrak{p}} M_\mathfrak{p} \to (\operatorname{coker}\varphi)_\mathfrak{p} \to 0 \tag{1.7}$$

which is exact, by Lemma 3.1.7. But $M_\mathfrak{p}$ is free over $R_\mathfrak{p}$ with basis $\{m_1/1, \dots, m_n/1\}$ and $\varphi_\mathfrak{p}$ maps the standard basis to this basis. That is, $\varphi_\mathfrak{p}$ is an isomorphism. So $0 = (\ker\varphi)_\mathfrak{p} = (\operatorname{coker}\varphi)_\mathfrak{p}$. Since M is finitely generated over R so is $\operatorname{coker}\varphi$. By Lemma 3.1.10 there exists $\beta \in R - \mathfrak{p}$ such that $\beta \cdot \operatorname{coker}\varphi = 0$. Then $(\operatorname{coker}\varphi)_\beta = 0$. Tensoring (1.6) with $(\ ) \otimes_R R_\beta$ we get the sequence

$$0 \to (\ker\varphi)_\beta \to R^n_\beta \xrightarrow{\varphi_\beta} M_\beta \to 0 \tag{1.8}$$

which is exact. Since M is a finitely presented R-module, M_β is a finitely presented R_β-module. By Lemma 3.1.13, $(\ker\varphi)_\beta$ is a finitely generated R_β-module. Since $\beta \in R - \mathfrak{p}$, by Theorem 3.1.6 there exists a homomorphism of rings $R_\beta \to R_\mathfrak{p}$ so we can tensor (1.8) with $(\cdot) \otimes_{R_\beta} R_\mathfrak{p}$ to get (1.7) again. That is, $(\ker\varphi)_\beta \otimes_{R_\beta} R_\mathfrak{p} \cong (\ker\phi)_\mathfrak{p} = 0$. Lemma 3.1.10 says there exists $\mu/\beta^k \in R_\beta - \mathfrak{p}R_\beta$ such that $\mu/\beta^k (\ker\phi)_\beta = 0$. But β is a unit in R_β so this is equivalent to $\mu (\ker\phi)_\beta = 0$. It is easy to check that $R_{\mu\beta} = R[(\mu\beta)^{-1}] = (R_\beta)_\mu$. This means $0 = \left((\ker\phi)_\beta\right)_\mu = (\ker\phi)_{\beta\mu}$. We also have $(\operatorname{coker}\phi)_{\beta\mu} = 0$. Tensor (1.6) with $R_{\mu\beta}$ to get $R^{(n)}_{\mu\beta} \cong M_{\mu\beta}$. Take $\alpha = \mu\beta$. □

1.2. Exercises.

EXERCISE 3.1.1. Let R be a commutative ring and W a multiplicative set. Let M be an R-module with submodules A and B. Prove:

(1) $W^{-1}(A+B) = W^{-1}A + W^{-1}B$
(2) $W^{-1}(A \cap B) = W^{-1}A \cap W^{-1}B$

EXERCISE 3.1.2. Let R be a commutative ring and assume $e \in R$ is a nonzero idempotent. Show that there is a natural homomorphism of rings $R[e^{-1}] \cong Re$. (Hint: The localization map $\theta : R \to R[e^{-1}]$ is onto and the kernel of θ is the principal ideal generated by the idempotent $1-e$.)

EXERCISE 3.1.3. Suppose R is a commutative ring, $R = R_1 \oplus R_2$ is a direct sum, and $\pi_i : R \to R_i$ is the projection. Let $\mathfrak{p}$ be a prime ideal in R_1 and $\mathfrak{q} = \pi_1^{-1}(\mathfrak{p})$. Prove that π_1 induces an isomorphism on local rings $R_\mathfrak{q} \cong (R_1)_\mathfrak{p}$.

EXERCISE 3.1.4. Suppose R is a commutative ring, $R = R_1 \oplus \cdots \oplus R_n$ is a direct sum, and $\pi_i : R \to R_i$ is the projection. Assume each R_i is a local ring with maximal ideal $\mathfrak{n}_i$. Let $\mathfrak{m}_i = \pi_i^{-1}(\mathfrak{n}_i)$. Prove:

(1) $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ is the complete list of maximal ideals of R.
(2) π_i induces an isomorphism on local rings $R_{\mathfrak{m}_i} \cong R_i$.
(3) The natural homomorphism $R \to R_{\mathfrak{m}_1} \oplus \cdots \oplus R_{\mathfrak{m}_n}$ is an isomorphism.

EXERCISE 3.1.5. Let R be a commutative ring, K a field, and $\phi : R \to K$ a homomorphism of rings. If P is the kernel of ϕ, show that P is a prime ideal of R and ϕ induces a homomorphism of fields $R_P/(PR_P) \to K$.

EXERCISE 3.1.6. Let R be a commutative ring and P a prime ideal in R. Show that $R_P/(PR_P)$ is isomorphic to the quotient field of R/P.

EXERCISE 3.1.7. Let $f : R \to S$ be a homomorphism of commutative rings and W a multiplicative subset of R. Prove:

(1) $f(W) \subseteq S$ is a multiplicative subset of S.
(2) If $Z = f(W)$ is the image of W, then $Z^{-1}S \cong W^{-1}S = S \otimes_R W^{-1}R$.
(3) If I is an ideal in R, then $W^{-1}(R/I) \cong (R/I) \otimes_R W^{-1}R \cong (W^{-1}R)/(I(W^{-1}R))$.

EXERCISE 3.1.8. Let R be a commutative ring. Let V and W be two multiplicative subsets of R. Prove:

(1) If $VW = \{vw \mid v \in V, w \in W\}$, then VW is a multiplicative subset of R.
(2) Let U be the image of V in $W^{-1}R$. Then $(VW)^{-1}R \cong U^{-1}(W^{-1}R) \cong V^{-1}(W^{-1}R)$.

EXERCISE 3.1.9. Let $R = \mathbb{Z}$ be the ring of integers and $S = \mathbb{Z}[2^{-1}]$ the localization of R obtained by inverting 2. Prove:

(1) If $P = (p)$ is a prime ideal of R and p is different from 2 and 0, then $R_P \cong S_P = S \otimes_R R_P$.
(2) If $P = (2)$ is the prime ideal of R generated by 2, then $S \otimes_R R_P$ is isomorphic to $\mathbb{Q}$. Therefore, R_P is not isomorphic to S_P.

EXERCISE 3.1.10. Let R be a commutative ring and P a prime ideal in R. Show that if $\alpha \in R - P$, then $R_P \cong (R_\alpha)_{PR_\alpha} \cong R_\alpha \otimes_R R_P$.

EXERCISE 3.1.11. Let $f : R \to S$ be a homomorphism of commutative rings. Let Q be a prime ideal in S and $P = f^{-1}(Q)$. Let $Q_P = Q \otimes_R R_P$ and $S_P = S \otimes_R R_P$. Prove:

(1) f induces a local homomorphism of local rings $g : R_P \to S_Q$.
(2) Q_P is a prime ideal of S_P.
(3) S_Q is isomorphic to the local ring of S_P at Q_P.
(4) The diagram

$$\begin{tikzcd} R_P \arrow[rr, "g"] \arrow[dr, "f\otimes 1"'] & & S_Q \\ & S_P \arrow[ur, "\phi"'] & \end{tikzcd}$$

commutes where ϕ is the localization map.

EXERCISE 3.1.12. Let R be an integral domain with quotient field K. Let $\operatorname{Max} R$ denote the set of all maximal ideals of R. If $\mathfrak{m} \in \operatorname{Max} R$, then $\mathfrak{m}$ is a prime ideal and by

Example 3.1.5 the local ring of R at $\mathfrak{m}$ is denoted $R_{\mathfrak{m}}$. By Exercise 3.1.15, $R_{\mathfrak{m}}$ can be viewed as a subring of K. Show that

$$R = \bigcap_{\mathfrak{m} \in \operatorname{Max} R} R_{\mathfrak{m}}.$$

EXERCISE 3.1.13. Let R be an integral domain with field of fractions K. Let M be a torsion free R-module (Definition 1.7.13) such that $K \otimes_R M$ is a finite dimensional K-vector space and $\dim_K(K \otimes_R M) = n$. Show that M contains a free R-submodule F of rank n such that M/F is a torsion R-module and the natural map $K \otimes_R F \to K \otimes_R M$ is an isomorphism.

EXERCISE 3.1.14. Let R be a commutative ring and $f \in R$. As remarked in Example 3.1.1 (3), $W = \{1, f, f^2, \dots\}$ is a multiplicative set. Localization of R at W is denoted $R[f^{-1}]$ and is sometimes called the R-algebra formed by "inverting f". Let α and β be two elements of R. Prove the following.

(1) If $\beta/1$ denotes the image of β in $R[\alpha^{-1}]$, then the ring $R[(\alpha\beta)^{-1}]$ is isomorphic to the ring $R[\alpha^{-1}][(\beta/1)^{-1}]$.
(2) If $i > 0$, then $R[\alpha^{-1}]$ and $R[\alpha^{-i}]$ are isomorphic as rings.

EXERCISE 3.1.15. Let R be a commutative ring and $W \subseteq R$ a multiplicative set. Let $V \subseteq W^{-1}R$ be a multiplicative set. Show that there exists a multiplicative set $U \subseteq R$ such that the rings $U^{-1}R$ and $V^{-1}(W^{-1}R)$ are isomorphic.

EXERCISE 3.1.16. Let R be a commutative ring, $W \subseteq R$ a multiplicative set, and $\theta : R \to W^{-1}R$ the natural map.

(1) The kernel of θ is equal to $\{x \in R \mid xw = 0 \text{ for some } w \in W\}$.
(2) θ is an isomorphism if and only if $W \subseteq \operatorname{Units}(R)$.

EXERCISE 3.1.17. Let R be a local PID with maximal ideal $\mathfrak{m}$. Let π be a generator for $\mathfrak{m}$. Let K be the quotient field of R. Prove:

(1) If π_1 is another irreducible element of R, then π and π_1 are associates. That is, up to associates, π is the unique irreducible element in R.
(2) As in Exercise 3.1.14, let $R[\pi^{-1}]$ be the R-algebra formed by inverting π. Then $R[\pi^{-1}]$ is equal to K, the quotient field of R.
(3) If x is a nonzero element of K, then x has a representation in the form $x = u\pi^n$, for a unit $u \in R^*$ and an integer n in $\mathbb{Z}$. The unit u and integer n are uniquely determined by x.

EXERCISE 3.1.18. Let R be a commutative ring, $f \in R - (0)$, and $R[f^{-1}]$ the R-algebra formed by inverting f (Exercise 3.1.14). Show that $R[f^{-1}]$ is a finitely generated R-algebra.

EXERCISE 3.1.19. Let R be a ring of characteristic 0 such that $(R, +)$ is a divisible abelian group. Show that the center of R contains a subfield isomorphic to $\mathbb{Q}$, hence R is a $\mathbb{Q}$-algebra. (Hint: Theorem 3.1.6.)

EXERCISE 3.1.20. As in Example 2.6.7, let S be the direct sum and P the direct product of the finite prime fields. Show that the quotient P/S is a $\mathbb{Q}$-algebra. (Hint: Exercise 3.1.19.)

2. Module Direct Summands of Rings

Let R be a ring and I a left ideal of R. The main result of this section, Lemma 3.2.4, is motivated by the question of whether R decomposes as an R-module into $I \oplus J$, for some left ideal J.

DEFINITION 3.2.1. Let R be a ring. An idempotent $e \in R$ is said to be *primitive* if e cannot be written as a sum of two nonzero orthogonal idempotents.

DEFINITION 3.2.2. Let R be a ring and $I \subseteq R$ a nonzero left ideal. Then I is a *minimal left ideal of R* if whenever J is a left ideal of R and $J \subseteq I$, then either $J = 0$, or $J = I$.

EXAMPLE 3.2.3. Let F be a field and $R = M_2(F)$ the ring of two-by-two matrices over F. Let

$$e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

The reader should verify the following facts.

(1) e_1 and e_2 are orthogonal idempotents.
(2) Re_1 is the set of all matrices with second column consisting of zeros.
(3) Re_2 is the set of all matrices with first column consisting of zeros.
(4) $R = Re_1 \oplus Re_2$ as R-modules.
(5) Re_1 is a minimal left ideal.
(6) e_1 is a primitive idempotent.

LEMMA 3.2.4. *Let R be a ring and I a left ideal of R.*

(1) I is an R-module direct summand of R if and only if $I = Re$ for some idempotent e.
(2) Suppose $e \in R$ is idempotent. Then e is primitive if and only if Re cannot be written as an R-module direct sum of proper left ideals of R.
(3) If I is a minimal left ideal, then I is an R-module direct summand of R if and only if $I^2 \neq 0$.
(4) Suppose $R = I \oplus J$ where I and J are two-sided ideals. Then $I = Re$ for some central idempotent e, I is a ring, and e is the multiplicative identity for I.

PROOF. (1): Assume $R = I \oplus L$. Write $1 = e + f$ where $e \in I$ and $f \in L$. Then $e = e^2 + ef$. Now $ef = e - e^2 \in I \cap L = 0$. Likewise $fe = 0$. Also $e + f = 1 = 1^2 = (e+f)^2 = e^2 + f^2$. In the direct sum the representation of 1 is unique, so $e = e^2$ and $f = f^2$. Let $x \in I$. Then $x = x \cdot 1 = xe + xf$. But $xf = x - xe \in I \cap L = 0$. So $Re = I$. Conversely assume $e^2 = e$ and prove that Re is a direct summand of R. Then $0 = e - e^2 = e(1-e) = (1-e)e$. Also $(1-e)^2 = 1 - e - e + e^2 = 1 - e$. This shows $e, 1-e$ are orthogonal idempotents. Since $1 = e + (1-e)$ we have $R = Re + R(1-e)$. Let $x \in Re \cap R(1-e)$. Then $x = ae = b(1-e)$ for some $a, b \in R$. Then $xe = ae^2 = ae = x$ and again $xe = b(1-e)e = 0$. Therefore $R = Re \oplus R(1-e)$.

(2): Use the same ideas as in (1) to show e is a sum of nonzero orthogonal idempotents if and only if Re decomposes into a direct sum of proper left ideals of R.

(3): Assume I is a minimal left ideal of R. Suppose $R = I \oplus L$ for some left ideal L of R. By (1), $I = Re$ for some idempotent e. Then $e = e^2 \in I^2$ so $I^2 \neq 0$. Conversely assume $I^2 \neq 0$. There is some $x \in I$ such that $Ix \neq 0$. But Ix is a left ideal of R and since I is minimal, we have $Ix = I$. For some $e \in I$, we have $ex = x$. Let $L = \operatorname{annih}_R(x) = \{r \in R \mid rx = 0\}$. Then L is a left ideal of R. Since $(1-e)x = x - ex = x - x = 0$ it follows that $1 - e \in L$. Therefore $1 = e + (1-e) \in I + L$ so $R = I + L$. Also, $e \in I$ and $ex = x \neq 0$ shows that $e \notin L$. Now $I \cap L$ is a left ideal in R and is contained in the minimal left ideal I. Since $I \cap L \neq I$, it follows that $I \cap L = 0$ which proves that $R = I \oplus L$ as R-modules.

(4): This follows from Theorem 1.1.8 (3). □

THEOREM 3.2.5. *Let R be a commutative ring and assume R decomposes into an internal direct sum $R = Re_1 \oplus \cdots \oplus Re_n$, where each e_i is a primitive idempotent. Then* *this decomposition is unique in the sense that, if $R = Rf_1 \oplus \cdots \oplus Rf_p$ is another such decomposition of R, then $n = p$, and after rearranging, $e_1 = f_1, \dots, e_n = f_n$.*

PROOF. Any idempotent of $R = Re_1 \oplus \cdots \oplus Re_n$ is of the form $x_1 + \cdots + x_n$ where x_i is an idempotent in Re_i. By Lemma 3.2.4, the only idempotents of Re_i are 0 and e_i. Hence, R has exactly n primitive idempotents, namely $e_1, \dots, e_n$. □

2.1. Exercises.

EXERCISE 3.2.1. Let R be a ring and I a left ideal in R. Prove that the following are equivalent.

(1) R/I is a projective left R-module.
(2) The R-module sequence $0 \to I \to R \to R/I \to 0$ is split exact.
(3) The left ideal I is finitely generated, and the left R-module R/I is flat.
(4) I is an R-module direct summand of R.
(5) There is an element $e \in R$ such that $1 - e \in I$ and $Ie = (0)$.
(6) There is an idempotent $e \in R$ such that $I = R(1-e)$.

EXERCISE 3.2.2. Let A be an R-algebra and e an idempotent in A.

(1) Show that eAe is an R-algebra.
(2) Show that there is an R-module direct sum decomposition:

$$A = eAe \oplus eA(1-e) \oplus (1-e)Ae \oplus (1-e)A(1-e).$$

3. The Prime Spectrum of a Commutative Ring

The set of all prime ideals in a commutative ring R is denoted $\operatorname{Spec} R$. We define a topology on $\operatorname{Spec} R$, the Zariski topology, and show that the assignment $R \mapsto \operatorname{Spec} R$ is a contravariant functor from the category of commutative rings to the category of topological spaces.

DEFINITION 3.3.1. Let R be a commutative ring. The *prime ideal spectrum* of R is

$$\operatorname{Spec} R = \{P \mid P \text{ is a prime ideal in } R\}.$$

The *maximal ideal spectrum* of R is

$$\operatorname{Max} R = \{\mathfrak{m} \mid \mathfrak{m} \text{ is a maximal ideal in } R\}.$$

Given a subset $L \subseteq R$, let

$$V(L) = \{P \in \operatorname{Spec} R \mid P \supseteq L\}.$$

Given a nonempty subset $Y \subseteq \operatorname{Spec} R$, let

$$I(Y) = \bigcap_{P \in Y} P.$$

Being an intersection of ideals, $I(Y)$ is an ideal. By definition, we take $I(\emptyset)$ to be the unit ideal R.

LEMMA 3.3.2. *Let L, L_1, L_2 denote subsets of R and Y_1, Y_2 subsets of* $\operatorname{Spec} R$.

(1) If $L_1 \subseteq L_2$, then $V(L_1) \supseteq V(L_2)$.
(2) If $Y_1 \subseteq Y_2$, then $I(Y_1) \supseteq I(Y_2)$.
(3) $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.
(4) If I is the ideal of R spanned by L, then $V(L) = V(I)$.

PROOF. Is left to the reader. □

LEMMA 3.3.3. *Given any collection $\{L_i\}$ of subsets of R*

(1) $V(\{1\}) = \emptyset$ *and* $V(\{0\}) = \operatorname{Spec} R$.
(2) $\bigcap_i V(L_i) = V(\bigcup L_i)$.
(3) $V(L_1) \cup V(L_2) = V\big(\{x_1x_2 \mid x_1 \in L_1, x_2 \in L_2\}\big)$.

PROOF. (1) is left to the reader. (2) follows because $P \in \cap V(L_i)$ if and only if $L_i \subseteq P$ for each i if and only if $\cup L_i \subseteq P$. For (3) suppose $P \supseteq L_1L_2$ and $L_1 \not\subseteq P$. Pick $x_1 \in L_1$ such that $x_1 \notin P$. Since $x_1L_2 \subseteq P$ and P is prime, $L_2 \subseteq P$. Therefore $P \in V(L_2)$. Conversely, if $P \in V(L_1) \cup V(L_2)$ then $L_1 \subseteq P$ or $L_2 \subseteq P$. Let $L_1 \subseteq P$. Multiplying, we get $L_1L_2 \subseteq P$. □

DEFINITION 3.3.4. By Lemma 3.3.3, the collection of sets $\{V(L) \mid L \subseteq R\}$ make up the closed sets for a topology on $\operatorname{Spec} R$, called the *Zariski topology*.

LEMMA 3.3.5. *Let R be a commutative ring. If $W \subseteq R$ is a multiplicative set and $0 \notin W$, then there exists a prime ideal $P \in \operatorname{Spec} R$ such that $P \cap W = \emptyset$.*

PROOF. Let $\mathscr{S} = \{I \subseteq R \mid I \text{ is an ideal and } I \cap W = \emptyset\}$. Then $(0) \in \mathscr{S}$. Apply Zorn's Lemma, Proposition 1.2.4. Then $\mathscr{S}$ has a maximal element, say P. To see that P is a prime ideal, assume $x \notin P$ and $y \notin P$. By maximality of P we know $Rx + P \cap W \neq \emptyset$ so there exists $a \in R$ and $u \in W$ such that $ax - u \in P$. Likewise $Ry + P \cap W \neq \emptyset$ so there exists $b \in R$ and $v \in W$ such that $by - v \in P$. Multiply, $abxy \equiv uv \pmod{P}$. Since $uv \in W$ and $P \cap W = \emptyset$ we have proved $xy \notin P$. □

DEFINITION 3.3.6. If R is a commutative ring, the set of all nilpotent elements of R is $\operatorname{Rad}_R(0) = \{x \in R \mid x^n = 0 \text{ for some } n > 0\}$. Then $\operatorname{Rad}_R(0)$ is called the *nil radical of R* and we show in Lemma 3.3.7 below that it is an ideal in R. More generally, if A is an ideal in R, the set

$$\operatorname{Rad}_R(A) = \{x \in R \mid x^n \in A \text{ for some } n > 0\}$$

is called the *nil radical of A*. When the ring R is understood, we usually write $\operatorname{Rad}(A)$ instead of $\operatorname{Rad}_R(A)$. If $A = \operatorname{Rad}(A)$, then we say A is a *radical ideal*. In Lemma 3.3.7 below we prove that $\operatorname{Rad}(A)$ is an ideal of R containing A.

LEMMA 3.3.7. *Let R be a commutative ring. Then the following are true.*

(1) $\operatorname{Rad}_R(0)$ *is an ideal in R and*

$$\operatorname{Rad}_R(0) = \bigcap_{P \in \operatorname{Spec} R} P.$$

(2) If A is an ideal in R, then $\operatorname{Rad}(A)$ *is an ideal in R which contains A and*

$$\operatorname{Rad}(A) = I(V(A)) = \bigcap_{P \in V(A)} P.$$

PROOF. (1): Pick $x \in \operatorname{Rad}_R(0)$. Fix $P \in \operatorname{Spec} R$. If $x^n = 0$, then either $x = 0$ or $n \geq 2$. If $n \geq 2$ then $x \cdot x^{n-1} \in P$ so $x \in P$ or $x^{n-1} \in P$. Inductively, $x \in P$ so $\operatorname{Rad}_R(0) \subseteq P$. If $x \notin \operatorname{Rad}_R(0)$, let $W = \{1, x, x^2, \dots\}$. Lemma 3.3.5 says there exists $P \in \operatorname{Spec} R$ such that $x \notin P$.

(2): Under the natural map $\eta : R \to R/A$ there is a one-to-one correspondence between ideals of R containing A and ideals of R/A. Under this correspondence, prime ideals correspond to prime ideals. To finish, apply Part (1). □

LEMMA 3.3.8. *Let A be an ideal in R and Y a subset of* $\operatorname{Spec} R$. *Then*

(1) $V(A) = V(\operatorname{Rad}(A))$, *and*
(2) $V(I(Y)) = \bar{Y}$, *the closure of Y in the Zariski topology.*

PROOF. (1): Since $A \subseteq \operatorname{Rad}(A)$, it follows that $V(A) \supseteq V(\operatorname{Rad}(A))$. Conversely, if $P \in \operatorname{Spec} R$ and $P \supseteq A$, then by Lemma 3.3.7, $P \supseteq \operatorname{Rad}(A)$. Then $P \in V(\operatorname{Rad}(A))$.

(2): Since $V(I(Y))$ is closed we have $V(I(Y)) \supseteq \bar{Y}$. Since $\bar{Y}$ is closed, $\bar{Y} = V(A)$ for some ideal A. Since $Y \subseteq \bar{Y}$, $I(Y) \supseteq I(\bar{Y}) = I(V(A)) = \operatorname{Rad}(A) \supseteq A$. Thus, $V(I(Y)) \subseteq V(A) = \bar{Y}$. $\square$

COROLLARY 3.3.9. *There is a one-to-one order-reversing correspondence between closed subsets of* $\operatorname{Spec} R$ *and radical ideals in R given by $Y \mapsto I(Y)$ and $A \mapsto V(A)$. Under this correspondence, irreducible closed subsets correspond to prime ideals.*

PROOF. The first part follows from Lemmas 3.3.2, 3.3.7, and 3.3.8. The last part is proved in Lemma 3.3.10. $\square$

LEMMA 3.3.10. *Let R be a commutative ring and Y a subset of* $\operatorname{Spec} R$*. Then Y is irreducible if and only if $P = I(Y)$ is a prime ideal in R. If Z is an irreducible closed subset of* $\operatorname{Spec} R$*, then $P = I(Z)$ is the unique minimal element of Z, and is called the* generic point *of Z.*

PROOF. Suppose Y is irreducible. Assume $x, y \in R$ and $xy \in I(Y)$. Notice that $Y \subseteq \bar{Y} = V(I(Y)) \subseteq V(xy) = V(x) \cup V(y)$. Since Y is irreducible, $Y \subseteq V(x)$ or $Y \subseteq V(y)$. Therefore, $x \in I(Y)$, or $y \in I(Y)$. This shows $I(Y)$ is a prime ideal. Conversely, assume $P = I(Y)$ is a prime ideal of R. The singleton set $\{P\}$ is irreducible, and by Lemma 1.3.4 the closure of $\{P\}$ is irreducible. By Lemma 3.3.8, the closure of $\{P\}$ is equal to $V(P)$, which is equal to $\bar{Y}$. By Lemma 1.3.4, Y is irreducible. The rest is left to the reader. $\square$

Let R be a commutative ring. If $\alpha \in R$, the basic open subset of $\operatorname{Spec} R$ associated to α is

$$U(\alpha) = \operatorname{Spec} R - V(\alpha) = \{Q \in \operatorname{Spec} R \mid \alpha \notin Q\}.$$

LEMMA 3.3.11. *Let R be a commutative ring.*

(1) Let $\alpha, \beta \in R$. The following are equivalent.
  - *(a) $V(\alpha) = V(\beta)$.*
  - *(b) $U(\alpha) = U(\beta)$.*
  - *(c) There exist $a \geq 1$, $b \geq 1$ such that $\alpha^a \in R\beta$ and $\beta^b \in R\alpha$.*

(2) If I is an ideal in R, then

$$\operatorname{Spec} R - V(I) = \bigcup_{\alpha \in I} U(\alpha)$$

Every open set can be written as a union of basic open sets. The collection of all basic open sets $\{U(\alpha) \mid \alpha \in R\}$ is said to be a basis *for the Zariski topology on* $\operatorname{Spec} R$.

PROOF. (1): By Lemma 3.3.7, $\operatorname{Rad}(R\alpha) = I(V(\alpha))$. By Lemma 3.3.8, $V(\alpha) = V(\operatorname{Rad}(R\alpha))$. So $V(\alpha) = V(\beta)$ if and only if $\operatorname{Rad}(R\alpha) = \operatorname{Rad}(R\beta)$ which is true if and only if there exist $a \geq 1$, $b \geq 1$ such that $\alpha^a \in R\beta$ and $\beta^b \in R\alpha$. The rest is left to the reader. $\square$

3.1. Idempotents and Subsets that are Open and Closed. The main result of this section, Theorem 3.3.13, states that there is a one-to-one correspondence between subsets of $\operatorname{Spec} R$ that are both open and closed and the set of principal ideals of R that are idempotent generated. Hence, there is a one-to-one correspondence between the left ideals of R that are R-module direct summands of R and the subsets of $\operatorname{Spec} R$ that are both open and closed.

Let R be any ring. The set of idempotents of R is denoted

$$\operatorname{idemp}(R) = \{x \in R \mid x^2 - x = 0\}.$$

The homomorphic image of an idempotent is an idempotent, so given a homomorphism of rings $R \to S$, there is a function $\operatorname{idemp}(R) \to \operatorname{idemp}(S)$.

LEMMA 3.3.12. *Let R be a commutative ring and $\operatorname{idemp}(R)$ the set of all idempotents of R.*

(1) If $e \in \operatorname{idemp}(R)$, then the closed set $V(1-e)$ is equal to the open set $U(e)$.
(2) Let $e, f \in \operatorname{idemp}(R)$. Then $V(e) = V(f)$ if and only if $e = f$.
(3) Let $e, f \in \operatorname{idemp}(R)$. Then $Re = Rf$ if and only if $e = f$.

PROOF. (1): Let $P \in \operatorname{Spec} R$. Since $e(1-e) = 0$, either $e \in P$, or $1-e \in P$. Since $1 = e + (1-e)$, P does not contain both e and $1-e$.

(2): Assume $V(e) = V(f)$. By Lemma 3.3.11, there exist $a \geq 1$, $b \geq 1$ such that $e = e^a \in Rf$ and $f = f^b \in Re$. Write $e = xf$ and $f = ye$ for some $x, y \in R$. Then $e = xf = xf^2 = (xf)f = ef = eye = ye^2 = ye = f$.

(3): $Re = Rf$ implies $V(e) = V(f)$, which by Part (2) implies $e = f$. □

THEOREM 3.3.13. *Let R be a commutative ring and define*

$$\mathscr{C} = \{Y \subseteq \operatorname{Spec} R \mid Y \text{ is open and closed}\}$$
$$\mathscr{D} = \{A \subseteq R \mid A \text{ is an ideal in } R \text{ which is an } R\text{-module direct summand of } R\}.$$

Then there are one-to-one correspondences:

$$\gamma : \operatorname{idemp}(R) \to \mathscr{C},$$

defined by $e \mapsto V(1-e) = U(e)$, and

$$\delta : \operatorname{idemp}(R) \to \mathscr{D},$$

defined by $e \mapsto Re$.

PROOF. Lemma 3.3.12, Parts (1) and (2) show that γ is well defined and one-to-one. By Lemma 3.2.4 (1), δ is well defined and onto. By Lemma 3.3.12 (3), δ is one-to-one. It remains to prove that γ is onto. Assume A_1, A_2 are ideals in R, $X_1 = V(A_1)$, $X_2 = V(A_2)$, $X_1 \cup X_2 = \operatorname{Spec} R$, $X_1 \cap X_2 = \emptyset$. We prove that $X_i = V(e_i)$ for some $e_i \in \operatorname{idemp}(R)$. Since $\emptyset = X_1 \cap X_2 = V(A_1 + A_2)$, we know A_1 and A_2 are comaximal and $A_1A_2 = A_1 \cap A_2$, by Exercise 1.1.9. Since $\operatorname{Spec} R = X_1 \cup X_2 = V(A_1A_2) = V(A_1 \cap A_2)$, Lemma 3.3.7 implies

$$A_1 \cap A_2 \subseteq \bigcap_{P \in \operatorname{Spec} R} P = \operatorname{Rad}_R(0).$$

That is, $A_1 \cap A_2$ consists of nilpotent elements. Write $1 = \alpha_1 + \alpha_2$, where $\alpha_i \in A_i$. Then $R = R\alpha_1 + R\alpha_2$ so $R\alpha_1$ and $R\alpha_2$ are comaximal. Also $R\alpha_1 \cap R\alpha_2 = R\alpha_1\alpha_2 \subseteq A_1 \cap A_2 \subseteq \operatorname{Rad}_R(0)$. So there exists $m > 0$ such that $(\alpha_1\alpha_2)^m = 0$. Then $R\alpha_1^m$ and $R\alpha_2^m$ are comaximal (Exercise 1.1.10) and $R\alpha_1^m \cap R\alpha_2^m = (0)$. By Proposition 1.1.9, R is isomorphic to the internal direct sum $R \cong R\alpha_1^m \oplus R\alpha_2^m$. By Theorem 1.1.8, there are orthogonal idempotents $e_1, e_2 \in R$ such that $1 = e_1 + e_2$ and $Re_i = R\alpha_i^m$. Then $\operatorname{Spec} R = V(e_1) \cup V(e_2)$ and $V(e_1) \cap$

$V(e_2) = \emptyset$. Moreover, $V(e_i) \supseteq V(R\alpha_i^m) \supseteq V(A_i) = X_i$. From this it follows that $X_i = V(e_i)$, hence γ is onto. $\square$

COROLLARY 3.3.14. *Suppose R is a commutative ring and* $\operatorname{Spec} R = X_1 \cup \cdots \cup X_r$, *where each X_i is a nonempty closed subset and $X_i \cap X_j = \emptyset$ whenever $i \neq j$. Then there are idempotents $e_1, \dots, e_r$ in R such that $X_i = U(e_i) = V(1-e_i)$ is homeomorphic to* $\operatorname{Spec} Re_i$, *and $R = Re_1 \oplus \cdots \oplus Re_r$.*

PROOF. By Theorem 3.3.13 there are unique idempotents $e_1, \dots, e_r$ in R such that $X_i = U(e_i) = V(1-e_i)$. Since $R = Re_i \oplus R(1-e_i)$, the map $\pi_i : R \to Re_i$ defined by $x \mapsto xe_i$ is a homomorphism of rings with kernel $R(1-e_i)$. By Exercise 3.3.5, π_i induces a homeomorphism $\operatorname{Spec} Re_i \to X_i$. If $i \neq j$, then $V(1-e_i) \cap V(1-e_j) = X_i \cap X_j = \emptyset$. It follows that the ideals $R(1-e_i)$ are pairwise relatively prime. By Theorem 1.1.7, the direct sum map

$$R \xrightarrow{\phi} Re_1 \oplus \cdots \oplus Re_r$$

is onto. By Exercise 1.1.9, the kernel of ϕ is the principal ideal generated by the product $(1-e_1)\cdots(1-e_r)$. But $X = X_1 \cup \cdots \cup X_r = V((1-e_1)\cdots(1-e_r))$. Therefore, $(1-e_1)\cdots(1-e_r) \in \operatorname{Rad}_R(0)$. Since the only nilpotent idempotent is 0, ϕ is an isomorphism. $\square$

COROLLARY 3.3.15. *The topological space* $\operatorname{Spec} R$ *is connected if and only if* 0 *and* 1 *are the only idempotents of R.*

COROLLARY 3.3.16. *Let e be an idempotent of R. The following are equivalent.*

(1) e is a primitive idempotent.
(2) $V(1-e) = U(e)$ is a connected component of $\operatorname{Spec} R$.
(3) 0 *and* 1 *are the only idempotents of the ring Re.*

PROOF. (1) is equivalent to (3): This follows from Lemma 3.2.4 (2).

(2) is equivalent to (3): Since $R = Re \oplus R(1-e)$, it follows from Exercise 3.3.5 that $V(1-e)$ is homeomorphic to $\operatorname{Spec} Re$. This follows from Corollary 3.3.15. $\square$

3.2. Exercises.

EXERCISE 3.3.1. Let R be a commutative ring and $P \in \operatorname{Spec} R$. Prove:

(1) The closure of the singleton set $\{P\}$ is equal to $V(P)$.
(2) The set $\{P\}$ is closed if and only if P is a maximal ideal in R.
(3) Let $U \subseteq \operatorname{Spec} R$ be an open set. Then $U = \operatorname{Spec} R$ if and only if $\operatorname{Max} R \subseteq U$.

EXERCISE 3.3.2. Prove that if R is a local ring, then 0 and 1 are the only idempotents in R.

EXERCISE 3.3.3. Let $\theta : R \to S$ be a homomorphism of commutative rings. Show that $P \mapsto \theta^{-1}(P)$ induces a function $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ which is continuous for the Zariski topology. If $\sigma : S \to T$ is another homomorphism, show that $(\sigma\theta)^\sharp = \theta^\sharp \sigma^\sharp$.

EXERCISE 3.3.4. For the following, let I and J be ideals in the commutative ring R. Prove that the nil radical satisfies the following properties.

(1) $I \subseteq \operatorname{Rad}(I)$
(2) $\operatorname{Rad}(\operatorname{Rad}(I)) = \operatorname{Rad}(I)$
(3) $\operatorname{Rad}(IJ) = \operatorname{Rad}(I \cap J) = \operatorname{Rad}(I) \cap \operatorname{Rad}(J)$
(4) $\operatorname{Rad}(I) = R$ if and only if $I = R$
(5) $\operatorname{Rad}(I+J) = \operatorname{Rad}(\operatorname{Rad}(I) + \operatorname{Rad}(J))$

(6) If $P \in \operatorname{Spec} R$, then for all $n > 0$, $P = \operatorname{Rad}(P^n)$.
(7) $I + J = R$ if and only if $\operatorname{Rad}(I) + \operatorname{Rad}(J) = R$.

EXERCISE 3.3.5. Let R be a commutative ring and $I \subsetneq R$ an ideal. Let $\eta : R \to R/I$ be the natural map and $\eta^\sharp : \operatorname{Spec}(R/I) \to \operatorname{Spec} R$ the continuous map of Exercise 3.3.3. Prove:

(1) $\eta^\sharp$ is a one-to-one order-preserving correspondence between the prime ideals of R/I and $V(I)$.
(2) There is a one-to-one correspondence between radical ideals in R/I and radical ideals in R containing I.
(3) Under $\eta^\sharp$ the image of a closed set is a closed set.
(4) $\eta^\sharp : \operatorname{Spec}(R/I) \to V(I)$ is a homeomorphism.
(5) If $I \subseteq \operatorname{Rad}_R(0)$, then $\eta^\sharp : \operatorname{Spec}(R/I) \to \operatorname{Spec}(R)$ is a homeomorphism.

EXERCISE 3.3.6. Let R be a commutative ring which is a direct sum of ideals $R = A_1 \oplus \cdots \oplus A_n$. As in Theorem 1.1.8, let $e_1, \dots, e_n$ be the orthogonal idempotents of R such that $A_i = Re_i$. For $1 \le i \le n$, let $\pi_i : R \to Re_i$ be the projection homomorphism. Prove:

(1) Let I be an ideal in R. Then I is prime if and only if there exists a unique $k \in \{1, \dots, n\}$ such that Ie_k is a prime ideal in Re_k and for all $i \neq k$, $Ie_i = Re_i$.
(2) Let $\pi_i^\sharp : \operatorname{Spec} R_i \to \operatorname{Spec} R$ be the continuous map defined in Exercise 3.3.3. Then $\operatorname{im} \pi_i^\sharp$ is equal to $V(1 - e_i) = U(e_i)$, hence is both open and closed.
(3) $\pi_i^\sharp : \operatorname{Spec} R_i \to V(1 - e_i) = U(e_i)$ is a homeomorphism.
(4) $\operatorname{Spec} R = \operatorname{im} \pi_1^\sharp \cup \cdots \cup \operatorname{im} \pi_n^\sharp$ and the union is disjoint.

EXERCISE 3.3.7. Let R be a commutative ring. Show that under the usual set inclusion relation, $\operatorname{Spec} R$ has at least one maximal element and at least one minimal element. (Hint: To prove that R contains a minimal prime ideal, reverse the set inclusion argument of Proposition 1.5.5.)

EXERCISE 3.3.8. Let R be a commutative ring and $I \subsetneq R$ an ideal. Prove that under the usual set inclusion relation, $V(I)$ contains at least one minimal element and at least one maximal element. A minimal element of $V(I)$ is called a *minimal prime over-ideal* of I.

EXERCISE 3.3.9. Let R be a commutative ring and W a multiplicative set. Let $\theta : R \to W^{-1}R$ be the localization. For any subset $S \subseteq W^{-1}R$, use the intersection notation $S \cap R = \theta^{-1}(S)$ for the preimage. Prove:

(1) If J is an ideal in $W^{-1}R$, then $J = W^{-1}(J \cap R)$.
(2) The continuous map $\theta^\sharp : \operatorname{Spec}(W^{-1}R) \to \operatorname{Spec}(R)$ is one-to-one.
(3) If $P \in \operatorname{Spec} R$ and $P \cap W = \emptyset$, then $W^{-1}P$ is a prime ideal in $W^{-1}R$.
(4) The image of $\theta^\sharp : \operatorname{Spec}(W^{-1}R) \to \operatorname{Spec}(R)$ consists of those prime ideals in R that are disjoint from W.
(5) If $P \in \operatorname{Spec} R$, there is a one-to-one correspondence between prime ideals in R_P and prime ideals of R contained in P.

EXERCISE 3.3.10. Let R be a commutative ring and α an element of R. Let R_α denote the localization $W^{-1}R$ with respect to the multiplicative set $W = \{\alpha^i \mid 0 \le i\}$ and $\theta : R \to R_\alpha$ the localization map. Prove:

(1) The image of $\theta^\sharp : \operatorname{Spec} R_\alpha \to \operatorname{Spec} R$ is the basic open set $U(\alpha) = \operatorname{Spec} R - V(\alpha)$.
(2) $\theta^\sharp : \operatorname{Spec} R_\alpha \to U(\alpha)$ is a homeomorphism.

EXERCISE 3.3.11. Let R be a commutative ring and W a multiplicative set. Prove:

(1) $\operatorname{Rad}_{W^{-1}R}(0) = W^{-1} \operatorname{Rad}_R(0)$.

(2) If I is a ideal of R, then $\operatorname{Rad}(W^{-1}I) = W^{-1}\operatorname{Rad}(I)$.

EXERCISE 3.3.12. Show that if R is a commutative ring, then $\operatorname{Spec} R$ is compact. That is, every open cover of $\operatorname{Spec} R$ has a finite subcover.

EXERCISE 3.3.13. Let $f : R \to S$ be a homomorphism of commutative rings. Let $\alpha \in R$ and assume $f(\alpha)$ is a unit in S. Prove that if $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is onto, then α is a unit in R.

4. Finitely Generated Projective Modules

As the title indicates, this section is about finitely generated projective modules over commutative rings. The first main result (Proposition 3.4.2) is that over a local ring R with maximal ideal $\mathfrak{m}$, a finitely generated projective module M is free, and a basis for $M/\mathfrak{m}M$ lifts to a basis for M. If R is a commutative ring and M is a finitely generated projective R-module, then for every $P \in \operatorname{Spec} R$, M_P is a free R_P-module. The second main result (Theorem 3.4.6) is a local to global theorem. If M is a finitely generated projective R-module, then for every $P \in \operatorname{Spec} R$ there exists $\alpha \in R - P$ such that M_α is a free R_α-module.

4.1. Finitely Generated Projective over a Local Ring is Free. As in Exercise 1.1.11, a local ring is a commutative ring that has a unique maximal ideal. Lemma 3.4.1 is an application of Nakayama's Lemma.

LEMMA 3.4.1. *Let R be a commutative ring and I an ideal in R. Let M be an R-module. If*

(1) I is nilpotent, or
(2) I is contained in every maximal ideal of R and M is finitely generated,

then a subset $X \subseteq M$ generates M as an R-module if and only if the image of X generates M/IM as an R/I-module.

PROOF. Let $\eta : M \to M/IM$. Suppose $X \subseteq M$ and let T be the R-submodule of M spanned by X. Then $\eta(T) = (T + IM)/IM$ is spanned by $\eta(X)$. If $T = M$, then $\eta(T) = M/IM$. Conversely, $\eta(T) = M/IM$ implies $M = T + IM$. By Corollary 2.2.5, this implies $M = T$. □

Another proof of Proposition 3.4.2 is presented in Corollary 3.7.5.

PROPOSITION 3.4.2. *Let R be a commutative local ring. If P is a finitely generated projective R-module, then P is free of finite rank. If $\mathfrak{m}$ is the maximal ideal of R and $\{x_i + \mathfrak{m}P \mid 1 \le i \le n\}$ is a basis for the vector space $P/\mathfrak{m}P$ over the residue field $R/\mathfrak{m}$, then $\{x_1, \dots, x_n\}$ is a basis for P over R. It follows that* $\operatorname{Rank}_R(P) = \dim_{R/\mathfrak{m}}(P/\mathfrak{m}P)$.

PROOF. Define $\phi : R^{(n)} \to P$ by $\phi(\alpha_1, \dots, \alpha_n) = \sum_{i=1}^n \alpha_i x_i$. The goal is to show that ϕ is onto and one-to-one, in that order. Denote by T the image of ϕ. Then $T = Rx_1 + \cdots + Rx_n$ which is the submodule of P generated by $\{x_1, \dots, x_n\}$. It follows from Lemma 3.4.1 that ϕ is onto. To show that ϕ is one-to-one we prove that $\ker\phi = 0$. Since P is R-projective, the sequence

$$0 \to \ker\phi \to R^{(n)} \xrightarrow{\phi} P \to 0$$

is split exact. Therefore, $\ker\phi$ is a finitely generated projective R-module. Upon tensoring with $(\ ) \otimes_R R/\mathfrak{m}$, ϕ becomes the isomorphism $(R/\mathfrak{m})^{(n)} \cong P/\mathfrak{m}P$. By Exercise 2.3.6,

$$0 \to \ker\phi \otimes_R R/\mathfrak{m} \to (R/\mathfrak{m})^{(n)} \xrightarrow{\phi} P/\mathfrak{m}P \to 0$$

is split exact. Therefore, $\ker\phi \otimes_R R/\mathfrak{m} = 0$, or in other words $\mathfrak{m}(\ker\phi) = \ker\phi$. By Nakayama's Lemma (Corollary 2.2.2), $\ker\phi = (0)$. $\square$

Corollary 3.4.3 is a special case of Proposition 10.4.14.

COROLLARY 3.4.3. *Let R be a commutative local ring with residue field k. Let $\psi : M \to N$ be a homomorphism of R-modules, where M is finitely generated and N is finitely generated and free. Then*

$$0 \to M \xrightarrow{\psi} N$$

is split exact if and only if $\psi \otimes 1 : M \otimes_R k \to N \otimes_R k$ is one-to-one.

PROOF. Assume $\psi \otimes 1$ is one-to-one. By Proposition 3.4.2 we can pick a generating set $\{x_1, \dots, x_n\}$ for the R-module M such that $\{x_1 \otimes 1, \dots, x_n \otimes 1\}$ is a basis for the k-vector space $M \otimes_R k$. Define $\pi : R^{(n)} \to M$ by mapping the ith standard basis vector to x_i. Then $\pi \otimes 1 : k^{(n)} \to M \otimes_R k$ is an isomorphism. The diagram

$$\begin{tikzcd}
R^{(n)} \arrow[r, "\pi"] \arrow[d] & M \arrow[r, "\psi"] \arrow[d] & N \arrow[d] \\
k^{(n)} \arrow[r, "\pi\otimes 1"] & M \otimes_R k \arrow[r, "\psi\otimes 1"] & N \otimes_R k
\end{tikzcd}$$

commutes. The composite map $\psi\pi \otimes 1$ is one-to-one. By Exercise 3.4.5, there is an R-module homomorphism $\tau : N \to R^{(n)}$ which is a left inverse for $\psi\pi$. Since π is onto, it follows that $\pi\tau$ is a left inverse for ψ.

Conversely, if ψ has a left inverse, then clearly $\psi \otimes 1$ is one-to-one. $\square$

4.2. A Finitely Generated Projective Module is Locally Free.

DEFINITION 3.4.4. Let M be a finitely generated projective module over the commutative ring R. For any prime ideal P of R, the localization M_P is a finitely generated projective R_P-module (Theorem 2.3.23). Therefore, M_P is a finitely generated free R_P-module (Proposition 3.4.2) and M_P has a well defined rank. If there is an integer $n \geq 0$ such that $n = \operatorname{Rank}_{R_P}(M_P)$ for all $P \in \operatorname{Spec} R$, then we say M has *constant rank* and write $\operatorname{Rank}_R(M) = n$.

PROPOSITION 3.4.5. *Let R be a commutative ring and S a commutative R-algebra. If M is a finitely generated projective R-module of constant rank $\operatorname{Rank}_R(M) = n$, then $M \otimes_R S$ is a finitely generated projective S-module of constant rank and $\operatorname{Rank}_S(M \otimes_R S) = n$.*

PROOF. By Theorem 2.3.23, $M \otimes_R S$ is a finitely generated projective S-module. Let $\theta : R \to S$ be the structure map. Let $Q \in \operatorname{Spec} S$ and $P = \theta^{-1}(Q) \in \operatorname{Spec} R$. Then by Exercise 3.1.11, θ extends to a local homomorphism of local rings $\theta : R_P \to S_Q$. The proof follows from

$$\begin{aligned}
(M \otimes_R S) \otimes_S S_Q &\cong M \otimes_R (S \otimes_S S_Q) \\
&\cong M \otimes_R S_Q \\
&\cong M \otimes_R (R_P \otimes_{R_P} S_Q) \\
&\cong (M \otimes_R R_P) \otimes_{R_P} S_Q \\
&\cong (R_P)^{(n)} \otimes_{R_P} S_Q \\
&\cong (S_Q)^{(n)}.
\end{aligned}$$

$\square$

In the following, for the localization of R at the multiplicative set $\{1, \alpha, \alpha^2, \dots\}$ we write R_α instead of $R[\alpha^{-1}]$.

THEOREM 3.4.6. *Let R be a commutative ring and M a finitely generated projective R-module.*

(1) Given $P \in \operatorname{Spec} R$ there exists $\alpha \in R - P$ such that M_α is a free R_α-module.
(2) If α is as in (1), then the values $\operatorname{Rank}_{R_Q}(M_Q)$ are constant for all $Q \in U(\alpha)$.
(3) The map

$$\begin{aligned} \operatorname{Spec} R &\xrightarrow{\phi} \{0,1,2,\dots\} \\ P &\mapsto \operatorname{Rank}_{R_P} M_P \end{aligned}$$

is continuous if $\{0,1,2,\dots\}$ is given the discrete topology (that is, the topology where every subset is closed, or equivalently, "points are open").

PROOF. (1): By Proposition 3.4.2 we know that M_P is a free module over R_P. By Corollary 2.1.8, M is an R-module of finite presentation. An application of Lemma 3.1.14 completes the proof.

(2): If $Q \in U(\alpha)$, then $\alpha \in R - Q$. By Exercise 3.1.10, $R_Q = (R_\alpha)_{QR_\alpha}$. Since M_α is R_α-free of rank n, it follows from Theorem 2.3.23 (1) that M_Q is R_Q-free of rank n.

(3): We need to prove that for every $n \geq 0$, the preimage $\phi^{-1}(n)$ is open in $\operatorname{Spec} R$. Let $P \in \operatorname{Spec} R$ such that $\operatorname{Rank}_{R_P} M_P = n$. It is enough to find an open neighborhood of P in the preimage of n. By Part (1), there exists $\alpha \in R - P$ such that M_α is free of rank n over R_α. Since $U(\alpha)$ is an open neighborhood of P in $\operatorname{Spec} R$, it is enough to show that $\operatorname{Rank}_{R_Q} M_Q = n$ for all $Q \in U(\alpha)$. This shows that (3) follows from Part (2). $\square$

COROLLARY 3.4.7. *Let R be a commutative ring and M a finitely generated projective R-module. Then there are idempotents $e_1, \dots, e_t$ in R satisfying the following.*

(1) $R = Re_1 \oplus \cdots \oplus Re_t$.
(2) $M = Me_1 \oplus \cdots \oplus Me_t$.
(3) If $R_i = Re_i$ and $M_i = M \otimes_R R_i$, then M_i is a finitely generated projective R_i-module of constant rank.
(4) If $\operatorname{Rank}_{R_i}(M_i) = n_i$, then $n_1, \dots, n_t$ are distinct.
(5) The integer t and the idempotents $e_1, \dots, e_t$ are uniquely determined by M.

In [**42**, Theorem IV.27] *the elements $e_1, \dots, e_t$ are called the* structure idempotents *of M.*

PROOF. The rank function $\phi : \operatorname{Spec} R \to \{0,1,2,\dots\}$ defined by $\phi(P) = \operatorname{Rank}_{R_P} M_P$ is continuous and locally constant (Theorem 3.4.6). Let $U_n = \phi^{-1}(\{n\})$ for each $n \geq 0$. Then $\{U_n \mid n \geq 0\}$ is a collection of subsets of $\operatorname{Spec} R$ each of which is open and closed. Moreover, the sets U_n are pairwise disjoint. Since $\operatorname{Spec} R$ is compact (Exercise 3.3.12) the image of ϕ is a finite set, say $\{n_1, \dots, n_t\}$. Let $e_1, \dots, e_t$ be the idempotents in R corresponding to the disjoint union $\operatorname{Spec} R = U_{n_1} \cup \cdots \cup U_{n_t}$ (Corollary 3.3.14). The rest is left to the reader. $\square$

COROLLARY 3.4.8. *If R is a commutative ring with no idempotents except* 0 *and* 1*, then for any finitely generated projective R-module M,* $\operatorname{Rank}_R M$ *is defined. That is, there exists $n \geq 0$ such that for every $P \in \operatorname{Spec} R$, $\operatorname{Rank}_{R_P} M_P = n$.*

PROOF. By Proposition 3.3.15 we know $\operatorname{Spec} R$ is connected. The continuous image of a connected space is connected. The rest follows from Corollary 3.4.7. $\square$

4.3. Exercises. For the following, R always denotes a commutative ring.

EXERCISE 3.4.1. Let L and M be finitely generated projective R-modules such that $\operatorname{Rank}_R(L)$ and $\operatorname{Rank}_R(M)$ are both defined. Prove:

(1) The rank of $L \oplus M$ is defined and is equal to the sum $\operatorname{Rank}_R(L) + \operatorname{Rank}_R(M)$.
(2) The rank of $L \otimes_R M$ is defined and is equal to the product $\operatorname{Rank}_R(L)\operatorname{Rank}_R(M)$.
(3) The rank of $\operatorname{Hom}_R(L,M)$ is defined and is equal to the product $\operatorname{Rank}_R(L)\operatorname{Rank}_R(M)$.

EXERCISE 3.4.2. Let $f : R \to S$ be a homomorphism of commutative rings and $P \in \operatorname{Spec} R$. Let $k(P) = R_P/PR_P$ be the residue field and $S_P = S \otimes_R R_P$. Let $Q \in \operatorname{Spec} S$ such that $P = f^{-1}(Q)$. Prove:

(1) $S \otimes_R k(P) \cong S_P/PS_P$.
(2) $Q \otimes_R k(P)$ is a prime ideal of $S \otimes_R k(P)$ and QS_P/PS_P is the corresponding prime ideal of S_P/PS_P.
(3) The localization of S_P/PS_P at QS_P/PS_P is S_Q/PS_Q.
(4) The localization of $S \otimes_R k(P)$ at the prime ideal $Q \otimes_R k(P)$ is $S_Q \otimes_R k(P)$.

EXERCISE 3.4.3. Let $f : R \to S$ be a homomorphism of commutative rings and $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 3.3.3.

(1) Let $W \subseteq R$ be a multiplicative set. Denote by $W^{-1}S$ the localization $S \otimes_R W^{-1}R$. Define all of the maps such that the diagram

$$\begin{tikzcd} \operatorname{Spec}(W^{-1}S) \arrow[r, "g^\sharp"] \arrow[d, "\varepsilon^\sharp"'] & \operatorname{Spec}(W^{-1}R) \arrow[d, "\eta^\sharp"] \\ \operatorname{Spec} S \arrow[r, "f^\sharp"] & \operatorname{Spec} R \end{tikzcd}$$

commutes. Show that $\varepsilon^\sharp$ and $\eta^\sharp$ are one-to-one.

(2) Let $I \subseteq R$ be an ideal. Define all of the maps such that the diagram

$$\begin{tikzcd} \operatorname{Spec}(S/IS) \arrow[r, "g^\sharp"] \arrow[d, "\varepsilon^\sharp"'] & \operatorname{Spec}(R/I) \arrow[d, "\eta^\sharp"] \\ \operatorname{Spec} S \arrow[r, "f^\sharp"] & \operatorname{Spec} R \end{tikzcd}$$

commutes. Show that $\varepsilon^\sharp$ and $\eta^\sharp$ are one-to-one.

(3) Let $P \in \operatorname{Spec} R$. Let $k(P) = R_P/PR_P$ be the residue field. Prove that there is a commutative diagram

$$\begin{tikzcd} \operatorname{Spec}(S \otimes_R k(P)) \arrow[r, "g^\sharp"] \arrow[d, "\varepsilon^\sharp"'] & \operatorname{Spec}(k(P)) \arrow[d, "\eta^\sharp"] \\ \operatorname{Spec} S \arrow[r, "f^\sharp"] & \operatorname{Spec} R \end{tikzcd}$$

where $\varepsilon^\sharp$ and $\eta^\sharp$ are one-to-one. Show that the image of $\varepsilon^\sharp$ is $(f^\sharp)^{-1}(P)$. (Hints: Take $W = R - P$ in (1), then take $I = PR_P$ in (2). We call $\operatorname{Spec}(S \otimes_R k(P))$ the *fiber* over P of the map $f^\sharp$.

EXERCISE 3.4.4. Let R be a commutative ring. Let M and N be finitely generated projective R-modules, and $\varphi : M \to N$ an R-module homomorphism. Let $\mathfrak{p} \in \operatorname{Spec} R$ and assume $\varphi \otimes 1 : M \otimes_R R_\mathfrak{p} \to N \otimes_R R_\mathfrak{p}$ is an isomorphism. Prove that there exists $\alpha \in R - \mathfrak{p}$ such that $\varphi \otimes 1 : M \otimes_R R_\alpha \to N \otimes_R R_\alpha$ is an isomorphism.

EXERCISE 3.4.5. Let R be a commutative local ring with residue field k. Let M and N be finitely generated free R-modules and $\psi : M \to N$ a homomorphism of R-modules. Show that if $\psi \otimes 1 : M \otimes_R k \to N \otimes_R k$ is one-to-one, then ψ has a left inverse. That is, there exists an R-module homomorphism $\sigma : N \to M$ such that $\sigma\psi = 1$ is the identity mapping on M.

EXERCISE 3.4.6. Let R be a commutative ring and S a commutative R-algebra that as an R-module is a progenerator. Show that if $\operatorname{Spec} R$ is connected, then the number of connected components of $\operatorname{Spec} S$ is bounded by $\operatorname{Rank}_R(S)$, hence is finite.

EXERCISE 3.4.7. Let R_1 and R_2 be rings and $S = R_1 \oplus R_2$ the direct sum. Let M be a left S-module. Using the projection maps $\pi_i : S \to R_i$, show that the R_i-modules $M_i = R_i \otimes_S M$ are S-modules. Show that M is isomorphic as an S-module to the direct sum $M_1 \oplus M_2$.

5. Faithfully Flat Modules and Algebras

5.1. Faithfully Flat Modules. Recall that in Definition 2.3.19 we defined a left R-module N to be flat if the functor $(\,) \otimes_R N$ is both left and right exact. In Exercise 2.8.2 we defined N to be faithfully flat if N is flat, and N has the property that for any right R-module M, $M \otimes_R N = 0$ implies $M = 0$. If R is a commutative ring, then Lemma 3.5.1 below adds more necessary and sufficient conditions for N to be faithfully flat.

LEMMA 3.5.1. *Let R be a commutative ring and N an R-module. The following are equivalent.*

(1) *A sequence of R-modules*
$$0 \to A \to B \to C \to 0$$
is exact if and only if
$$0 \to A \otimes_R N \to B \otimes_R N \to C \otimes_R N \to 0$$
is exact.

(2) *A sequence of R-modules*
$$A \xrightarrow{f} B \xrightarrow{g} C$$
is exact if and only if
$$A \otimes_R N \xrightarrow{f\otimes 1} B \otimes_R N \xrightarrow{g\otimes 1} C \otimes_R N$$
is exact.

(3) *N is faithfully flat. That is, N is flat and for any R-module M, if $M \otimes_R N = 0$, then $M = 0$.*

(4) *N is flat and for every maximal ideal $\mathfrak{m}$ of R, $N \neq \mathfrak{m}N$.*

PROOF. (1) implies (2): Start with a sequence of R-modules
$$A \xrightarrow{f} B \xrightarrow{g} C$$
and assume in the sequence
$$A \otimes_R N \xrightarrow{f\otimes 1} B \otimes_R N \xrightarrow{g\otimes 1} C \otimes_R N$$

that $\operatorname{im}(f\otimes 1)=\ker(g\otimes 1)$. We must prove that $\operatorname{im} f=\ker g$. Factor f through $A/\ker f$ and factor g through $\operatorname{im} g$ to get the sequence

$$0\to A/\ker f\xrightarrow{\bar f} B\xrightarrow{\bar g}\operatorname{im} g\to 0 \tag{5.1}$$

where $\bar f$ is one-to-one and $\bar g$ is onto. It is enough to prove $\operatorname{im}\bar f=\ker\bar g$. Tensor (5.1) with N to get the sequence

$$0\to A/\ker f\otimes_R N\xrightarrow{\bar f\otimes 1} B\otimes_R N\xrightarrow{\bar g\otimes 1}\operatorname{im} g\otimes_R N\to 0. \tag{5.2}$$

By (1) we know that $\bar f\otimes 1$ is one-to-one and $\bar g\otimes 1$ is onto. By (1), it is enough to show (5.2) is exact. To do this, it is enough to show $\operatorname{im}(\bar f\otimes 1)=\operatorname{im}(f\otimes 1)$ and $\ker(\bar g\otimes 1)=\ker(g\otimes 1)$. Consider the commutative diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[d, "="] \\ A/\ker f \arrow[r, "\bar f"] & B \end{tikzcd}$$

in which the natural map α is onto, and $\bar f$ is one-to-one. Tensor with N to get the commutative diagram

$$\begin{tikzcd} A\otimes_R N \arrow[r, "f\otimes 1"] \arrow[d, "\alpha\otimes 1"'] & B\otimes_R N \arrow[d, "="] \\ A/\ker f\otimes_R N \arrow[r, "\bar f\otimes 1"] & B\otimes_R N \end{tikzcd}$$

in which $\alpha\otimes 1$ is onto. It follows that $\operatorname{im}(\bar f\otimes 1)=\operatorname{im}(f\otimes 1)$. Consider the commutative diagram

$$\begin{tikzcd} B \arrow[r, "\bar g"] \arrow[d, "="'] & \operatorname{im} g \arrow[d, "\beta"] \\ B \arrow[r, "g"] & C \end{tikzcd}$$

in which the inclusion map β is one-to-one and $\bar g$ is onto. Tensor with N to get the commutative diagram

$$\begin{tikzcd} B\otimes_R N \arrow[r, "\bar g\otimes 1"] \arrow[d, "="'] & \operatorname{im} g\otimes_R N \arrow[d, "\beta\otimes 1"] \\ B\otimes_R N \arrow[r, "g\otimes 1"] & C\otimes_R N \end{tikzcd}$$

in which $\beta\otimes 1$ is one-to-one because N is flat. It follows that $\ker(\bar g\otimes 1)=\ker(g\otimes 1)$.

(1) implies (3): Clearly N is flat. Assume $N\otimes_R M=0$. Then $0\to N\otimes_R M\to 0$ is exact and (1) implies $0\to M\to 0$ is exact.

(3) implies (4): Let $\mathfrak m$ be a maximal ideal of R. Then $M=R/\mathfrak m$ is not zero. By (3), $0\neq N\otimes_R R/\mathfrak m=N/\mathfrak m N$. Therefore $N\neq\mathfrak m N$.

(4) implies (3): Suppose $M\neq 0$ and prove $N\otimes_R M\neq 0$. Let $x\in M$, $x\neq 0$. Then if $I=\operatorname{annih}_R(x)$, we have $I\neq R$. Let $\mathfrak m$ be a maximal ideal of R containing I. By (4) we get $IN\subseteq\mathfrak m N\neq N$. Then $N\otimes_R R/I=N/IN\neq 0$. Tensor the exact sequence $0\to R/I\to M$ with $(\cdot)\otimes N$ and by flatness we know $0\to N\otimes_R R/I\to N\otimes_R M$ is exact. Therefore $N\otimes_R M\neq 0$.

(3) implies (2): Start with a sequence of R-modules

$$A \xrightarrow{f} B \xrightarrow{g} C$$

and assume

$$A \otimes_R N \xrightarrow{f \otimes 1} B \otimes_R N \xrightarrow{g \otimes 1} C \otimes_R N$$

is exact.

Step 1: Show that $\operatorname{im} f \subseteq \ker g$. Tensor the exact sequence

$$A \xrightarrow{g \circ f} \operatorname{im}(g \circ f) \to 0.$$

with N to get the exact sequence

$$A \otimes_R N \xrightarrow{g \circ f \otimes 1} \operatorname{im}(g \circ f) \otimes_R N \to 0.$$

By Lemma 2.3.7, $\operatorname{im}(g \circ f) \otimes_R N = \operatorname{im}((g \otimes 1) \circ (f \otimes 1)) = 0$. By (3) we have $\operatorname{im}(g \circ f) = 0$, so $g \circ f = 0$.

Step 2: Show $\operatorname{im} f \supseteq \ker g$. Set $H = \ker g / \operatorname{im} f$. To prove $H = 0$ it is enough to show $H \otimes_R N = 0$. Tensor the exact sequence

$$A \xrightarrow{f} \ker g \to H \to 0.$$

with N to get the exact sequence

$$A \otimes_R N \xrightarrow{f \otimes 1} \ker g \otimes_R N \to H \otimes_R N \to 0.$$

The reader should verify that $\ker g \otimes_R N = \ker(g \otimes 1)$ and $H \otimes_R N = \ker(g \otimes 1)/\operatorname{im}(f \otimes 1) = 0$. The proof follows.

(2) implies (1): Is left to the reader. □

EXAMPLE 3.5.2. If N is projective, then N is flat (Exercise 2.3.6) but not necessarily faithfully flat. For example, say the ring $R = I \oplus J$ is an internal direct sum of two nonzero ideals I and J. Then $IJ = 0$, $I^2 = I$, $J^2 = J$ and $I + J = R$. The sequence $0 \to I \to 0$ is not exact. Tensor with $(\cdot) \otimes_R J$ and get the exact sequence $0 \to 0 \to 0$. So J is not faithfully flat.

PROPOSITION 3.5.3. *Let R be a commutative ring. The R-module*

$$E = \bigoplus_{\mathfrak{m} \in \operatorname{Max} R} R_{\mathfrak{m}}$$

is faithfully flat.

PROOF. Each $R_{\mathfrak{m}}$ is flat by Lemma 3.1.7, so E is flat by Exercise 3.5.4. For every maximal ideal $\mathfrak{m}$ of R, $\mathfrak{m}R_{\mathfrak{m}} \neq R_{\mathfrak{m}}$ so $\mathfrak{m}E \neq E$. To finish the proof, apply Lemma 3.5.1. □

5.2. Faithfully Flat Algebras.

LEMMA 3.5.4. *If $\theta : R \to S$ is a homomorphism of commutative rings such that S is a faithfully flat R-module, then the following are true.*

(1) For any R-module M,

$$M \to M \otimes_R S$$
$$x \mapsto x \otimes 1$$

is one-to-one. In particular, θ is one-to-one, so we can view $R = \theta(R)$ as a subring of S.

(2) For any ideal $I \subseteq R$, $IS \cap R = I$.

(3) *The continuous map* $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ *of Exercise 3.3.3 is onto.*

PROOF. (1): Let $x \neq 0$, $x \in M$. Then Rx is a nonzero submodule of M. If follows from Lemma 3.5.1 (2) that $Rx \otimes_R S \neq 0$. But $Rx \otimes_R S = S(x \otimes 1)$ so $x \otimes 1 \neq 0$.

(2): Apply Part (1) with $M = R/I$. Then $\bar{\theta} : R/I \to R/I \otimes_R S = S/IS$ is one-to-one.

(3): Let $P \in \operatorname{Spec} R$. By Exercise 3.5.3, $S_P = S \otimes_R R_P$ is faithfully flat over R_P. By Part (2), $PR_P = PS_P \cap R_P$, so PS_P is not the unit ideal. Let $\mathfrak{m}$ be a maximal ideal of S_P containing PS_P. Then $\mathfrak{m} \cap R_P \supseteq PR_P$. Since PR_P is a maximal ideal, $\mathfrak{m} \cap R_P = PR_P$. Let $Q = \mathfrak{m} \cap S$. So $Q \cap R = (\mathfrak{m} \cap S) \cap R = \mathfrak{m} \cap R = (\mathfrak{m} \cap R_P) \cap R = PR_P \cap R = P$. $\square$

LEMMA 3.5.5. *If $\theta : R \to S$ is a homomorphism of commutative rings, then the following are equivalent.*

(1) *S is faithfully flat as an R-module.*
(2) *S is a flat R-module and the continuous map $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is onto.*
(3) *S is a flat R-module and for each maximal ideal $\mathfrak{m}$ of R, there is a maximal ideal $\mathfrak{n}$ of S such that $\mathfrak{n} \cap R = \mathfrak{m}$.*

PROOF. (1) implies (2): Follows from Lemma 3.5.4 (3).

(2) implies (3): There is a prime P of S and $P \cap R = \mathfrak{m}$. Let $\mathfrak{n}$ be a maximal ideal of S containing P. Then $\mathfrak{n} \cap R \supseteq P \cap R = \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\mathfrak{n} \cap R = \mathfrak{m}$.

(3) implies (1): For each maximal ideal $\mathfrak{m}$ of R, pick a maximal ideal $\mathfrak{n}$ of S lying over $\mathfrak{m}$. Then $\mathfrak{m}S \subseteq \mathfrak{n} \neq S$. By Lemma 3.5.1 (3), S is faithfully flat. $\square$

PROPOSITION 3.5.6. *Let R be a commutative ring and $\varepsilon : R \to A$ a homomorphism of rings such that ε makes A into a progenerator R-module.*

(1) *Under ε, R is mapped isomorphically onto an R-module direct summand of A.*
(2) *If B is a subring of A containing the image of ε, then the image of ε is an R-module direct summand of B.*
(3) *A is faithfully flat as an R-module.*

PROOF. (1): By Corollary 2.2.4, A is R-faithful. The sequence

$$0 \to R \xrightarrow{\varepsilon} A$$

is exact, where $\varepsilon(r) = r \cdot 1$. By Exercise 2.4.2, there is a splitting map for ε if and only if

$$\operatorname{Hom}_R(A,R) \xrightarrow{\mathrm{H}_\varepsilon} \operatorname{Hom}_R(R,R) \to 0 \tag{5.3}$$

is exact. Let $\mathfrak{m}$ be a maximal ideal in R. By Theorem 2.3.23, $A \otimes_R R/\mathfrak{m} = A/\mathfrak{m}A$ is a progenerator over the field $R/\mathfrak{m}$. In other words, $A/\mathfrak{m}A$ is a nonzero finite dimensional vector space over $R/\mathfrak{m}$. The diagram

$$\begin{tikzcd}
R/\mathfrak{m} \otimes_R \operatorname{Hom}_R(A,R) \arrow[r, "1\otimes \mathrm{H}_\varepsilon"] \arrow[d, "\cong"'] & R/\mathfrak{m} \otimes_R \operatorname{Hom}_R(R,R) \arrow[r] \arrow[d, "\cong"] & 0 \\
\operatorname{Hom}_{R/\mathfrak{m}}(A/\mathfrak{m}A, R/\mathfrak{m}) \arrow[r, "\mathrm{H}_\varepsilon"] & \operatorname{Hom}_{R/\mathfrak{m}}(R/\mathfrak{m}, R/\mathfrak{m}) \arrow[r] & 0
\end{tikzcd}$$

commutes. The bottom row is exact since $0 \to R/\mathfrak{m} \to A/\mathfrak{m}A$ is split exact over $R/\mathfrak{m}$. The vertical maps are isomorphisms by Corollary 2.4.13. Therefore the top row is exact. Corollary 2.4.3 says that (5.3) is exact. This proves (1).

(2): Assume $R \subseteq B \subseteq A$ is a tower of subrings. If $\sigma : A \to R$ is a left inverse for $\varepsilon : R \to A$, then σ restricts to a left inverse for $R \to B$.

(3): This follows from Exercise 2.8.2. $\square$

Let S be a faithfully flat R-algebra. In the terminology of Exercise 2.4.1, Proposition 3.5.7 shows that the functor $S \otimes_R ()$ from the category of left R-modules to the category of left S-modules is faithful.

PROPOSITION 3.5.7. *Let S be a faithfully flat R-algebra. If M and N are R-modules, then the function*

$$\operatorname{Hom}_R(M,N) \xrightarrow{\phi} \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N)$$

defined by $f \mapsto 1 \otimes f$ is a monomorphism of abelian groups.

PROOF. By Lemma 2.3.17 (4), $S \otimes_R ()$ is a functor from the category of left R-modules to the category of left S-modules. The reader should verify that the assignment $f \mapsto 1 \otimes f$ defines a homomorphism of abelian groups $\phi : \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N)$. Suppose $f : M \to N$ is a homomorphism of left R-modules and $1 \otimes f : S \otimes_R M \to S \otimes_R N$ is the zero homomorphism. In the commutative diagram

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\alpha"'] & & N \\ & \operatorname{im} f \arrow[ur, "\beta"'] & \end{tikzcd}$$

α is onto and β is one-to-one. Since S is flat, in the commutative diagram

$$\begin{tikzcd} S \otimes_R M \arrow[rr, "1 \otimes f"] \arrow[dr, "1 \otimes \alpha"'] & & S \otimes_R N \\ & S \otimes_R \operatorname{im} f \arrow[ur, "1 \otimes \beta"'] & \end{tikzcd}$$

$1 \otimes \alpha$ is onto and $1 \otimes \beta$ is one-to-one. By assumption, the image of $1 \otimes f$ is (0). Therefore, $S \otimes_R \operatorname{im} f = (0)$. Since S is faithfully flat, this implies $\operatorname{im} f = (0)$. $\square$

5.3. Another Hom Tensor Relation.

PROPOSITION 3.5.8. *Let S be a flat commutative R-algebra. Let M and N be R-modules, and assume M is finitely generated.*

(1) *The natural map*

$$S \otimes_R \operatorname{Hom}_R(M,N) \xrightarrow{\alpha} \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N)$$

is a monomorphism of S-modules.

(2) *If M is a finitely presented R-module, then α is an isomorphism of S-modules.*

PROOF. If M is finitely generated and projective, then this follows from Corollary 2.4.13.

(1): By Exercise 2.2.5, M has a free resolution. So there are index sets I and J and an exact sequence

$$R^J \to R^I \to M \to 0 \tag{5.4}$$

of R-modules. Since M is finitely generated, we assume I is a finite set. Since S is flat, the functor $S \otimes_R (\cdot)$ is exact. By Lemmas 2.3.15 and 2.3.13,

$$S^J \to S^I \to S \otimes_R M \to 0 \tag{5.5}$$

is an exact sequence of S-modules. By Proposition 2.4.5, the contravariant functor $\operatorname{Hom}_R(\cdot, N)$ is left exact. Applying it to (5.4), we get the exact sequence

$$0 \to \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(R^I,N) \to \operatorname{Hom}_R(R^J,N). \tag{5.6}$$

By Lemma 2.4.7 and Proposition 2.4.8, (5.6) can be written as

$$0 \to \operatorname{Hom}_R(M,N) \to \prod_I N \to \prod_J N. \tag{5.7}$$

Tensoring (5.7) with the flat module S gives the exact sequence

$$0 \to S \otimes_R \operatorname{Hom}_R(M,N) \to S \otimes_R \prod_I N \to S \otimes_R \prod_J N. \tag{5.8}$$

Apply the left exact functor $\operatorname{Hom}_S(\cdot, S \otimes_R N)$ to (5.5). By Lemma 2.4.7 and Proposition 2.4.8,

$$0 \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \to \prod_I (S \otimes_R N) \to \prod_J (S \otimes_R N) \tag{5.9}$$

is an exact sequence of S-modules. Since I is a finite set, $\prod_I N$ is equal to $\bigoplus_I N$ and $S \otimes_R \bigoplus_I N \cong \bigoplus_I (S \otimes_R N) \cong \prod_I S \otimes_R N$ by Lemma 2.3.15. Combining (5.8) and (5.9) with the natural maps yields a commutative diagram

$$\begin{tikzcd} S \otimes_R \operatorname{Hom}_R(M,N) \arrow[r, "f_1", "\text{1-to-1}"'] \arrow[d, "\alpha"'] & \bigoplus_I (S \otimes_R N) \arrow[r, "f_2"] \arrow[d, "\beta"'] & S \otimes_R \prod_J N \arrow[d, "\gamma"'] \\ \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \arrow[r, "g_1", "\text{1-to-1}"'] & \bigoplus_I (S \otimes_R N) \arrow[r, "g_2"] & \prod_J (S \otimes_R N). \end{tikzcd} \tag{5.10}$$

Since f_1 and β are one-to-one, α is one-to-one.

(2): Because M is of finite presentation, the index sets I and J can both be chosen to be finite. Hence we assume the vertical maps β and γ are both isomorphisms. To see that α is onto, let x be an element of the lower left corner of (5.10). Set $y = \beta^{-1}(g_1(x))$. Then $\gamma(f_2(y)) = g_2(\beta(y)) = g_2(g_1(x)) = 0$. So $y = f_1(z)$ for some z in the upper left corner. Then $x = \alpha(z)$. Note that this also follows from a slight variation of the Snake Lemma 2.5.2. $\square$

PROPOSITION 3.5.9. *Let S be a flat commutative R-algebra and A an R-algebra. Let M be a finitely presented A-module and N any A-module. The natural map*

$$S \otimes_R \operatorname{Hom}_A(M,N) \xrightarrow{\alpha} \operatorname{Hom}_{S \otimes_R A}(S \otimes_R M, S \otimes_R N)$$

is an isomorphism of S-modules.

PROOF. Is left to the reader. $\square$

EXAMPLE 3.5.10. We show by example that Proposition 3.5.8 is false without the finitely generated hypothesis on M. Let $R = \mathbb{Z}$ and $S = \mathbb{Q}$. Let $M = \bigoplus_{i=1}^{\infty} \mathbb{Z}$ be the free abelian group on $\mathbb{N}$ and $N = \mathbb{Q}/\mathbb{Z}$. By Lemma 3.1.7, S is a flat R-algebra. By Exercise 2.3.20, $S \otimes_R N = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = (0)$. Therefore,

$$\prod_{i=1}^{\infty} (S \otimes_R N) = \prod_{i=1}^{\infty} (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}) = (0).$$

Let $\gamma : \mathbb{N} \to \mathbb{Q}/\mathbb{Z}$ be defined by $i \mapsto 1/2^i + \mathbb{Z}$. For any $n > 1$, if i is chosen so that $2^i > n$, then $n/2^i + \mathbb{Z} \neq 0 + \mathbb{Z}$. Therefore, γ is an element of infinite order in $\prod_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z}$. There is an exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\ell_\gamma} \prod_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z}$$

where ℓ_γ is defined by $1 \mapsto \gamma$. Tensoring with $S = \mathbb{Q}$,

$$0 \to \mathbb{Q} \xrightarrow{1\otimes \ell_\gamma} \mathbb{Q} \otimes_{\mathbb{Z}} \left(\prod_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z} \right)$$

is exact, so the group $\mathbb{Q} \otimes_{\mathbb{Z}} (\prod_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z})$ is non-trivial. However, its image under the natural map

$$\mathbb{Q} \otimes_{\mathbb{Z}} \left(\prod_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z} \right) \to \prod_{i=1}^{\infty} (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z})$$

is the trivial group (0). In particular, this shows tensoring does not distribute across an infinite direct product. We also have

$$\begin{aligned} S \otimes_R \operatorname{Hom}_R(M,N) &= \mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}} \left(\bigoplus_{i=1}^{\infty} \mathbb{Z}, \mathbb{Q}/\mathbb{Z} \right) \\ &= \mathbb{Q} \otimes_{\mathbb{Z}} \left(\prod_{i=1}^{\infty} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \right) \\ &= \mathbb{Q} \otimes_{\mathbb{Z}} \left(\prod_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z} \right) \end{aligned}$$

is a non-trivial group. Since

$$\operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) = \operatorname{Hom}_{\mathbb{Q}} \left(\mathbb{Q} \otimes_{\mathbb{Z}} \bigoplus_{i=1}^{\infty} \mathbb{Z}, \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \right) = (0)$$

is the trivial group, this shows the natural map α of Proposition 3.5.8 is not one-to-one.

For another proof of Proposition 3.5.11, see Proposition 3.7.9.

PROPOSITION 3.5.11. *Let S be a commutative flat R-algebra and M a finitely generated R-module. Then* $\operatorname{annih}_S(S \otimes_R M) = S \operatorname{annih}_R(M)$. *In particular, if M is a faithful R-module, then $S \otimes_R M$ is a faithful S-module.*

PROOF. By Lemma 1.1.10,

$$0 \to \operatorname{annih}_R(M) \to R \xrightarrow{\theta_R} \operatorname{Hom}_R(M,M) \tag{5.11}$$

is an exact sequence of R-modules. Likewise,

$$0 \to \operatorname{annih}_S(S \otimes_R M) \to S \xrightarrow{\theta_S} \operatorname{Hom}_S(S \otimes_R M, S \otimes_R M) \tag{5.12}$$

is an exact sequence of S-modules. Since S is a flat R-module,

$$0 \to S \otimes_R \operatorname{annih}_R(M) \xrightarrow{1\otimes\theta_R} S \otimes_R \operatorname{Hom}_R(M,M) \tag{5.13}$$

is an exact sequence of S-modules. Since θ_S factors through $1 \otimes \theta_R$ and the natural monomorphism α of Proposition 3.5.8, the kernel of θ_S is equal to the kernel of $1 \otimes \theta_R$. This follows from Theorem 2.5.3, or by direct observation. Thus $S \operatorname{annih}_R(M) = \operatorname{annih}_S(S \otimes_R M)$. □

5.4. Faithfully Flat Base Change.

LEMMA 3.5.12. *Let S be a commutative faithfully flat R-algebra and M an R-module.*

(1) M is finitely generated over R if and only if $S\otimes_R M$ is finitely generated over S.
(2) M is of finite presentation over R if and only if $S\otimes_R M$ is of finite presentation over S.
(3) M is finitely generated projective over R if and only if $S\otimes_R M$ is finitely generated projective over S.
(4) M is flat over R if and only if $S\otimes_R M$ is flat over S.
(5) M is faithfully flat over R if and only if $S\otimes_R M$ is faithfully flat over S.
(6) If M is an R-generator, then $S\otimes_R M$ is an S-generator. If M is a finitely presented R-module and $S\otimes_R M$ is an S-generator, then M is an R-generator.
(7) If $S\otimes_R M$ is faithful over S, then M is faithful over R.

PROOF. (1): If M is finitely generated, then Theorem 2.3.23 (4) shows $S\otimes_R M$ is finitely generated. Conversely, choose generators $\{t_1,\dots,t_m\}$ for $S\otimes_R M$. After breaking up summations and factoring out elements of S, we can assume each t_i looks like $1\otimes x_i$ where $x_i\in M$. Consider the sequence

$$R^{(n)}\to M\to 0 \tag{5.14}$$

which is defined by $(r_1,\dots,r_n)\mapsto \sum r_i x_i$. Tensoring (5.14) with S gives the sequence

$$S^{(n)}\to S\otimes_R M\to 0$$

which is exact. Since S is faithfully flat, (5.14) is exact.

(2): Assume M is finitely presented. Suppose $R^{(n)}\to R^{(n)}\to M\to 0$ is exact. Tensoring is right exact, so $S^{(n)}\to S^{(n)}\to S\otimes_R M\to 0$ is exact. Therefore $S\otimes_R M$ is finitely presented. Conversely assume $S\otimes_R M$ is finitely presented. By Part (1) M is finitely generated over R. Suppose $\phi: R^{(n)}\to M$ is onto. Let $N=\ker\phi$. It is enough to show that N is finitely generated. Since

$$0\to N\to R^{(n)}\xrightarrow{\phi} M\to 0$$

is exact and S is faithfully flat,

$$0\to S\otimes_R N\to S^{(n)}\xrightarrow{1\otimes\phi} S\otimes_R M\to 0$$

is exact. By Lemma 3.1.13 (3), $S\otimes_R N$ is finitely generated over S. Part (1) says that N is finitely generated over R.

(3): If M is finitely generated and projective over R, then Theorem 2.3.23 says the same holds for $S\otimes_R M$ over S. Conversely, suppose $S\otimes_R M$ is finitely generated and projective over S. By Corollary 2.1.8, $S\otimes_R M$ is of finite presentation over S. By Part (2), M is of finite presentation over R. To show that M is R-projective, by Proposition 2.4.5 (2) it is enough to show $\operatorname{Hom}_R(M,\cdot)$ is a right exact functor. Start with an exact sequence

$$A\xrightarrow{\alpha} B\to 0 \tag{5.15}$$

of R-modules. It is enough to show

$$\operatorname{Hom}_R(M,A)\xrightarrow{\mathrm{H}_\alpha}\operatorname{Hom}_R(M,B)\to 0 \tag{5.16}$$

is exact. Since S is faithfully flat over R, it is enough to show

$$S\otimes_R\operatorname{Hom}_R(M,A)\xrightarrow{1\otimes\mathrm{H}_\alpha} S\otimes_R\operatorname{Hom}_R(M,B)\to 0 \tag{5.17}$$

is exact. Tensoring is right exact, so tensoring (5.15) with $S \otimes_R (\cdot)$ gives the exact sequence

$$S \otimes_R A \xrightarrow{1 \otimes \alpha} S \otimes_R B \to 0. \tag{5.18}$$

Since we are assuming $S \otimes_R M$ is S-projective, by Proposition 2.4.5 (2) we can apply the functor $\operatorname{Hom}_S(S \otimes_R M, \cdot)$ to (5.18) yielding

$$\operatorname{Hom}_S(S \otimes_R M, S \otimes_R A) \xrightarrow{\mathrm{H}_{1\otimes\alpha}} \operatorname{Hom}_S(S \otimes_R M, S \otimes_R B) \to 0 \tag{5.19}$$

which is exact. Combine (5.17) and (5.19) to get the commutative diagram

$$\begin{tikzcd}
S \otimes_R \operatorname{Hom}_R(M,A) \arrow[r, "1\otimes \mathrm{H}_\alpha"] \arrow[d, "\cong"] & S \otimes_R \operatorname{Hom}_R(M,B) \arrow[d, "\cong"] & \\
\operatorname{Hom}_S(S \otimes_R M, S \otimes_R A) \arrow[r, "\mathrm{H}_{1\otimes\alpha}"] & \operatorname{Hom}_S(S \otimes_R M, S \otimes_R B) \arrow[r] & 0
\end{tikzcd}$$

where the vertical maps are the natural maps from Proposition 3.5.8. Since the bottom row is exact and the vertical maps are isomorphisms, it follows that $1 \otimes \mathrm{H}_\alpha$ is onto.

(4): Assume $M \otimes_R S$ is a flat S-module. By Exercise 3.5.9, $M \otimes_R S$ is flat over R. Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of R-modules. Then

$$0 \to A \otimes_R M \otimes_R S \to B \otimes_R M \otimes_R S \to C \otimes_R M \otimes_R S \to 0$$

is an exact sequence of R-modules. Since S is faithfully flat over R,

$$0 \to A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

is an exact sequence of R-modules.

(6): Assume M is a finitely presented R-module and $S \otimes_R M$ is an S-generator. To show M is an R-generator, we apply Exercise 2.4.1. Suppose $f : A \to B$ is a nonzero homomorphism of R-modules. We show that there exists an R-module homomorphism $\beta : M \to A$ such that $f\beta : M \to B$ is nonzero. Since S is faithfully flat over R, $1 \otimes f : S \otimes_R A \to S \otimes_R B$ is nonzero. Since $S \otimes_R M$ is an S-generator, there exists $h : S \otimes_R M \to S \otimes_R A$ such that $(1 \otimes f)h : S \otimes_R M \to S \otimes_R B$ is nonzero. By Proposition 3.5.8, $\alpha : S \otimes_R \operatorname{Hom}_R(M,A) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R A)$ is an isomorphism. So there exist $s_1, \dots, s_m$ in S and $h_1, \dots, h_m$ in $\operatorname{Hom}_R(M,A)$ such that $h = \alpha(\sum_{i=1}^m s_i \otimes h_i)$. Hence there exists $x \in A$ and some $1 \le i \le m$ such that $f h_i(x) \neq 0$. Therefore β exists.

(7): Let $\theta_R : R \to \operatorname{Hom}_R(M,M)$ be the homomorphism of Lemma 1.1.10. We also have $\theta_S : S \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R M)$, and the diagram

$$\begin{tikzcd}
S \arrow[rr, "\theta_S"] \arrow[dr, "1\otimes\theta_R"'] & & \operatorname{Hom}_S(S \otimes_R M, S \otimes_R M) \\
& S \otimes_R \operatorname{Hom}_R(M,M) \arrow[ur, "\alpha"'] &
\end{tikzcd}$$

commutes, where α is the homomorphism of Proposition 3.5.8. By assumption, θ_S is one-to-one. Therefore, $1 \otimes \theta_R$ is one-to-one. Since S is faithfully flat over R, θ_R is one-to-one.

(5): Is left to the reader. $\square$

5.5. Faithfully Flat Descent of Central Algebras.

DEFINITION 3.5.13. Let R be a commutative ring and A an R-algebra. If the structure homomorphism $R \to Z(A)$ from R to the center of A is an isomorphism, then we say A is a *central* R-algebra.

PROPOSITION 3.5.14. *Let R be a commutative ring. Let A be an R-algebra and S a commutative faithfully flat R-algebra. If $A \otimes_R S$ is a central S-algebra, then A is a central R-algebra.*

PROOF. Assume $A \otimes_R S$ is a central S-algebra. Since S is flat over R, $Z(A) \otimes_R S \to A \otimes_R S$ is one-to-one. By hypothesis, the composite map

$$R \otimes_R S \to Z(A) \otimes_R S \to Z(A \otimes_R S)$$

is an isomorphism. Since S is faithfully flat over R, $R \to Z(A)$ is an isomorphism. $\square$

PROPOSITION 3.5.15. *Let R be a commutative ring and A an R-algebra. If $A_{\mathfrak{m}} = A \otimes_R R_{\mathfrak{m}}$ is a central $R_{\mathfrak{m}}$-algebra for every maximal ideal $\mathfrak{m}$ of R, then A is a central R-algebra.*

PROOF. Let $\mathfrak{m}$ be a maximal ideal of R. Since $R_{\mathfrak{m}}$ is a flat R-module, $Z(A) \otimes_R R_{\mathfrak{m}} \to A_{\mathfrak{m}}$ is one-to-one. Clearly, $Z(A) \otimes_R R_{\mathfrak{m}} \subseteq Z(A_{\mathfrak{m}})$. We are given that the composite map

$$R_{\mathfrak{m}} \to Z(A) \otimes_R R_{\mathfrak{m}} \subseteq Z(A_{\mathfrak{m}})$$

is an isomorphism. Therefore, $R_{\mathfrak{m}} \to Z(A) \otimes_R R_{\mathfrak{m}}$ is an isomorphism. By Exercise 3.5.1, $R \to Z(A)$ is an isomorphism. $\square$

5.6. Exercises.

EXERCISE 3.5.1. Let R be a commutative ring, let M and N be R-modules, and $f \in \operatorname{Hom}_R(M,N)$. For any prime ideal $P \in \operatorname{Spec} R$ there is the R_P-module homomorphism $f_P : M_P \to N_P$ obtained by "localizing at P".

1. Prove that the following are equivalent.
   - (a) f is one-to-one.
   - (b) f_P is one-to-one for all $P \in \operatorname{Spec} R$.
   - (c) $f_{\mathfrak{m}}$ is one-to-one for all $\mathfrak{m} \in \operatorname{Max} R$.
2. Prove that the following are equivalent.
   - (a) f is onto.
   - (b) f_P is onto for all $P \in \operatorname{Spec} R$.
   - (c) $f_{\mathfrak{m}}$ is onto for all $\mathfrak{m} \in \operatorname{Max} R$.

EXERCISE 3.5.2. Let R be a commutative ring. Let M and N be finitely generated and projective R-modules of constant rank and assume $\operatorname{Rank}_R(M) = \operatorname{Rank}_R(N)$. Let $f \in \operatorname{Hom}_R(M,N)$. Show that if f is onto, then f is one-to-one.

EXERCISE 3.5.3. (Faithfully Flat Is Preserved under a Change of Base) If A is a commutative R-algebra and M is a faithfully flat R-module, show that $A \otimes_R M$ is a faithfully flat A-module.

EXERCISE 3.5.4. Let R be a ring and $\{M_i \mid i \in I\}$ a set of right R-modules. Prove that the direct sum $\bigoplus_{i \in I} M_i$ is a flat R-module if and only if each M_i is a flat R-module.

EXERCISE 3.5.5. Let R be a ring. Let M and N be right R-modules. If M is a flat R-module and N is a faithfully flat R-module, show that $M \oplus N$ is a faithfully flat R-module.

EXERCISE 3.5.6. State and prove a version of Lemma 3.5.1 for a ring R which is not necessarily commutative.

EXERCISE 3.5.7. Let R be a ring. Show that R is a faithfully flat R-module. Show that a free R-module is faithfully flat.

EXERCISE 3.5.8. Let R be a ring and $S = R[x]$ the polynomial ring which can be viewed as a left R-module. Prove:

(1) S is a free R-module.
(2) S is a faithfully flat R-module.
(3) The exact sequence $0 \to R \to S$ of R-modules is split. That is, $R \cdot 1$ is an R-module direct summand of S.

EXERCISE 3.5.9. (Flat over Flat Is Flat) Let $\theta : R \to A$ be a homomorphism of rings and M a left A-module. Using θ, view A as a left R-right A-bimodule and M as a left R-module. Show that if A is a flat R-module, and M is a flat A-module, then M is a flat R-module.

EXERCISE 3.5.10. (Faithfully Flat over Faithfully Flat Is Faithfully Flat) If A is a commutative faithfully flat R-algebra and M a faithfully flat A-module, show that M is a faithfully flat R-module.

EXERCISE 3.5.11. Let R be a ring, $M \in {}_R\mathfrak{M}_R$ and $N \in {}_R\mathfrak{M}$. Prove:

(1) If M and N are flat left R-modules, then $M \otimes_R N$ is a flat left R-module.
(2) Assume R is commutative. If M and N are faithfully flat R-modules, then $M \otimes_R N$ is a faithfully flat R-module.

EXERCISE 3.5.12. Let $\theta : R \to S$ be a local homomorphism of local rings (see Exercise 1.1.11). If S is a flat R-algebra, show that S is faithfully flat.

EXERCISE 3.5.13. Let R be a commutative ring. Assume $f_1, \dots, f_n$ are elements of $R - (0)$. Let $S = R_{f_1} \oplus \cdots \oplus R_{f_n}$ be the direct sum. Let $\theta : R \to S$ be defined by $\theta(x) = (x/1, \dots, x/1)$. Prove that the following are equivalent.

(1) $f_1, \dots, f_n$ generate the unit ideal of R. That is, $R = Rf_1 + \cdots + Rf_n$.
(2) S is a faithfully flat R-algebra.

EXERCISE 3.5.14. Let R be a commutative ring and $\{\alpha_i \mid i \in I\}$ a subset of $R - (0)$. Let $S = \prod_{i \in I} R[\alpha_i^{-1}]$. Then S is an R-algebra, where the structure homomorphism is the unique map $R \to S$ of Exercise 1.6.14 which commutes with each natural map $R \to R[\alpha_i^{-1}]$. Prove that the following are equivalent.

(1) S is a faithfully flat R-algebra.
(2) There exists a finite subset $\{i_1, \dots, i_n\} \subseteq I$ such that $R[\alpha_{i_1}^{-1}] \bigoplus \cdots \bigoplus R[\alpha_{i_n}^{-1}]$ is faithfully flat over R.
(3) There exists a finite subset $\{i_1, \dots, i_n\} \subseteq I$ such that $R = R\alpha_{i_1} + \cdots + R\alpha_{i_n}$.

EXERCISE 3.5.15. Let $R = \mathbb{Z}$ be the ring of integers and $S = \mathbb{Z}[2^{-1}]$ the localization of R obtained by inverting 2. Prove:

(1) S is not a projective R-module. (See Exercise 2.2.7.)
(2) S is a flat R-module.
(3) S is not a finitely generated R-module.
(4) S is not a faithfully flat R-module.
(5) The exact sequence $0 \to R \to S$ is not split exact. That is, $R \cdot 1$ is not a direct summand of S.

EXERCISE 3.5.16. Let R be a commutative ring and I an ideal of R which is contained in the nil radical of R. Show that R/I is a flat R-algebra if and only if $I = (0)$.

EXERCISE 3.5.17. Let R be a commutative ring and $W \subseteq R$ a multiplicative set. Show that $W^{-1}R$ is a faithfully flat R-algebra if and only if $W \subseteq \operatorname{Units}(R)$.

EXERCISE 3.5.18. Let $f : R \to S$ be a homomorphism of commutative rings and $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 3.3.3. Assume

(a) $f^\sharp$ is one-to-one,
(b) the image of $f^\sharp$ is an open subset of $\operatorname{Spec} R$, and
(c) for every $\mathfrak{q} \in \operatorname{Spec} S$, if $\mathfrak{p} = \mathfrak{q} \cap R$, then the natural map $R_\mathfrak{p} \to S_\mathfrak{q}$ is an isomorphism.

If (a), (b) and (c) are satisfied, then we say $f^\sharp$ is an *open immersion*. Under these hypotheses, prove the following.

(1) For every $\mathfrak{q} \in \operatorname{Spec} S$, if $\mathfrak{p} = \mathfrak{q} \cap R$, then $S \otimes_R R_\mathfrak{p}$ is isomorphic to $S_\mathfrak{q}$.
(2) If $\alpha \in R$ and $U(\alpha)$ is a nonempty basic open subset of the image of $f^\sharp$, then $R[\alpha^{-1}]$ is isomorphic to $S \otimes_R R[\alpha^{-1}]$.

EXERCISE 3.5.19. Let $f : R \to S$ be a homomorphism of commutative rings. Show that f is an isomorphism of rings if and only if

(a) $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is a homeomorphism and
(b) for every $\mathfrak{q} \in \operatorname{Spec} S$, if $\mathfrak{p} = \mathfrak{q} \cap R$, then the natural map $R_\mathfrak{p} \to S_\mathfrak{q}$ is an isomorphism.

EXERCISE 3.5.20. Let $f : R \to S$ be a homomorphism of commutative rings. In each of the following, give a specific example to show that f is not an isomorphism if either condition (a) or (b) of Exercise 3.5.19 is not satisfied.

(1) Give an example such that condition (a) is satisfied, condition (b) is not satisfied, and f is not an isomorphism.
(2) Give an example such that $f^\sharp$ is one-to-one, condition (b) is satisfied, and f is not an isomorphism.
(3) Give an example such that $f^\sharp$ is onto, condition (b) is satisfied, and f is not an isomorphism.

5.7. Locally of Finite Type is Finitely Generated as an Algebra. If S is a commutative R-algebra, then S is said to be *locally of finite type* in case there exist elements $f_1, \dots, f_n$ in S such that $S = Sf_1 + \cdots + Sf_n$ and for each i, $S[f_i^{-1}]$ is a finitely generated R-algebra. Proposition 3.5.16 is from [**45**, Proposition 1, p. 87].

PROPOSITION 3.5.16. *Let S be a commutative R-algebra. Then S is locally of finite type if and only if S is a finitely generated R-algebra.*

PROOF. Assume S is locally of finite type and prove that S is finitely generated as an R-algebra. The converse is trivial. We are given $f_1, \dots, f_n$ in S such that $S = Sf_1 + \cdots + Sf_n$ and for each i, $S[f_i^{-1}]$ is a finitely generated R-algebra. Fix elements $u_1, \dots, u_n$ in S such that $1 = u_1 f_1 + \cdots + u_n f_n$. Fix elements $y_{i1}, \dots, y_{im}$ in $S[f_i^{-1}]$ such that $S[f_i^{-1}] = R[y_{i1}, \dots, y_{im}]$. There exist elements s_{ij} in S and nonnegative integers e_i such that $y_{ij} = s_{ij} f_i^{-e_i}$ in $S[f_i^{-1}]$. Let S_1 be the finitely generated R-subalgebra of S generated by the finite set of elements $\{s_{ij}\} \cup \{f_1, \dots, f_n\} \cup \{u_1, \dots, u_n\}$. To finish, it is enough to show that S_1 is equal to S. Let α be an arbitrary element of S and let $1 \le i \le n$. Consider $\alpha/1$ as an element of $S[f_i^{-1}]$. Since $S[f_i^{-1}]$ is generated over R by $s_{i1}, \dots, s_{im}$ and f_i^{-1}, there exists an element

β_i in S_1 such that $\alpha/1 = \beta_i f_i^{-k_i}$ for some $k_i \geq 0$. For some $\ell_i \geq 0$, $f_i^{\ell_i}(\beta_i - f_i^{k_i}\alpha) = 0$ in S. For some large integer L, $f_i^L \alpha = f_i^{L-k_i}\beta_i$ is an element of S_1, for each i. For any positive integer N, $\alpha = 1\alpha = (u_1 f_1 + \cdots + u_n f_n)^N \alpha$. By the multinomial expansion, when N is sufficiently large, $(u_1 f_1 + \cdots + u_n f_n)^N$ is in the ideal $S_1 f_1^L + \cdots + S_1 f_n^L$. Therefore, α is in S_1. □

COROLLARY 3.5.17. *Let $f : R \to S$ be a homomorphism of commutative rings. If $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is an open immersion (see Exercise 3.5.18), then S is a finitely generated R-algebra.*

PROOF. Is left to the reader. □

COROLLARY 3.5.18. *Let R be a commutative semilocal ring. If $\mathfrak{m} \in \operatorname{Max} R$, then $R_\mathfrak{m}$ is a finitely generated R-algebra. The map $\operatorname{Spec} R_\mathfrak{m} \to \operatorname{Spec} R$ is an open immersion.*

PROOF. If $\operatorname{Max} R = \{\mathfrak{m}\}$, then $R_\mathfrak{m} = R$ and there is nothing to prove. Assume $n \geq 1$ and $\operatorname{Max} R = \{\mathfrak{m}, \mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$. For $i = 1, \ldots, n$ pick $\alpha_i \in \mathfrak{m}_i - \mathfrak{m}$. Set $\alpha = \alpha_1 \cdots \alpha_n$. Then $\alpha \in \mathfrak{m}_i - \mathfrak{m}$ for each i. Let $R[\alpha^{-1}]$ be the R-algebra formed by inverting α. Let $\theta : R \to R[\alpha^{-1}]$. By Exercise 3.3.9, the image of $\theta^\sharp : \operatorname{Spec} R[\alpha^{-1}] \to \operatorname{Spec} R$ consists of those prime ideals of R that do not contain α. So $\operatorname{Max}(R[\alpha^{-1}]) = \{\mathfrak{m}\}$. By Exercise 3.1.10, $R_\mathfrak{m} = R[\alpha^{-1}] \otimes_R R_\mathfrak{m}$. By Exercise 3.5.1, the natural map $\phi : R[\alpha^{-1}] \to R_\mathfrak{m}$ is an isomorphism. By Exercise 3.1.18, $R[\alpha^{-1}]$ is a finitely generated R-algebra. Since $\operatorname{Spec} R[\alpha^{-1}] \to \operatorname{Spec} R$ is an open immersion, this also shows $\operatorname{Spec} R_\mathfrak{m} \to \operatorname{Spec} R$ is an open immersion. □

6. Locally Free Modules

In this section we study finitely generated projective modules over commutative rings from a local point of view. An R-module is said to be locally free of finite rank if there exist $f_1, \ldots, f_n$ in R such that $R = Rf_1 + \cdots + R_n$ and for each i, the localization M_{f_i} is a free R_{f_i}-module of finite rank. If $U_(f_i)$ denotes the image of the natural map $\operatorname{Spec} R_{f_i} \to SpecR$, then $\{U(f_i)\}$ is an open cover of $\operatorname{Spec} R$. The first main result of this section (Proposition 3.6.2) shows that an R-module M is locally free of finite rank if and only if M is finitely generated and projective. An important corollary shows that if M is a finitely generated R-module, where R is an integral domain with quotient field K, then M is an R-progenerator if and only if for every maximal ideal $\mathfrak{m}$ in $\operatorname{Max} R$, the dimension of the vector space $M/\mathfrak{m}M$ over the field $R/\mathfrak{m}$ is equal to the dimension of the vector space $M \otimes_R K$ over K.

The set of isomorphism classes of finitely generated projective R-modules of constant rank one is called the Picard group of R, and is denoted $\operatorname{Pic}(R)$. We show that under tensor product, $\operatorname{Pic}(R)$ is an abelian group and $R \mapsto \operatorname{Pic}(R)$ defines a covariant functor from the category of commutative rings to the category of abelian groups. In Section 12.2, the Picard group of an integral domain R with quotient field K is described in terms of invertible fractional ideals.

6.1. Locally Free of Finite Rank Equals Finitely Generated Projective.

DEFINITION 3.6.1. Let R be a commutative ring and M an R-module. Then M is *locally free of finite rank* if there exist elements $f_1, \ldots, f_n$ in R such that $R = Rf_1 + \cdots + Rf_n$ and for each i, $M_{f_i} = M \otimes_R R_{f_i}$ is free of finite rank over R_{f_i}.

PROPOSITION 3.6.2. *Let R be a commutative ring and M an R-module. The following are equivalent.*

(1) M is finitely generated projective.

(2) *M is locally free of finite rank.*
(3) *M is an R-module of finite presentation and for each* $\mathfrak{p} \in \operatorname{Spec} R$*,* $M_{\mathfrak{p}}$ *is a free* $R_{\mathfrak{p}}$*-module.*
(4) *M is an R-module of finite presentation and for each* $\mathfrak{m} \in \operatorname{Max} R$*,* $M_{\mathfrak{m}}$ *is a free* $R_{\mathfrak{m}}$*-module.*

PROOF. (1) implies (3): This part follows directly from Corollary 2.1.8 and Proposition 3.4.2. It is trivial that (3) implies (4).

(4) implies (2): Using Lemma 3.1.14, for each $\mathfrak{m} \in \operatorname{Max} R$ pick $\alpha_{\mathfrak{m}} \in R - \mathfrak{m}$ such that $M_{\alpha_{\mathfrak{m}}} = M \otimes_R R_{\alpha_{\mathfrak{m}}}$ is free of finite rank over $R_{\alpha_{\mathfrak{m}}}$. Let $U(\alpha_{\mathfrak{m}}) = \operatorname{Spec} R - V(\alpha_{\mathfrak{m}})$ be the basic open set associated to $\alpha_{\mathfrak{m}}$. Since $U(\alpha_{\mathfrak{m}})$ is an open neighborhood of $\mathfrak{m}$, we have an open cover $\{U(\alpha_{\mathfrak{m}}) \mid \mathfrak{m} \in \operatorname{Max} R\}$ of $\operatorname{Spec} R$ (Exercise 3.3.1). By Exercise 3.3.12, there is a finite subset of $\{\alpha_{\mathfrak{m}} \mid \mathfrak{m} \in \operatorname{Max} R\}$, say $\{\alpha_1, \dots, \alpha_n\}$ such that $\{U(\alpha_1), \dots, U(\alpha_n)\}$ is an open cover of $\operatorname{Spec} R$. For each i, M_{α_i} is free of finite rank over R_{α_i} which proves M is locally free of finite rank.

(2) implies (1): Assume $\{U(f_1), \dots, U(f_n)\}$ is an open cover of $\operatorname{Spec} R$ and that for each i, M_{f_i} is free of rank N_i over R_{f_i}. Let $N = \max\{N_1, \dots, N_n\}$. Then

$$F_i = M_{f_i} \oplus R_{f_i}^{(N-N_i)}$$

is free of rank N over R_{f_i}. Set $S = \bigoplus_i R_{f_i}$. Then $R \to S$ is faithfully flat (Exercise 3.5.13). Set $F = \bigoplus_i F_i$. Then F is free over S of rank N and $M \otimes_R S = \bigoplus_i M_{f_i}$ is a direct summand of F (Exercise 3.6.1). Now apply Lemma 3.5.12 (3). □

Let R be a commutative ring. For any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$, write $k_{\mathfrak{p}}$ for the residue field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. If M is a finitely generated R-module, then M can be used to define a rank function $\operatorname{Spec} R \to \{0, 1, 2, \dots\}$, where $\mathfrak{p} \mapsto \dim_{k_{\mathfrak{p}}}(M \otimes_R k_{\mathfrak{p}})$. The next two corollaries to Proposition 3.6.2 utilize this rank function to give us a powerful test for locally free modules and for flatness over an integral domain.

COROLLARY 3.6.3. *Let R be an integral domain with quotient field K. For each maximal ideal* $\mathfrak{m} \in \operatorname{Max}(R)$*, write* $k_{\mathfrak{m}}$ *for* $R/\mathfrak{m}$*. The following are equivalent for any finitely generated R-module M.*

(1) *M is a locally free R-module of constant rank n.*
(2) $\dim_K(M \otimes_R K) = n$ *and for every* $\mathfrak{m} \in \operatorname{Max}(R)$*,* $\dim_{k_{\mathfrak{m}}}(M/\mathfrak{m}M) = n$*.*

PROOF. (1) implies (2): If $M \cong R^{(n)}$, then $M \otimes_R k_{\mathfrak{m}} \cong k_{\mathfrak{m}}^{(n)}$ and $M \otimes_R K \cong K^{(n)}$.

(2) implies (1): Let $\mathfrak{m}$ be a maximal ideal of R and write $M_{\mathfrak{m}}$ for $M \otimes_R R_{\mathfrak{m}}$. Since $M/\mathfrak{m}M$ is free of dimension n over $k_{\mathfrak{m}}$, there exist $x_1, \dots, x_n$ in $M_{\mathfrak{m}}$ which restrict to a $k_{\mathfrak{m}}$-basis under the natural map $M_{\mathfrak{m}} \to M/\mathfrak{m}M$. For some $\alpha \in R - \mathfrak{m}$, the finite set $x_1, \dots, x_n$ is in the image of the natural map $M_\alpha \to M_{\mathfrak{m}}$. Define $\theta : R_\alpha^{(n)} \to M_\alpha$ by mapping the standard basis vector e_i to x_i. By Lemma 3.4.1, $M_{\mathfrak{m}}$ is generated by $x_1, \dots, x_n$ as an $R_{\mathfrak{m}}$-module. Therefore, upon localizing θ at the maximal ideal $\mathfrak{m}R_\alpha$, it becomes onto. Because the cokernel of θ is a finitely generated R_α-module, by Lemma 3.1.11, there exists $\beta \in R_\alpha - \mathfrak{m}R_\alpha$ such that if we replace α with $\alpha\beta$, then θ is onto. The diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker\theta \arrow[r] \arrow[d, "\alpha"] & R_\alpha^{(n)} \arrow[r, "\theta"] \arrow[d, "\beta"] & M_\alpha \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker\theta \otimes_R K \arrow[r] & K^{(n)} \arrow[r, "\theta\otimes 1"] & M \otimes_R K \arrow[r] & 0
\end{tikzcd}$$

commutes, where the second row is obtained by tensoring the top row with $(\ )\otimes_R K$. Since the top row is exact, by Lemma 3.1.7 so is the second row. Since R is an integral domain, $R \to K$ is one-to-one. Therefore β is one-to-one. Since $M \otimes K$ has dimension n and $\theta \otimes 1$ is onto, it follows that $\ker \theta \otimes_R K = 0$. The Snake Lemma implies that $\ker \theta = 0$. We have shown that every maximal ideal $\mathfrak{m} \in \operatorname{Max}(R)$ has a basic open neighborhood $U(\alpha)$ such that M_α is a free R_α-module of rank n. The argument that was used to show (4) implies (2) in Proposition 3.6.2 can now be applied to finish the proof. □

COROLLARY 3.6.4. *Let R be an integral domain with quotient field K and M a finitely generated R-module. Then the following are equivalent.*

(1) M is of finite presentation and flat.
(2) M is an R-progenerator.
(3) There exists $n > 0$ such that $\dim_K(M \otimes_R K) = n$ and for every maximal ideal $\mathfrak{m}$ in $\operatorname{Max}(R)$, $\dim_{k_\mathfrak{m}}(M/\mathfrak{m}M) = n$.

PROOF. By Theorem 2.6.19 and Corollary 2.2.4, (1) and (2) are equivalent. Proposition 3.6.2, Corollary 3.6.3, and Corollary 2.2.4 imply that (2) and (3) are equivalent. □

6.2. Invertible Modules and the Picard Group. In this short section we define an important invariant of a commutative ring. Given a commutative ring R, the Picard group of R, denoted $\operatorname{Pic}(R)$, parametrizes the isomorphism classes of projective R-modules of constant rank one. Under tensor product, $\operatorname{Pic}(R)$ is an abelian group, and $R \mapsto \operatorname{Pic}(R)$ is a covariant functor from the category of commutative rings to the category of abelian groups.

LEMMA 3.6.5. *Let M be a finitely generated projective faithful module over the commutative ring R. Then the following are equivalent.*

(1) $\operatorname{Rank}_R(M) = 1$.
(2) $\operatorname{Rank}_R(M^*) = 1$.
(3) $\operatorname{Hom}_R(M,M) \cong R$.
(4) $M^* \otimes_R M \cong R$.

PROOF. The hypotheses on M imply that M is an R-progenerator module. Fix a prime $P \in \operatorname{Spec} R$. Then $M_P \cong R_P^{(m)}$ for some positive integer m. By Corollary 2.4.13 and Exercise 3.4.1, $M^* \otimes_R R_P = \operatorname{Hom}_R(M,R) \otimes_R R_P \cong \operatorname{Hom}_{R_P}(M_P,R_P)$ is isomorphic to $R_P^{(m)}$. Likewise, $R_P \otimes_R \operatorname{Hom}_{R_P}(M,M) \cong \operatorname{Hom}_{R_P}(M_P,M_P)$ is isomorphic to $R_P^{(m^2)}$. By properties of tensors and Exercise 3.4.1, $R_P \otimes_R M^* \otimes_R M \cong (R_P \otimes_R M^*) \otimes_{R_P} M_P$ is isomorphic to $R_P^{(m^2)}$. From this it follows that (1) – (4) are equivalent for the prime P. Since P was arbitrary, this proves the lemma. □

DEFINITION 3.6.6. If M is an R-module that satisfies any of the equivalent properties of Lemma 3.6.5, then we say M is *invertible*. Given a commutative ring R let $\operatorname{Pic}(R)$ be the set of isomorphism classes of invertible R-modules. The isomorphism class containing a module M is denoted by $|M|$. As stated in Proposition 3.6.8, $\operatorname{Pic}(R)$ is an abelian group, which is called the *Picard group* of R.

PROPOSITION 3.6.7. *Let R be a commutative ring and M an R-module. Then M is invertible if and only if there exists an R-module N such that $M \otimes_R N \cong R$. In this case, $N \cong M^* = \operatorname{Hom}_R(M,R)$.*

PROOF. Assume M is an invertible R-module. By Lemma 3.6.5, if we take N to be M^*, then $M \otimes_R N \cong R$. Conversely, assume $M \otimes_R N \cong R$. By Proposition 2.3.25, both M

and N are R-progenerators. Fix a prime $P \in \operatorname{Spec} R$. Then $M_P \cong R_P^{(m)}$ and $N_P \cong R_P^{(n)}$ for some positive integers m, n. Tensor both sides of $M \otimes_R N \cong R$ with R_P to get $R_P \cong R_P \otimes_R (M \otimes_R N) \cong (M \otimes_R R_P) \otimes_{R_P} (N \otimes_R R_P \cong R_P^{(m)} \otimes_{R_P} R_P^{(n)} \cong R_P^{(mn)}$. It follows that $m = n = 1$. Since P was arbitrary, this shows M has constant rank 1. Tensor both sides of $M \otimes_R N \cong R$ with M^* to get $M^* \cong M^* \otimes_R M \otimes_R N \cong R \otimes_R N \cong N$. $\square$

PROPOSITION 3.6.8. *Under the binary operation* $|P| \cdot |Q| = |P \otimes_R Q|$, $\operatorname{Pic}(R)$ *is an abelian group. The identity element is the class* $|R|$*. The inverse of* $|M| \in \operatorname{Pic}(R)$ *is* $|M^*|$*. The assignment* $R \mapsto \operatorname{Pic}(R)$ *defines a (covariant) functor from the category of commutative rings to the category of abelian groups.*

PROOF. Is left to the reader. $\square$

EXAMPLE 3.6.9. See Exercise 2.2.2. Let k be any field. Let x and y be indeterminates. Let f be the polynomial $f = y^2 - x(x^2 - 1)$. Let R be the factor ring

$$R = \frac{k[x,y]}{(y^2 - x(x^2 - 1))}.$$

Then R is an integral domain. Let M be the maximal ideal of R generated by x and y. If we invert $x^2 - 1$, then $x = y^2(x^2 - 1)^{-1}$, so M becomes principal. If we invert x, then M becomes the unit ideal, and is principal. Since $R(x^2 - 1)$ and $R(x)$ are comaximal, there is an open cover $U(x^2 - 1) \cup U(x) = \operatorname{Spec} R$ on which M is locally free of rank 1. Proposition 3.6.2 shows that $|M| \in \operatorname{Pic} R$. Note that M^2 is generated by x^2, xy, y^2. But an ideal that contains x^2 and y^2 also contains x. We see that M^2 is generated by x, hence is free of rank one. The map

$$\begin{aligned} M \otimes_R M &\to M^2 \\ a \otimes b &\mapsto ab \end{aligned}$$

is R-linear. Since this map is onto and both sides are projective of rank one, it is an isomorphism. This proves that $M^* \cong M$ and $|M|^{-1} = |M|$.

EXAMPLE 3.6.10. If R is a commutative ring with the property that every progenerator module is free, then $\operatorname{Pic}(R)$ contains just one element, namely $|R|$. Using the notation of abelian groups, we usually write $\operatorname{Pic}(R) = (0)$ in this case. For example, $\operatorname{Pic}(R) = (0)$ in each of the following cases.

(1) R is a field (Theorem 1.6.13).
(2) R is a local ring (Proposition 3.4.2).
(3) R is a principal ideal domain (Example 2.1.6).
(4) R is a semilocal ring (Exercise 4.2.5).

6.3. Exercises.

EXERCISE 3.6.1. Let R_1 and R_2 be rings and let $S = R_1 \oplus R_2$ be the direct sum. Let M_1 be an R_1-module and M_2 an R_2-module and let $M = M_1 \oplus M_2$. Prove:

(1) M is an S-module.
(2) If M_i is free of rank N over R_i for each i, then M is free of rank N over S.
(3) If M_i is finitely generated and projective over R_i for each i, then M is finitely generated and projective over S.

EXERCISE 3.6.2. Let R_1 and R_2 be commutative rings. Show that $\operatorname{Pic}(R_1 \oplus R_2)$ is isomorphic to $\operatorname{Pic}(R_1) \oplus \operatorname{Pic}(R_2)$.

EXERCISE 3.6.3. Let R be a commutative ring. A *quadratic extension* of R is an R-algebra S which as an R-module is an R-progenerator of rank two. Prove that a quadratic extension S of R is commutative. (Hint: First prove this when S is free of rank two. For the general case, use the fact that S is locally free of rank two.)

EXERCISE 3.6.4. Let R be a commutative ring and M a finitely generated projective R-module of constant rank n. Show that there exist elements $f_1,\dots,f_m$ of R satisfying the following:

(1) $R = Rf_1 + \cdots + Rf_m$.
(2) If $S = R_{f_1} \oplus \cdots \oplus R_{f_m}$, then $M \otimes_R S$ is a free S-module of rank n.

EXERCISE 3.6.5. Let R be a commutative ring and M an R-progenerator. Prove:

(1) If L is an invertible R-module, then there is an isomorphism of R-algebras
$$\operatorname{Hom}_R(M,M) \cong \operatorname{Hom}_R(M \otimes_R L, M \otimes_R L).$$
(2) If N is an R-progenerator such that $\operatorname{Hom}_R(M,M)$ and $\operatorname{Hom}_R(N,N)$ are isomorphic as R-algebras, then there exists an invertible R-module L such that N and $M \otimes_R L$ are isomorphic as R-modules.

EXERCISE 3.6.6. Let k be a field and $A = k[x]$ the polynomial ring over k in one variable. Let $R = k[x^2,x^3]$ be the k-subalgebra of A generated by x^2 and x^3. In Algebraic Geometry, the ring $k[x^2,x^3]$ corresponds to a cuspidal cubic curve. Show:

(1) R and A have the same quotient field, namely $K = k(x)$.
(2) A is a finitely generated R-module.
(3) The conductor ideal from A to R is $\mathfrak{m} = (x^2,x^3)$ which is a maximal ideal of R (see Exercise 1.1.8).
(4) Use Corollary 3.6.4 to show that A is not flat over R. (Hint: Consider $R/\mathfrak{m}$ and $A/\mathfrak{m}A$.)
(5) The rings $R[x^{-2}]$ and $A[x^{-2}]$ are equal, hence the extension $R \to A$ is flat upon localization to the nonempty basic open set $U(x^2)$.

For a continuation of this example, see Exercise 6.1.7.

EXERCISE 3.6.7. Let k be a field, $n > 1$ an integer, $T = k[x,y]$, $S = k[x^n,xy,y^n]$, and $S \to T$ the set containment map. Using Corollary 3.6.4 and Exercise 2.3.21, show that T is not flat over S. See [**18**, Exercise 4.4.19] for more properties of the extension T/S.

EXERCISE 3.6.8. Let k be a field and $A = k[x]$ the polynomial ring over k in one variable. Let $R = k[x^2-1,x^3-x]$ be the k-subalgebra of A generated by the polynomials x^2-1 and x^3-x. In Algebraic Geometry, the ring $k[x^2-1,x^3-x]$ corresponds to a nodal cubic curve. Show:

(1) The quotient field of $k[x^2-1,x^3-x]$ is $k(x)$. In other words, $k[x^2-1,x^3-x]$ and $k[x]$ are birational.
(2) $k[x^2-1,x^3-x]$ is not a UFD.
(3) A is a finitely generated R-module.
(4) The conductor ideal from A to R is $\mathfrak{m} = (x^2-1,x^3-x)$ which is a maximal ideal of R (see Exercise 1.1.8).
(5) A is not flat over R.
(6) The rings $R[(x^2-1)^{-1}]$ and $A[(x^2-1)^{-1}]$ are equal, hence the extension $R \to A$ is flat upon localization to the nonempty basic open set $U(x^2-1)$.

For a continuation of this example, see Exercise 6.1.9.

7. Flat Modules and Algebras

An R-module M is flat if the functor $M \otimes_R (\cdot)$ is left exact. This section contains a deeper look into the theory of flat modules over a commutative ring R, and algebras over R that are flat as R-modules. First we show that an R-module M is flat if and only if M_P is flat over R_P for every $P \in \operatorname{Spec} R$. Secondly we show that M is flat if and only if the functor $M \otimes_R (\cdot)$ is left exact on every exact sequence $0 \to A \to B$ of finitely generated R-modules. This is called a finiteness criterion for flatness. In Section 7.7.3 we prove that an R-module M is finitely generated and projective if and only if M is of finite presentation and flat. Section 7.7.4 contains some material which will be applied in Section 9.6. We remark that some of the results in this section are proved for modules over a general ring.

7.1. Flat if and only if Locally Flat.

PROPOSITION 3.7.1. *Let R be a commutative ring and A an R-module. The following are equivalent.*

(1) A is a flat R-module.
(2) A_p is a flat R_p-module, for every $p \in \operatorname{Spec} R$.
(3) $A_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module, for every $\mathfrak{m} \in \operatorname{Max} R$.

PROOF. (1) implies (2): This follows from Theorem 2.3.23.
(2) implies (3): This is trivially true.
(3) implies (1): Denote by S the exact sequence

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

of R-modules. Let $\mathfrak{m} \in \operatorname{Max} R$. Because $R_\mathfrak{m}$ is flat over R and $A_\mathfrak{m}$ is flat over $R_\mathfrak{m}$,

$$(S) \otimes_R R_\mathfrak{m} \otimes_{R_\mathfrak{m}} A_\mathfrak{m} = (S) \otimes_R A_\mathfrak{m}$$

is an exact sequence. Take the direct sum over all $\mathfrak{m}$. It follows from Exercise 1.6.8 that

$$(S) \otimes_R \left(\bigoplus_{\mathfrak{m} \in \operatorname{Max} R} A_\mathfrak{m} \right) = (S) \otimes_R A \otimes_R \left(\bigoplus_{\mathfrak{m} \in \operatorname{Max} R} R_\mathfrak{m} \right)$$

is exact. By Proposition 3.5.3,

$$E = \bigoplus_{\mathfrak{m} \in \operatorname{Max} R} R_\mathfrak{m}$$

is a faithfully flat R-module, so $(S) \otimes_R A$ is exact. $\square$

PROPOSITION 3.7.2. *Let $f : R \to S$ be a homomorphism of commutative rings. The following are equivalent.*

(1) S is a flat R-algebra.
(2) $S_\mathfrak{q}$ is a flat $R_\mathfrak{p}$-algebra, for every $\mathfrak{q} \in \operatorname{Spec} S$, if $f^{-1}(\mathfrak{q}) = \mathfrak{p}$.
(3) $S_\mathfrak{m}$ is a flat $R_\mathfrak{p}$-algebra, for every $\mathfrak{m} \in \operatorname{Max} S$, if $f^{-1}(\mathfrak{m}) = \mathfrak{p}$.

PROOF. Is left to the reader. (Hints: For (1) implies (2), use Exercise 3.7.2. For (3) implies (1), there is an isomorphism $(A \otimes_R S) \otimes_S S_\mathfrak{m} \cong (A \otimes_R R_\mathfrak{p}) \otimes_{R_\mathfrak{p}} S_\mathfrak{m}$ for any R-module A.) $\square$

7.2. A Finiteness Criterion for Flat.

PROPOSITION 3.7.3. *Let R be any ring and M a right R-module. Then M is flat if and only if given any exact sequence*

$$0 \to A \to B$$

of finitely generated left R-modules, the sequence

$$0 \to M \otimes_R A \to M \otimes_R B$$

is an exact sequence of $\mathbb{Z}$-modules.

PROOF. If M is flat, the second statement is trivially true. We prove the converse. Start with an exact sequence

$$0 \to A \xrightarrow{\alpha} B$$

of left R-modules. We need to show that

$$0 \to M \otimes_R A \xrightarrow{1\otimes\alpha} M \otimes_R B$$

is exact. We show that if $v = \sum_{i=1}^n x_i \otimes y_i$ is an element in the kernel of $1 \otimes \alpha$, then $v = 0$. Set A_1 equal to $Ry_1 + \cdots + Ry_n$, which is a finitely generated submodule of A. Set B_1 equal to $R\alpha(y_1) + \cdots + R\alpha(y_n)$, which is a finitely generated submodule of B. As in Exercise 2.7.3, $B = \varinjlim B_\alpha$ where $\{B_\alpha\}$ is the directed system of finitely generated submodules of B. By Corollary 2.7.10, $M \otimes_R B = \varinjlim (M \otimes_R B_\alpha)$. In $M \otimes_R B_1$ we have the element $u = \sum x_i \otimes \alpha(y_i)$ and the image of u in $\varinjlim (M \otimes_R B_\alpha)$ is equal to $(1 \otimes \alpha)(v) = 0$. By Lemma 2.7.5, there exists B_2, a finitely generated submodule of B which contains B_1, such that under the restriction map $\phi_2^1 : M \otimes_R B_1 \to M \otimes_R B_2$ we have $\phi_2^1(u) = 0$. The sequence

$$0 \to A_1 \xrightarrow{\alpha} B_2$$

is exact and the modules are finitely generated over R. Therefore, tensoring with M gives the exact sequence

$$0 \to M \otimes_R A_1 \xrightarrow{1\otimes\alpha} M \otimes_R B_2.$$

In $M \otimes_R A_1$ there is the element $v_1 = \sum_{i=1}^n x_i \otimes y_i$ which maps onto v in $M \otimes_R A$. Under $1 \otimes \alpha$, the image of v_1 in $M \otimes_R B_2$ is $\phi_2^1(u)$, which is 0. Therefore $v_1 = 0$, hence $v = 0$. $\square$

If R is any ring, M is any left R-module, and I is a right ideal in R, the multiplication map

$$\mu : I \otimes_R M \to M$$

is defined by $r \otimes x \mapsto rx$. The image of μ is

$$IM = \left\{ \sum_{i=1}^n r_i x_i \mid n \geq 1, r_i \in I, x_i \in M \right\}$$

which is a $\mathbb{Z}$-submodule of M. If I is a two-sided ideal, then IM is an R-submodule of M.

COROLLARY 3.7.4. *Let R be any ring and M a left R-module. The following are equivalent.*

(1) M is a flat R-module.

(2) For every right ideal I of R, the sequence

$$0 \to I \otimes_R M \xrightarrow{\mu} M \to M/IM \to 0$$

is an exact sequence of $\mathbb{Z}$-modules.

(3) *For every finitely generated right ideal I of R, the sequence*

$$0 \to I \otimes_R M \xrightarrow{\mu} M \to M/IM \to 0$$

is an exact sequence of $\mathbb{Z}$-modules.

(4) *If there exist $a_1, \dots, a_r$ in R and $x_1, \dots, x_r$ in M such that $\sum_i a_i x_i = 0$, then there exist an integer s, elements $\{b_{ij} \in R \mid 1 \le i \le r, 1 \le j \le s\}$ in R, and $y_1, \dots, y_s$ in M satisfying $\sum_i a_i b_{ij} = 0$ for all j and $x_i = \sum_j b_{ij} y_j$ for all i.*

PROOF. (1) implies (2): is routine.

(2) implies (3): is trivial.

(3) implies (2): Let I be any right ideal in R. According to Exercise 2.7.3, $I = \varinjlim I_\alpha$, where each I_α is a finitely generated right ideal in R and $I_\alpha \subseteq I$. By Corollary 2.7.10, $\varinjlim (I_\alpha \otimes_R M) = I \otimes_R M$. By hypothesis the sequence

$$0 \to I_\alpha \otimes_R M \xrightarrow{\mu_\alpha} M$$

is exact for each α. By Theorem 2.7.6, the sequence

$$0 \to \varinjlim I_\alpha \otimes_R M \to M$$

is exact, which proves (2).

(2) implies (1): Start with the exact sequence of right $\mathbb{Z}$-modules

$$0 \to I \otimes_R M \to R \otimes_R M.$$

Since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, the sequence

$$\operatorname{Hom}_{\mathbb{Z}}(R \otimes_R M, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}_{\mathbb{Z}}(I \otimes_R M, \mathbb{Q}/\mathbb{Z}) \to 0$$

is an exact sequence of $\mathbb{Z}$-modules. By Theorem 2.4.10, the sequence

$$\operatorname{Hom}_R(R, \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}_R(I, \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \to 0$$

is an exact sequence of $\mathbb{Z}$-modules. By Lemma 2.6.4, $\operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is an injective right R-module. By Theorem 2.6.18, this implies M is a flat left R-module.

(1) implies (4): Assume M is a flat R-module and $\sum_i a_i x_i = 0$ for some elements $a_i \in R$ and $x_i \in M$. Define $\theta : R^{(r)} \to R$ by the assignment $(b_1, \dots, b_r) \mapsto \sum_i a_i b_i$. Then θ is a homomorphism of right R-modules and the image of θ is the right ideal of R generated by $a_1, \dots, a_r$. Let $K = \ker(\theta)$ and apply the tensor functor $() \otimes_R M$ to the exact sequence $0 \to K \to R^{(r)} \to R$. The sequence

$$0 \to K \otimes_R M \to M^{(r)} \xrightarrow{\theta_M} M$$

is an exact sequence of $\mathbb{Z}$-modules, since M is flat. Moreover, θ_M is defined by the assignment $(m_1, \dots, m_r) \mapsto \sum_i a_i m_i$. We identify $K \otimes_R M$ with $\ker(\theta_M)$. Since $(x_1, \dots, x_r) \in \ker(\theta_M)$, there exists $\lambda = \sum_j \kappa_j \otimes y_j \in K \otimes_R M$ such that $\lambda = (x_1, \dots, x_r)$. Since $\kappa_j \in K$, we can write $\kappa_j = (b_{1j}, \dots, b_{rj})$ for each j. This proves (4).

(4) implies (2): Let I be any right ideal of R and let $\theta : I \otimes_R M \to M$. Suppose λ is an arbitrary element of the kernel of θ. Then there exist $a_1, \dots, a_r$ in I and $x_1, \dots, x_r$ in M such that $\lambda = \sum_i a_i \otimes x_i$ and $\theta(\lambda) = \sum_i a_i x_i = 0$. By (4) there are elements b_{ij} in R and y_j in M such that $x_i = \sum_j b_{ij} y_j$ and $\sum_i a_i b_{ij} = 0$. In this case,

$$\lambda = \sum_i a_i \otimes \left(\sum_j b_{ij} y_j \right) = \sum_j \left(\sum_i a_i b_{ij} \right) \otimes y_j = 0$$

so θ is one-to-one. $\square$

In Corollary 3.7.5 we show that over a local ring a finitely generated module M is flat if and only if it is free if and only if it is projective. Since we do not assume M is of finite presentation, this statement is stronger than that of Theorem 2.6.19.

COROLLARY 3.7.5. *Let R be a local ring and M a finitely generated R-module. The following are equivalent.*

(1) M is a free R-module.
(2) M is a projective R-module.
(3) M is a flat R-module.

PROOF. (1) implies (2): Follows straight from the definition of projective.

(2) implies (3): This is Exercise 2.3.6.

(3) implies (1): If $\mathfrak{m}$ is the maximal ideal of R and $\{x_i + \mathfrak{m}M \mid 1 \le i \le n\}$ is a basis for the vector space $M/\mathfrak{m}M$ over the residue field $R/\mathfrak{m}$, then $\{x_1, \dots, x_n\}$ generate M over R. This follows from Lemma 3.4.1.

To prove that $\{x_1, \dots, x_n\}$ is a free basis for M, it is enough to show that any dependence relation $\sum_{i=1}^n a_i x_i = 0$ is trivial. The proof is by induction on n. We prove that if $1 \le j \le n$ and $\xi_1, \dots, \xi_j$ are elements of M such that $\{\xi_i + \mathfrak{m}M \mid 1 \le i \le j\}$ is a linearly independent set in $M/\mathfrak{m}M$ over $R/\mathfrak{m}$, then $\xi_1, \dots, \xi_j$ are linearly independent over R.

For the basis step, say $x \in M - \mathfrak{m}M$ and that there exists $a \in R$ such that $ax = 0$. By Corollary 3.7.4 (4), there exist $b_1, \dots, b_s$ in R and $y_1, \dots, y_s$ in M such that $ab_j = 0$ for each b_j and $x = \sum_j b_j y_j$. Since $x \notin \mathfrak{m}M$, not all of the b_j are in $\mathfrak{m}$. Suppose $b_1 \in R - \mathfrak{m}$. Then b_1 is invertible in R, so $ab_1 = 0$ implies $a = 0$.

Inductively assume $n > 1$ and that the result holds for $n-1$ elements of M. Assume $\{x_i + \mathfrak{m}M \mid 1 \le i \le n\}$ are linearly independent over the residue field $R/\mathfrak{m}$ and that there is a dependence relation $\sum_i a_i x_i = 0$. By Corollary 3.7.4 (4), there exist b_{ij} in R and $y_1, \dots, y_s$ in M such that $\sum_i a_i b_{ij} = 0$ for each j and $x_i = \sum_j b_{ij} y_j$ for each i. Since $x_n \notin \mathfrak{m}M$, not all of the b_{nj} are in $\mathfrak{m}$. Let $b_{n1} \in R - \mathfrak{m}$. Then b_{n1} is invertible in R, so we can solve $\sum_i a_i b_{i1} = 0$ for a_n to get

$$a_n = -b_{n1}^{-1} \sum_{i=1}^{n-1} a_i b_{i1} = \sum_{i=1}^{n-1} c_i a_i.$$

Substitute to get

$$\begin{aligned} 0 &= \sum_i a_i x_i \\ &= a_1 x_1 + \cdots + a_{n-1} x_{n-1} + \sum_{i=1}^{n-1} c_i a_i x_n \\ &= a_1(x_1 + c_1 x_n) + \cdots + a_{n-1}(x_{n-1} + c_{n-1} x_n). \end{aligned}$$

The set $\{x_1 + c_1 x_n, \dots, x_{n-1} + c_{n-1} x_n\}$ is linearly independent modulo $\mathfrak{m}M$. By the induction hypothesis we conclude that $a_1 = a_2 = \cdots = a_{n-1} = 0$. Since $a_n = \sum_{i=1}^{n-1} c_i a_i = 0$, we are done. □

7.3. Finitely Presented and Flat is Projective. In this section the ring R is a general ring, not necessarily commutative. The goal is to prove that an R-module M is finitely generated and projective if and only if M is of finite presentation and flat.

LEMMA 3.7.6. *Let R be any ring, M a flat left R-module and*

$$0 \to A \xrightarrow{\subseteq} B \xrightarrow{\theta} M \to 0$$

an exact sequence of left R-modules, where $A = \ker(\theta)$.

(1) *For any right ideal I of R, $A \cap IB = IA$.*
(2) *Suppose B is a free left R-module, and $\{b_i \mid i \in J\}$ is a basis for B over R. If $x = \sum_i r_i b_i$ is in A, then there exist $a_i \in A$ such that $x = \sum_i r_i a_i$.*
(3) *Suppose B is a free left R-module. For any finite set $\{a_1, \dots, a_n\}$ of elements of A, there exists $f \in \operatorname{Hom}_R(B,A)$ such that $f(a_i) = a_i$ for $i = 1, \dots, n$.*

PROOF. (1): The multiplication map μ induces a commutative diagram

$$\begin{tikzcd} I \otimes_R A \arrow[r, "\mu"] \arrow[d] & IA \arrow[r] \arrow[d, "\subseteq"] & 0 \\ I \otimes_R B \arrow[r, "\mu"] & IB \arrow[r] & 0 \end{tikzcd}$$

of $\mathbb{Z}$-modules with exact rows. The image of $I \otimes_R A \to B$ is equal to IA and clearly $IA \subseteq A \cap IB$. Since M is flat, Corollary 3.7.4 implies $\mu : I \otimes_R M \cong IM$ is an isomorphism. The diagram

$$\begin{tikzcd} & I \otimes_R A \arrow[r] \arrow[d, "\gamma"] & I \otimes_R B \arrow[r, "1\otimes\theta"] \arrow[d, "\mu"] & I \otimes_R M \arrow[r] \arrow[d, "\cong"] & 0 \\ 0 \arrow[r] & A \cap IB \arrow[r] & IB \arrow[r, "\theta"] & IM & \end{tikzcd}$$

is commutative and the rows are exact. The Snake Lemma (Theorem 2.5.2) says that γ is onto. This proves that the image of $I \otimes_R A \to B$ is equal to $A \cap IB$.

(2): Suppose we are given $x = \sum_i r_i b_i \in A$, where only finitely many of the r_i are nonzero. Let I be the right ideal of R generated by the coordinates $\{r_i\}$ of x. Then $x \in A \cap IB = IA$. Since $IA = (\sum_i r_i R)A = \sum_i r_i RA = \sum_i r_i A$, there exist $a_i \in A$ such that $x = \sum_i r_i a_i$.

(3): Let $\{b_j \mid j \in J\}$ be a basis for the free module B. Let $x_1, \dots, x_n$ be elements in A. The proof is by induction on n. Assume $n = 1$. Since $x_1 \in B$, we write $x_1 = \sum_j r_j b_j$ where $r_j \in R$ and only finitely many of r_j are nonzero. By Part (2) there exist $a_j \in A$ such that $x = \sum_j r_j a_j$. Define $f : B \to A$ on the basis by setting $f(b_j) = a_j$. Then $f(x_1) = x_1$.

Inductively, assume $n > 1$ and that the result holds for any set involving $n-1$ or fewer elements of A. By the $n = 1$ case, there exists $f_1 : A \to B$ such that $f_1(x_1) = x_1$. By the $n-1$ case applied to the set $x_2 - f_1(x_2), \dots, x_n - f_1(x_n)$, there exists $f_2 : A \to B$ such that $f_2(x_j - f_1(x_j)) = x_j - f_1(x_j)$ for $j = 2, \dots, n$. Set $f = f_1 + f_2 - f_2 f_1$. Note that

$$f(x_1) = f_1(x_1) + f_2(x_1) - f_2(f_1(x_1)) = x_1,$$

and if $2 \le j \le n$, then

$$\begin{aligned} f(x_j) &= f_1(x_j) + f_2(x_j) - f_2(f_1(x_j)) \\ &= f_1(x_j) + f_2(x_j - f_1(x_j)) \\ &= f_1(x_j) + x_j - f_1(x_j) \\ &= x_j. \end{aligned}$$

$\square$

We give another proof of Theorem 2.6.19.

COROLLARY 3.7.7. *Let R be any ring and M a finitely generated left R-module. The following are equivalent.*

(1) *M is projective.*
(2) *M is of finite presentation and flat.*

PROOF. (1) implies (2): If M is finitely generated and projective, then M is flat by Exercise 2.3.6 and of finite presentation by Corollary 2.1.8.

(2) implies (1): Let

$$0 \to A \to B \xrightarrow{\theta} M \to 0$$

be a finite presentation of M, where B is a finitely generated free left R-module, and A is a finitely generated submodule of B. According to Lemma 3.7.6 (3), this sequence is split exact. □

7.4. Flat Algebras. The goal of this section is to prove Corollary 3.7.10, which will be applied in Section 9.6.

LEMMA 3.7.8. *Let S be a commutative flat R-algebra. If I and J are ideals in R, then*

(1) $(I \cap J)S = IS \cap JS$.
(2) If J is finitely generated, then $(I : J)S = (IS : JS)$.

PROOF. (1): The sequence of R-modules

$$0 \to I \cap J \to R \to R/I \oplus R/J$$

is exact, by Theorem 1.1.7. Tensoring with S,

$$0 \to (I \cap J) \otimes_R S \to S \to S/IS \oplus S/JS$$

is exact. By Corollary 3.7.4, this implies $(I \cap J) \otimes_R S = (I \cap J)S = IS \cap JS$.

(2): Step 1: $J = Ra$ is principal. Let $\ell_a : R \to R$ be "left-multiplication by a" and $\eta : R \to R/I$ the natural map. The kernel of the composite map $\eta \circ \ell_a$ is $(I : Ra)$. Tensor the exact sequence

$$0 \to (I : Ra) \to R \xrightarrow{\eta \circ \ell_a} R/I$$

with S and use Corollary 3.7.4 to get

$$0 \to (I : Ra)S \to S \xrightarrow{\eta \circ \ell_a} S/IS.$$

This shows $(I : Ra)S = (IS : aS)$.

Step 2: $J = Ra_1 + \cdots + Ra_n$. By Exercise 1.1.13, $(I : J) = \bigcap_i (I : Ra_i)$. By Part (1) and Step 1,

$$(I : J)S = \bigcap_i (I : Ra_i)S = \bigcap_i (IS : Ra_iS) = (IS : \sum_i Ra_iS) = (IS : JS).$$

□

In Proposition 3.7.9 we give another proof of Proposition 3.5.11.

PROPOSITION 3.7.9. *Let S be a commutative flat R-algebra and M a finitely generated R-module. Then* $\operatorname{annih}_R(M)S = \operatorname{annih}_S(M \otimes_R S)$.

PROOF. The proof is by induction on the number of generators of M. Assume $M = Ra$ is a principal R-module. If $\mathfrak{a} = \operatorname{annih}_R(M)$, then $R/\mathfrak{a} = M$. By Corollary 3.7.4, $\mathfrak{a} \otimes_R S = \mathfrak{a}S$. Tensor the exact sequence $0 \to \mathfrak{a} \to R \to M \to 0$ with S to get $\mathfrak{a}S = \operatorname{annih}_R(M)S = \operatorname{annih}_S(M \otimes_R S)$. Inductively, assume I and J are finitely generated submodules of M for which the proposition holds. Since S is flat, we view $I \otimes_R S$, $J \otimes_R S$, and $(I+J) \otimes_R S$ as submodules of $M \otimes_R S$. We have

$$\begin{aligned}
\operatorname{annih}_R(I+J)S &= (\operatorname{annih}_R(I) \cap \operatorname{annih}_R(J))\, S \quad \text{(Exercise 1.6.1)} \\
&= \operatorname{annih}_R(I)S \cap \operatorname{annih}_R(J)S \quad \text{(Lemma 3.7.8)} \\
&= \operatorname{annih}_S(I \otimes_R S) \cap \operatorname{annih}_S(J \otimes_R S) \quad \text{(Induction Hypothesis)} \\
&= \operatorname{annih}_S(I \otimes_R S + J \otimes_R S) \quad \text{(Exercise 1.6.1)} \\
&= \operatorname{annih}_S\left((I+J) \otimes_R S\right).
\end{aligned}$$

Hence the proposition holds for $I+J$. □

COROLLARY 3.7.10. *Let R be a commutative ring and W a multiplicative set.*

(1) If M is a finitely generated R-module, then $W^{-1}\operatorname{annih}_R(M) = \operatorname{annih}_{W^{-1}R}(W^{-1}M)$.
(2) If I and J are finitely generated ideals in R, then $W^{-1}(I : J) = (W^{-1}I : W^{-1}J)$.

PROOF. (1): Follows from Proposition 3.7.9.

(2): By Exercise 1.1.3, $(I : J) = \operatorname{annih}_R\left((I+J)/I\right)$. To complete the proof, apply Part (1). □

7.5. Exercises.

EXERCISE 3.7.1. Let A be an R-algebra and M a faithfully flat left A-module which is also faithfully flat as a left R-module. Prove that A is a faithfully flat R-algebra.

EXERCISE 3.7.2. Let $f : R \to S$ be a homomorphism of commutative rings such that S is a flat R-algebra. Let $V \subseteq R$ and $W \subseteq S$ be multiplicative sets such that $f(V) \subseteq W$. Prove that $W^{-1}S$ is a flat $V^{-1}R$-module.

EXERCISE 3.7.3. Let R be a ring, M a left R-module, and $a \in R$. Let $\ell_a : M \to M$ be "left multiplication by a". Prove:

(1) If M is a flat R-module, and $\ell_a : R \to R$ is one-to-one, then $\ell_a : M \to M$ is also one-to-one.
(2) If R is commutative, A is a flat R-algebra, and $a \in R$ is not a zero divisor, then a is not a zero divisor in A.
(3) If R is an integral domain and A is a flat R-algebra, then the structure homomorphism $R \to A$ which maps $x \mapsto x \cdot 1$ is one-to-one, hence A is a faithful R-module.

EXERCISE 3.7.4. Let $R \subseteq S$ be an extension of integral domains. Assume R has the property that for every $\mathfrak{m} \in \operatorname{Max} R$, $R_{\mathfrak{m}}$ is a principal ideal domain (a Dedekind domain has this property). Show that S is a flat R-algebra. (Hint: Use Proposition 3.7.1 to assume R is a local PID. Use Corollary 3.7.4.)

CHAPTER 4

Artinian and Noetherian Rings and Modules

If an R-module M satisfies the descending chain condition (DCC) on submodules, then M is said to be artinian. If M satisfies the ascending chain condition (ACC) on submodules, then M is called noetherian. Viewing the ring R as a left R-module, we say R is artinian, if the DCC on left ideals holds. Likewise, R is noetherian, if the ACC on left ideals holds. We prove in Theorem 4.5.1 that an artinian ring is noetherian. Theorem 4.1.16 shows that a commutative noetherian ring R has a unique decomposition as a finite direct sum of ideals of the form Re, where the ring Re has only two idempotents. We prove that a module has a composition series if and only if both the ACC and the DCC hold on submodules.

Section 4.2 begins with the definition of the Jacobson radical. If R is a ring, the Jacobson radical of R is the intersection of all maximal left ideals in R. If R is commutative, then the Jacobson radical contains the nil radical, but in general the two radicals are not equal. In terms of the Jacobson radical, we state and prove a version of Nakayama's Lemma for noncommutative rings. In Section 4.3 we study semisimple rings. These are rings which are artinian and have trivial Jacobson radical. We prove that a ring is semisimple if and only if every module is projective.

In this book, a simple ring is an artinian ring with no proper two-sided ideal. We prove that a semisimple ring is a finite direct sum of simple rings. The main result on this subject is the Wedderburn-Artin Theorem which shows that a simple ring R is isomorphic to the ring of n-by-n-matrices over a division ring D. The ring D is unique up to isomorphism and is called the division ring component of R. The proof is an application of Morita Theory.

Theorem 4.5.6 is an important structure theorem for commutative artinian rings. In it we show that a commutative artinian ring is a finite direct sum of local artinian rings. For instance, this implies that over a commutative artinian ring any finitely generated projective module of constant rank is a free module.

In Section 4.6 we apply the results from all of the previous sections to compute some nontrivial examples. First we completely classify all k-algebras of dimension 3, for an arbitrary field k. Secondly we give a complete classification of all finite rings of order p^3, where p is a prime.

1. Chain Conditions

DEFINITION 4.1.1. Let R be any ring and M an R-module. Let $\mathscr{S}$ be the set of all R-submodules of M, partially ordered by $\subseteq$, the set inclusion relation. The reader is referred to Section 1.2 for the definitions of ACC, DCC, maximum condition, and minimum condition on the partially ordered set $\mathscr{S}$. We say that M satisfies the *ascending chain condition (ACC) on submodules*, if $\mathscr{S}$ satisfies the ACC. We say that M satisfies the *descending chain condition (DCC) on submodules*, if $\mathscr{S}$ satisfies the DCC. We say that M satisfies the *maximum condition on submodules*, if $\mathscr{S}$ satisfies the maximum condition. We say that M satisfies the *minimum condition on submodules*, if $\mathscr{S}$ satisfies the minimum condition.

DEFINITION 4.1.2. Let R be any ring and M an R-module. We say M is *noetherian* if M satisfies the ACC on submodules. We say M is *artinian* if M satisfies the DCC on submodules. The ring R is said to be (left) *noetherian* if R is noetherian when viewed as a left R-module. In this case we say R satisfies the ACC on left ideals. The ring R is said to be (left) *artinian* if R is artinian when viewed as a left R-module. In this case we say R satisfies the DCC on left ideals.

LEMMA 4.1.3. *Let R be a ring and M an R-module. Then M is artinian, that is M satisfies the DCC on submodules, if and only if M satisfies the minimum condition on submodules.*

PROOF. This follows from Proposition 1.2.1. $\square$

COROLLARY 4.1.4. *Let R be a ring. Then R is artinian, that is R satisfies the DCC on left ideals, if and only if R satisfies the minimum condition on left ideals.*

EXAMPLE 4.1.5. We list a few examples of artinian rings. Some of the proofs will come later.

(1) A division ring has only two left ideals, hence satisfies both ACC and DCC on left ideals.
(2) If M is a finite dimensional vector space over a division ring D, then $\operatorname{Hom}_D(M,M)$ is artinian, by Exercise 4.1.12.
(3) By Exercise 4.1.13, any finite dimensional algebra over a field is artinian.

LEMMA 4.1.6. *Let R be a ring and M an R-module. The following are equivalent.*

(1) M is noetherian. That is, M satisfies the ACC on submodules.
(2) M satisfies the maximum condition on submodules.
(3) Every submodule of M is finitely generated.

PROOF. (1) and (2) are equivalent by Proposition 1.2.1.

(2) implies (3): Let A be a submodule of M and let $\mathfrak{S}$ be the set of all finitely generated submodules of A. Let B be a maximal member of $\mathfrak{S}$. If $B = A$, then we are done. Otherwise, let x be an arbitrary element of $A - B$. So $B + Rx$ is a finitely generated submodule of A which properly contains B. This contradicts the maximality of B.

(3) implies (1): Suppose $M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots$ is a chain of submodules in M. The set theoretic union $U = \bigcup_{n \geq 0} M_n$ is also a submodule of M. Then U is finitely generated, so for large enough m, M_m contains each element of a generating set for U. Then $U \subseteq M_m$. Moreover, for each $i \geq m$, $U \subseteq M_m \subseteq M_i \subseteq U$. This proves that the ACC is satisfied by M. $\square$

COROLLARY 4.1.7. *Let R be a ring. The following are equivalent.*

(1) R is noetherian. That is, R satisfies the ACC on left ideals.
(2) Every left ideal of R is finitely generated as an R-module.
(3) Every nonempty set of left ideals of R contains a maximal member.

EXAMPLE 4.1.8. We list a few examples of noetherian rings. Some of the proofs will come later.

(1) In a principal ideal ring R, left ideals are principal, so Corollary 4.1.7 (3) is satisfied. In particular, a PID is noetherian.
(2) It follows from the Hilbert Basis Theorem, which is prove in Theorem 6.2.1 below, that a polynomial ring $k[x_1, \dots, x_n]$ in n variables over a field k is noetherian.
(3) We will prove in Theorem 4.5.1 below that an artinian ring is noetherian.

LEMMA 4.1.9. *Let R be any ring and*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

a short exact sequence of R-modules.

(1) *The following are equivalent.*
   (a) *B satisfies the ACC on submodules.*
   (b) *A and C satisfy the ACC on submodules.*
(2) *The following are equivalent.*
   (a) *B satisfies the DCC on submodules.*
   (b) *A and C satisfy the DCC on submodules.*

PROOF. (2): Is left to the reader.

(1): (a) implies (b): Assume B satisfies the ACC on submodules. By virtue of α we can identify A with an R-submodule of B. Any ascending chain of submodules of A is also an ascending chain of submodules in B, hence is eventually constant. Therefore A satisfies the ACC on submodules. If $C_0 \subseteq C_1 \subseteq C_2 \subseteq \dots$ is a chain of submodules in C, then $\beta^{-1}(C_0) \subseteq \beta^{-1}(C_1) \subseteq \beta^{-1}(C_2) \subseteq \dots$ is a chain of submodules of B. There exists d such that for all $i > d$, $\beta^{-1}(C_d) = \beta^{-1}(C_i)$. But β is onto, so $C_d = C_i$ and we have shown C satisfies the ACC on submodules.

(b) implies (a): Assume A and C satisfy the ACC on submodules. For simplicity's sake, identify A with the kernel of β. Let $B_0 \subseteq B_1 \subseteq B_2 \subseteq \dots$ be a chain of submodules in B. For each i set $C_i = \beta(B_i)$ and let A_i be the kernel of $\beta : B_i \to C_i$. The ascending chain $C_0 \subseteq C_1 \subseteq C_2 \subseteq \dots$ eventually is constant. The reader should verify that the A_is form an ascending chain $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$ in A which also is eventually constant. Find some $d > 0$ such that for all $i > d$ we have $A_d = A_i$ and $C_d = C_i$. The diagram

$$\begin{tikzcd}
0 \arrow[r] & A_d \arrow[r, "\alpha"] \arrow[d, "="] & B_d \arrow[r, "\beta"] \arrow[d, "\subseteq"] & C_d \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & A_i \arrow[r, "\alpha"] & B_i \arrow[r, "\beta"] & C_i \arrow[r] & 0
\end{tikzcd}$$

commutes. By the Five Lemma, (Theorem 2.5.1), the center vertical arrow is onto so $B_d = B_i$. □

COROLLARY 4.1.10. *Let R be a ring, M an R-module and A a submodule.*

(1) *The following are equivalent.*
   (a) *M satisfies the ACC on submodules.*
   (b) *A and M/A satisfy the ACC on submodules.*
(2) *The following are equivalent.*
   (a) *M satisfies the DCC on submodules.*
   (b) *A and M/A satisfy the DCC on submodules.*

PROOF. Apply Lemma 4.1.9 to the exact sequence $0 \to A \to M \to M/A \to 0$. □

COROLLARY 4.1.11. *Let R be a ring and $M_1, \dots, M_n$ some R-modules.*

(1) *The following are equivalent.*
   (a) *For each i, M_i satisfies the ACC on submodules.*
   (b) *$M_1 \oplus \cdots \oplus M_n$ satisfies the ACC on submodules.*
(2) *The following are equivalent.*
   (a) *For each i, M_i satisfies the DCC on submodules.*

(b) $M_1 \oplus \cdots \oplus M_n$ *satisfies the DCC on submodules.*

PROOF. If $n = 2$, the result follows from Lemma 4.1.9 applied to the exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$. Use induction on n. Apply Lemma 4.1.9 to the exact sequence

$$0 \to M_1 \oplus \cdots \oplus M_{n-1} \to M_1 \oplus \cdots \oplus M_n \to M_n \to 0$$

to finish the proof. □

COROLLARY 4.1.12. *If R is a noetherian ring and M is a finitely generated R-module, then*

(1) M satisfies the ACC on submodules,
(2) M is finitely presented,
(3) M satisfies the maximum condition on submodules, and
(4) every submodule of M is finitely generated.

PROOF. By Lemma 1.6.11, for some $m > 0$, M is the homomorphic image of $R^{(m)}$. There is an exact sequence

$$0 \to K \to R^{(m)} \xrightarrow{\theta} M \to 0$$

where K is defined to be the kernel of θ. To prove (2) it is enough to prove K is finitely generated. If we prove M and K both satisfy the ACC on submodules, then we get (1) and Lemma 4.1.6 implies (2), (3) and (4). By Definition 4.1.2, R as an R-module satisfies the ACC on submodules. By Corollary 4.1.11, $R^{(m)}$ satisfies the ACC on submodules. By Lemma 4.1.9, M and K both satisfy the ACC on submodules. □

COROLLARY 4.1.13. *Let R be a noetherian ring.*

(1) If I is a two-sided ideal of R, then R/I is noetherian.
(2) If R is commutative and $W \subseteq R$ is a multiplicative set, then R_W is noetherian.

PROOF. (1) Lemma 4.1.9 applied to the exact sequence of R-modules

$$0 \to I \to R \to R/I \to 0$$

shows that R/I satisfies the ACC on left ideals, hence is noetherian.

(2) Let J be an ideal in R_W. If $x/w \in J$, then $x/1 \in J$. Let I be the ideal of R consisting of all x such that $x/1 \in J$. Then I is finitely generated, $I_W = J$, and a generating set for I as an ideal in R maps to a generating set for I_W as an ideal of R_W. □

PROPOSITION 4.1.14. *Let R be a commutative noetherian ring.*

(1) $\operatorname{Spec} R$ *is a noetherian topological space.*
(2) $\operatorname{Spec} R$ *has a finite number of irreducible components.*
(3) $\operatorname{Spec} R$ *has a finite number of connected components.*

PROOF. Apply Corollary 3.3.9 and Proposition 1.3.7 □

COROLLARY 4.1.15. *Let R be a commutative noetherian ring and I an ideal of R which is not the unit ideal. There is a one-to-one correspondence between the irreducible components of $V(I)$ and the minimal prime over-ideals of I given by $Z \mapsto I(Z)$.*

PROOF. Let $V(I) = Z_1 \cup \cdots \cup Z_r$ be the decomposition into irreducible components, which exists by Propositions 4.1.14 and 1.3.7. For each i, let $P_i = I(Z_i)$. By Lemma 3.3.10, each of the ideals $P_1, \dots, P_r$ is prime. First we show that each P_i is minimal. Assume $I \subseteq Q \subseteq P_i$, for some prime Q. Then $V(I) \supseteq V(Q) \supseteq Z_i$. By Lemma 3.3.10, $V(Q)$ is irreducible. By the uniqueness part of Proposition 1.3.7, $V(Q) = Z_i$. Therefore, $Q = I(V(Q)) = P_i$.

Now let P be a minimal prime over-ideal of I. We show that P is equal to one of $P_1,\dots,P_r$. By Lemma 3.3.10, $V(P)$ is an irreducible subset of $V(I)$. Since $V(P)\subseteq Z_1\cup\cdots\cup Z_r$, $V(P)\subseteq Z_i$, for some i. Therefore, $I\subseteq P_i\subseteq P$. Since P is minimal, $P=P_i$. ☐

THEOREM 4.1.16. *Let R be a commutative noetherian ring. Then there exist primitive idempotents $e_1,\dots,e_n$ in R such that R is the internal direct sum $R=Re_1\oplus\cdots\oplus Re_n$. This decomposition is unique in the sense that, if $R=Rf_1\oplus\cdots\oplus Rf_p$ is another such decomposition of R, then $n=p$, and after rearranging, $e_1=f_1$, ..., $e_n=f_n$.*

PROOF. Let $\operatorname{Spec} R=X_1\cup\cdots\cup X_n$ be the decomposition into connected components, which exists by Propositions 4.1.14 and 1.3.7. By Corollary 3.3.14 there are idempotents $e_1,\dots,e_n$ in R such that $X_i=U(e_i)=V(1-e_i)$ is homeomorphic to $\operatorname{Spec} Re_i$, and $R=Re_1\oplus\cdots\oplus Re_n$. Corollary 3.3.16 implies each e_i is a primitive idempotent. The uniqueness claim comes from Theorem 3.2.5. ☐

EXAMPLE 4.1.17. Consider the localization $\mathbb{Z}[2^{-1}]$ of $\mathbb{Z}$ at the multiplicative set $\{1,2,2^2,2^3,\dots\}$. By Example 4.1.8, the principal ideal domain $\mathbb{Z}$ is noetherian. By Corollary 4.1.13, $\mathbb{Z}[2^{-1}]$ is a noetherian ring. As a $\mathbb{Z}$-module $\mathbb{Z}[2^{-1}]$ is not noetherian since

$$\mathbb{Z}\cdot 2^{-1}\subsetneq\mathbb{Z}\cdot 2^{-2}\subsetneq\mathbb{Z}\cdot 2^{-3}\subsetneq\cdots\subsetneq\mathbb{Z}\cdot 2^{-i}\subsetneq\cdots$$

is a strictly increasing chain of $\mathbb{Z}$-submodules.

1.1. Exercises.

EXERCISE 4.1.1. Let $R_1,\dots,R_n$ be rings. Prove that the direct sum $R_1\oplus\cdots\oplus R_n$ is an artinian ring if and only if each R_i is an artinian ring.

EXERCISE 4.1.2. Let R be an artinian ring and M a finitely generated R-module. Show that M satisfies the DCC on submodules.

EXERCISE 4.1.3. Prove that if R is an artinian ring and I is a two-sided ideal in R, then R/I is artinian.

EXERCISE 4.1.4. Let R be a commutative artinian ring and W is a multiplicative set in R. Show that $W^{-1}R$ is artinian.

EXERCISE 4.1.5. Let R be a noetherian ring and M a finitely generated R-module. Prove that the following are equivalent.

(1) M is flat.
(2) M is projective.

EXERCISE 4.1.6. Prove that if R is an artinian domain, then R is a division ring.

EXERCISE 4.1.7. Let $\theta: R\to S$ be a homomorphism of commutative rings such that S is a faithfully flat R algebra. Prove:

(1) If S is artinian, then R is artinian.
(2) If S is noetherian, then R is noetherian.

EXERCISE 4.1.8. Let R be a noetherian commutative ring. Show that if M and N are finitely generated R-modules, then $\operatorname{Hom}_R(M,N)$ is a finitely generated R-module.

EXERCISE 4.1.9. This exercise is based on an example attributed to Lance Small. Let R be the subring of $M_2(\mathbb{Q})$ consisting of all matrices of the form $\begin{pmatrix} a & 0\\ b & c\end{pmatrix}$ where $a\in\mathbb{Z}$ and $b,c\in\mathbb{Q}$. Show that every left ideal of R is finitely generated. Show that R does not satisfy the ACC on right ideals. Conclude that R is left noetherian but not right noetherian. Show R is not isomorphic to the opposite ring R^o.

1.2. Composition Series.

DEFINITION 4.1.18. Let R be any ring and M an R-module. We say M is *simple* if $M \neq 0$ and 0 is a maximal submodule of M. So if M is a simple module, then (0) and M are the only submodules.

DEFINITION 4.1.19. Let R be any ring and M an R-module. Suppose there is a strictly descending finite chain of submodules

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$$

starting with $M = M_0$ and ending with $M_n = 0$. The *length* of the chain is n. A *composition series* for M is a chain such that M_i/M_{i+1} is simple. If M has no composition series, define $\ell(M) = \infty$. Otherwise, let $\ell(M)$ be the minimum of the lengths of all composition series of M. The number $\ell(M)$ is called the *length* of M. If $\ell(M) < \infty$, then we say M is a *module of finite length*. We prove in Proposition 4.1.20 below that if M has a composition series, then every composition series has the same length. We show in Proposition 4.1.21 below that a module M of finite length satisfies both the ACC and DCC on submodules. In particular, M is finitely generated.

PROPOSITION 4.1.20. *Let R be any ring and M an R module. Suppose that M has a composition series of length n. Then*

1. *If N is a proper submodule of M, then $\ell(N) < \ell(M)$.*
2. *Every chain in M has length less than or equal to $\ell(M)$.*
3. *Every composition series has length n.*
4. *Every chain in M can be extended to a composition series.*

PROOF. (1): Suppose

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$$

is a composition series for M such that $n = \ell(M)$. For each i, set $N_i = N \cap M_i$. The reader should verify that the kernel of the composite map $N_i \to M_i \to M_i/M_{i+1}$ is N_{i+1}. Therefore, $N_i/N_{i+1} \to M_i/M_{i+1}$ is one-to-one. Either $N_{i+1} = N_i$, or $N_i/N_{i+1} \cong M_i/M_{i+1}$ is simple. If we delete any repetitions from $N = N_0 \supseteq N_1 \supseteq \cdots N_n = 0$, then we are left with a composition series for N. This shows $\ell(N) \leq \ell(M)$. For contradiction's sake assume $\ell(N) = \ell(M)$. Then $N_i/N_{i+1} \cong M_i/M_{i+1}$ for each $i = 0, \ldots, n-1$. By a finite induction argument we conclude that $N = M$, a contradiction.

(2): Given any chain of submodules

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_m = 0$$

starting at M and ending at 0, apply Part (1) to get

$$0 < \ell(M_{m-1}) < \cdots < \ell(M_1) < \ell(M)$$

which proves that $m \leq \ell(M)$.

(3): Follows straight from Part (2) and the definition of $\ell(M)$.

(4): Consider any chain of submodules

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_m = 0$$

starting at M and ending at 0. If $m = \ell(M)$, then this is a composition series. Otherwise for some i, M_i/M_{i+1} is not simple, so there exists a proper submodule $M_i \subsetneq N \subsetneq M_{i+1}$. Insert N into the chain, re-label and get a chain of length $m+1$. Repeat this insertion procedure until the length of the new chain is equal to $\ell(M)$, at which point it must be a composition series. $\square$

PROPOSITION 4.1.21. *Let R be any ring and M an R-module. The following are equivalent.*

(1) M has a composition series.
(2) M satisfies both the ACC and the DCC on submodules.

PROOF. (1) implies (2): By Proposition 4.1.20 all chains in M are of bounded length.
(2) implies (1): By Lemma 4.1.6, every submodule of M satisfies the maximum condition on submodules. Set $M_0 = M$. Let M_1 be a maximal submodule of M_0. Iteratively suppose $i > 0$ and let M_{i+1} be a maximal submodule of M_i. The strictly descending chain $M_0, M_1, M_2, \dots$ must converge to 0 since M satisfies the DCC on submodules. The result is a composition series. □

PROPOSITION 4.1.22. *Let R be any ring and*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

an exact sequence of R-modules of finite length. Then $\ell(B) = \ell(A) + \ell(C)$.

PROOF. Start with a composition series $A = A_0 \supsetneq A_1 \supsetneq \cdots \supsetneq A_m = 0$ for A and a composition series $C = C_0 \supsetneq C_1 \supsetneq \cdots \supsetneq C_n = 0$ for C. Then

$$B = \beta^{-1}(C_0) \supsetneq \beta^{-1}(C_1) \supsetneq \cdots \supsetneq \beta^{-1}(C_n) = \alpha(A_0) \supsetneq \alpha(A_1) \supsetneq \cdots \supsetneq \alpha(A_m) = 0$$

is a composition series for B. □

1.3. Infinite Chains. This short section has only one goal, which is to prove Proposition 4.1.23. It is an application of the Well Ordering Principle (Axiom 1.2.2) and uses transfinite induction. To simplify the statement of the proposition and its proof we use some terminology from the theory of Ordinal Numbers which we define here. For more on this subject the reader is referred to a book on Set Theory, for example [**58**]. Let I be a well ordered set and $\beta \in I$. As in Section 1.2, denote by $(-\infty, \beta) = \{\xi \in I \mid \xi < \beta\}$ the segment of I determined by β. We say β has an *immediate predecessor* if the set $(-\infty, \beta)$ contains a maximal element, say α. In this case we write $\beta = \alpha + 1$. This is equivalent to the statement that β is the minimal element of the set $\{\xi \in I \mid \alpha < \xi\}$. The proposition shows that a group G is the union of a chain of subgroups $\{G_\alpha\}_{\alpha \in I}$ indexed by a well ordered set I with the property that for every $\alpha \in I$, the subgroup $G_{\alpha+1}$ is equal to the subgroup of G generated by G_α and a single element $x_{\alpha+1}$. The set I and the subgroups making up the chain are not unique. For our purposes the following proposition is sufficient. Nevertheless we remark that if one uses properties of ordinal numbers it is possible to choose I to be minimal among all such ordinals.

PROPOSITION 4.1.23. *Let G be a group and H a subgroup of G. Then there exists a well ordered set I and a family of subgroups $\{G_\xi \mid \xi \in I\}$ satisfying the following.*

(1) If 1 denotes the least element of I, then $G_1 = H$.
(2) If α and β are in I and $\alpha \le \beta$, then $H \subseteq G_\alpha \subseteq G_\beta$.
(3) For each $\beta \in I$, if β has an immediate predecessor, say α, then there exists $x_\beta \in G$ such that G_β is the subgroup of G generated by G_α and $\{x_\beta\}$. If β has no immediate predecessor, then $G_\beta = \bigcup_{\xi \in (-\infty, \beta)} G_\xi$.
(4) $G = \bigcup_{\xi \in I} G_\xi$.

PROOF. If $H = G$, then take $I = \{1\}$, $G_1 = H$, and stop. Otherwise let $X = (G - H) \cup \{e\}$, where e is the identity element of G. By Axiom 1.2.2, there exists a well ordered set I and a function $I \to X$. If $\xi \in I$, then the image of ξ in X will be denoted x_ξ. Without loss of generality, assume the least element of I is 1 and $x_1 = e$ and if $1 < \xi$, then $x_\xi \neq e$. Set $G_1 = H$. The proof is based on Proposition 1.2.3. Assume inductively that $\gamma \in I$, $1 < \gamma$, and that we have defined a family of subgroups $\{G_\xi \mid \xi \in (-\infty, \gamma)\}$ satisfying:

(a) If $\alpha \leq \beta < \gamma$, then $H \subseteq G_\alpha \subseteq G_\beta$.
(b) If $\beta < \gamma$ and β has an immediate predecessor, say α, then G_β is the subgroup of G generated by G_α and x_β. If β has no immediate predecessor, then $G_\beta = \bigcup_{\xi \in (-\infty,\beta)} G_\xi$.

To define G_γ, there are two cases. If γ has an immediate predecessor, say α, then we define G_γ to be the subgroup of G generated by G_α and x_γ. If γ has no immediate predecessor, then G_γ is defined to be $\bigcup_{\xi \in (-\infty,\gamma)} G_\xi$, which is a subgroup of G since $\{G_\xi \mid \xi \in (-\infty, \gamma)\}$ is a chain of subgroups. By Proposition 1.2.3 this defines $\{G_\xi \mid \xi \in I\}$ satisfying properties (1), (2) and (3).

To complete the proof, we show that there exists a chain of subgroups of G that satisfies properties (1) — (4). Let $\mathscr{S}$ be the set of all chains of subgroups of G of the form $C = \{G_\xi \mid \xi \in I\}$ where I is a well ordered set and properties (1) — (3) are satisfied. By the construction above, $\mathscr{S}$ is nonempty. Given a chain $C = \{G_\xi \mid \xi \in I\}$ in $\mathscr{S}$, let $G(C) = \bigcup\{G_\xi \mid \xi \in I\}$ be the union of the subgroups in C. The usual set containment relation on the sets $G(C)$ defines a partial order on $\mathscr{S}$. That is, if C_1 and C_2 are in $\mathscr{S}$, then $C_1 \leq C_2$ if $G(C_1) \subseteq G(C_2)$. By a Zorn's Lemma argument, $\mathscr{S}$ contains a maximal member, say $C = \{G_\xi \mid \xi \in I\}$. If $G(C) \neq G$, then we apply the procedure in the first paragraph to get a nontrivial chain of subgroups of G containing $G(C)$ of the form $C_1 = \{K_\eta \mid \eta \in J\}$ where J is a well ordered set and if 1 is the least element of J, then $K_1 = G(C)$. The set $I + J$ is well ordered in the usual way (see Exercise 4.1.15). Combining the two chains C and C_1 gives a chain of subgroups in $\mathscr{S}$ that is strictly larger than C, a contradiction. Therefore, C satisfies properties (1) — (4). $\square$

1.4. Exercises.

EXERCISE 4.1.10. Let D be a division ring and V a finite dimensional vector space over D. Prove:

(1) V is a simple module if and only if $\dim_D(V) = 1$.
(2) $\dim_D(V) = \ell(V)$.

EXERCISE 4.1.11. Let D be a division ring and V a vector space over D. Prove that the following are equivalent.

(1) V is finite dimensional over D.
(2) V is a D-module of finite length.
(3) V satisfies the ACC on submodules.
(4) V satisfies the DCC on submodules.

EXERCISE 4.1.12. Let D be a division ring.

(1) Prove that the ring $M_n(D)$ of all n-by-n matrices over D is both artinian and noetherian.
(2) Let M be a finite dimensional D-vector space. Prove that the ring $\mathrm{Hom}_D(M,M)$ is both artinian and noetherian.

EXERCISE 4.1.13. Let k be a field and R a k-algebra which is finite dimensional as a k-vector space. Prove that the ring R is both artinian and noetherian. See Exercise 6.2.5 for the converse of this statement when R is commutative.

EXERCISE 4.1.14. Let $\theta : R \to S$ be a homomorphism of rings. Let M be a left S-module. View M as a left R-module using θ (Example 1.1.11 (3)). Show that if M is an R-module of finite length, then M is an S-module of finite length.

EXERCISE 4.1.15. Let I_1 be a well ordered set with binary relation $R_1 \subseteq I_1 \times I_1$. Let I_2 be a well ordered set with binary relation $R_2 \subseteq I_2 \times I_2$. Using the distributive law $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$, the set $R_1 \cup (I_1 \times I_2) \cup R_2$ is a subset of $(I_1 \cup I_2) \times (I_1 \cup I_2)$ and hence defines a binary relation on $I_1 \cup I_2$. Show that this makes $I_1 \cup I_2$ into a well ordered set. Usually this well ordered set is denoted $I_1 + I_2$ and in words we say, "elements of I_1 are comparable by R_1, elements of I_1 are less than elements of I_2, and elements of I_2 are comparable by R_2".

2. The Jacobson Radical and Nakayama's Lemma

DEFINITION 4.2.1. Let R be any ring and M a left R-module. As in Section 1.1.3, we say N is a maximal submodule of M in case N is a maximal member of the set $\{S \subseteq M \mid S \text{ is a submodule of } M \text{ and } S \neq M\}$, ordered by set inclusion. By Theorem 1.1.12 (3), N is a maximal submodule of M if and only if N/M is simple. The *Jacobson radical* of M is

$$\begin{aligned} \mathrm{J}(M) &= \bigcap \{N \mid N \text{ is a maximal submodule of } M\} \\ &= \bigcap \{\ker f \mid f \in \operatorname{Hom}_R(M,S) \text{ and } S \text{ is simple}\}. \end{aligned}$$

By $\mathrm{J}(R)$ we denote the Jacobson radical of R viewed as a left R-module. Then $\mathrm{J}(R)$ is equal to the intersection of all maximal left ideals of R.

LEMMA 4.2.2. *$\mathrm{J}(R)$ is a two-sided ideal of R.*

PROOF. For any R-module M, let $g \in \operatorname{Hom}_R(M,M)$, let S be any simple R-module and let $f \in \operatorname{Hom}_R(M,S)$. Then $f \circ g \in \operatorname{Hom}_R(M,S)$ so $\mathrm{J}(M) \subseteq \ker(f \circ g)$. Then $f(g(\mathrm{J}(M))) = 0$ for all f. That is, $g(\mathrm{J}(M)) \subseteq \mathrm{J}(M)$. Given $r \in R$, let $\rho_r \in \operatorname{Hom}_R(R,R)$ be "right multiplication by r" (Lemma 2.4.7). Then $\rho_r(\mathrm{J}(R)) = \mathrm{J}(R) \cdot r \subseteq \mathrm{J}(R)$. □

THEOREM 4.2.3. *(Nakayama's Lemma) Let R be any ring and I a left ideal of R. The following are equivalent.*

(1) $I \subseteq \mathrm{J}(R)$.
(2) $1 + I = \{1 + x \mid x \in I\} \subseteq \operatorname{Units}(R)$.
(3) If M is a finitely generated left R-module and $IM = M$, then $M = 0$.
(4) If M is a finitely generated left R-module and N is a submodule of M and $IM + N = M$, then $N = M$.

PROOF. (1) implies (2): Let $x \in I$. Assume $1 + x$ has no left inverse. Then $R(1+x) \neq R$. By Zorn's Lemma, Proposition 1.2.4, $R(1+x)$ is contained in some maximal left ideal L of R. Then $1 + x = y \in L$. But $I \subseteq \mathrm{J}(R) \subseteq L$. So $x \in L$. Therefore $1 = y - x \in L$. This contradiction means there exists $u \in R$ such that $u(1+x) = 1$. We show u has a left inverse. Since $1 = u + ux$, $u = 1 - ux = 1 + (-u)x \in 1 + I$ and by the previous argument, u has a left inverse. Then $u \in \operatorname{Units}(R)$ and $1 + x = u^{-1}$.

(2) implies (1): Assume L is a maximal left ideal and L does not contain I. Then $I + L = R$, so $1 = x + y$ for some $x \in I$ and $y \in L$. Hence $y = 1 - x = 1 + (-x) \in 1 + I \subseteq \operatorname{Units}(R)$, a contradiction.

(1) plus (2) implies (3): Assume $IM = M$ and prove that $M = 0$. Now $I \subseteq \mathrm{J}(R)$ and $IM = M$ implies $\mathrm{J}(R)M \subseteq M = IM \subseteq \mathrm{J}(R)M$. Therefore $\mathrm{J}(R)M = M$. Assume $M \neq 0$. Pick a generating set $\{x_1, \ldots, x_n\}$ for M with $n \geq 1$ minimal. A typical element of M

looks like $\sum_{i=1}^{n} r_i x_i$, $r_i \in R$. A typical element of $\mathrm{J}(R)M$ looks like $\sum_{i=1}^{n} a_i r_i x_i$, $a_i \in \mathrm{J}(R)$. By Lemma 4.2.2, $b_i = a_i r_i \in \mathrm{J}(R)$, so each element of $\mathrm{J}(R)M$ can be written in the form $\sum_{i=1}^{n} b_i x_i$, $b_i \in \mathrm{J}(R)$. In particular, $x_1 = \sum_{i=1}^{n} b_i x_i$, some $b_i \in \mathrm{J}(R)$. Then $x_1(1-b_1) = \sum_{i=2}^{n} b_i x_i$. Now $1-b_1 \in 1+I$, so $1-b_1$ is a unit. This shows that M is generated by $x_2, \dots, x_n$. This contradiction implies $M = 0$.

(3) implies (4): Since M is finitely generated so is M/N. Then

$$I(M/N) = \frac{IM+N}{N} = M/N$$

and by (3) we conclude that $M/N = 0$, or $N = M$.

(4) implies (1): Assume L is a maximal left ideal of R and that L does not contain I. Then $I+L = R$. Apply (4) with $L = N$, $R = M$. Since $IR \supseteq I$ we have $IR+L = R$ so $L = R$, a contradiction. $\square$

COROLLARY 4.2.4. *Let*

$$\mathrm{J}_r(R) = \bigcap\{I \mid I \text{ is a maximal right ideal of } R\}.$$

Then $\mathrm{J}_r(R) = \mathrm{J}(R)$.

PROOF. By Lemma 4.2.2 both $\mathrm{J}_r(R)$ and $\mathrm{J}(R)$ are two-sided ideals of R. It follows from Theorem 4.2.3 (2) that $1+\mathrm{J}(R)$ consists of units of R. Apply a right-sided version of Theorem 4.2.3 to the right ideal $\mathrm{J}(R)$ and conclude that $\mathrm{J}(R) \subseteq \mathrm{J}_r(R)$. The converse follows by symmetry. $\square$

COROLLARY 4.2.5. *If I is a left ideal of R which consists of nilpotent elements, then* $I \subseteq \mathrm{J}(R)$.

PROOF. Let $a \in I$ and assume $a^n = 0$ for some $n \geq 1$. Then $(1-a)(1+a+a^2+\cdots+a^{n-1}) = 1$. So $1+I \subseteq \mathrm{Units}(R)$. $\square$

COROLLARY 4.2.6. *If R is artinian, then* $\mathrm{J}(R)$ *is nilpotent.*

PROOF. Consider the chain of left ideals

$$\mathrm{J}(R) \supseteq \mathrm{J}(R)^2 \supseteq \mathrm{J}(R)^3 \supseteq \dots.$$

There is some $n \geq 1$ such that $\mathrm{J}(R)^n = \mathrm{J}(R)^{n+1}$. Assume $\mathrm{J}(R)^n \neq 0$. Since R is artinian, by Lemma 4.1.3, the minimum condition is satisfied on left ideals. Consider the set $\mathscr{L}$ of all finitely generated left ideals L such that $\mathrm{J}(R)^n L \neq 0$. Since $\mathrm{J}(R)^n = \mathrm{J}(R)^n \mathrm{J}(R) \neq 0$, there exists $a \in \mathrm{J}(R)$ such that $\mathrm{J}(R)^n Ra \neq 0$. Since $Ra \in \mathscr{L}$, the set is nonempty. Pick a minimal element L of $\mathscr{L}$. Now $\mathrm{J}(R)^n L \subseteq L$. Since $L \neq 0$, Theorem 4.2.3 (3) says $\mathrm{J}(R)^n L$ is a proper subset of L. But $\mathrm{J}(R)^n (\mathrm{J}(R)^n L) = \mathrm{J}(R)^{2n} L = \mathrm{J}(R)^n L \neq 0$. There exists $a \in \mathrm{J}(R)^n L$ such that $\mathrm{J}(R)^n Ra \neq 0$. So $Ra \in \mathscr{L}$. But $Ra \subseteq \mathrm{J}(R)^n L \subsetneq L$. This is a contradiction, because L is minimal. We conclude $\mathrm{J}(R)^n = 0$. $\square$

COROLLARY 4.2.7. *Let R be a ring.*

(1) If M is a maximal two-sided ideal of R, then $\mathrm{J}(R) \subseteq M$.
(2) If $f : R \to S$ is an epimorphism of rings, then $f(\mathrm{J}(R)) \subseteq \mathrm{J}(S)$.
(3) If R is commutative and A is an R-algebra which is finitely generated as an R-module, then $\mathrm{J}(R)A \subseteq \mathrm{J}(A)$.

PROOF. (1): Assume the contrary. The ideal $\mathrm{J}(R)+M$ is a two-sided ideal of R. Since M is maximal, $\mathrm{J}(R)+M = R$. By Theorem 4.2.3 (4), $M = R$, a contradiction.

(2): Let $x \in \mathrm{J}(R)$ and $a \in R$. By Theorem 4.2.3, $1+ax \in \mathrm{Units}(R)$, so $f(1+ax) = 1+f(a)f(x) \in \mathrm{Units}(S)$. Therefore the left ideal $Sf(x)$ is contained in $\mathrm{J}(S)$.

(3): Let M be a finitely generated left A-module. Then M is finitely generated as an R-module. If $(\mathrm{J}(R)A)M = M$, then $\mathrm{J}(R)(AM) = \mathrm{J}(R)M = M$. By (1) implies (3) of Theorem 4.2.3, $M = 0$. By (3) implies (1) of Theorem 4.2.3, $\mathrm{J}(R)A \subseteq \mathrm{J}(A)$. □

2.1. Idempotents and the Jacobson Radical. As in Section 3.3.1, if R is a ring, then $\mathrm{idemp}(R) = \{x \in R \mid x^2 - x = 0\}$ denotes the set of idempotents of R. The homomorphic image of an idempotent is an idempotent, so given a homomorphism of rings $A \to B$, there is a function $\mathrm{idemp}(A) \to \mathrm{idemp}(B)$. If this function is onto, then we say idempotents of B lift to idempotents of A. Corollary 4.2.8 is a corollary to Theorem 4.2.3, Nakayama's Lemma. It provides useful sufficient conditions for lifting idempotents modulo an ideal.

COROLLARY 4.2.8. *Let R be a ring and I a two-sided ideal of R.*

(1) If R is commutative and $I \subseteq \mathrm{J}(R)$, then $\mathrm{idemp}(R) \to \mathrm{idemp}(R/I)$ *is one-to-one.*
(2) If I consists of nilpotent elements, then $\mathrm{idemp}(R) \to \mathrm{idemp}(R/I)$ *is onto.*

PROOF. (1): Let $e_0, e_1 \in \mathrm{idemp}(R)$ and assume $x = e_0 - e_1 \in I$. We show that $x = 0$. Look at

$$\begin{aligned} x^3 &= e_0^3 - 3e_0^2 e_1 + 3e_0 e_1^2 - e_1^3 \\ &= e_0 - 3e_0 e_1 + 3e_0 e_1 - e_1 \\ &= e_0 - e_1 \\ &= x. \end{aligned}$$

Then $x(x^2 - 1) = 0$. By Theorem 4.2.3, $x^2 - 1$ is a unit, which implies that $x = 0$.

(2): Assume I consists of nilpotent elements. By Corollary 4.2.5, $I \subseteq \mathrm{J}(R)$. If $x \in R$, denote by $\bar{x}$ the image of x in R/I. Assume $\bar{x}^2 = \bar{x}$. It follows that $(1-\bar{x})^2 = 1 - \bar{x}$. Since $x - x^2 \in I$, for some $n > 0$ we have $(x - x^2)^n = x^n(1-x)^n = 0$. Set $e_0 = x^n$ and $e_1 = (1-x)^n$. Then $e_0 e_1 = e_1 e_0 = 0$, $\bar{e}_0 = \bar{x}^n = \bar{x}$, and $\bar{e}_1 = (1-\bar{x})^n = 1 - \bar{x}$. This says that $e_0 + e_1 - 1 \in I$, so by Theorem 4.2.3, $u = e_0 + e_1$ is a unit in R. We have $1 = e_0 u^{-1} + e_1 u^{-1} = u^{-1} e_0 + u^{-1} e_1$, hence $e_0 = e_0^2 u^{-1} = u^{-1} e_0^2$, and $e_0 u = e_0^2 = u e_0$. We have shown that e_0 commutes with u. From this it follows that $e_0 u^{-1}$ is an idempotent of R. Since $\bar{u} = 1$, $\bar{e}_0 \bar{u}^{-1} = \bar{x}$. □

2.2. Exercises.

EXERCISE 4.2.1. Let R be a ring, I an ideal contained in $\mathrm{J}(R)$, and $\eta : R \to R/I$ the natural map. Prove the following:

(1) If $\eta(r)$ is a unit in R/I, then r is a unit in R.
(2) The natural map $\eta : \mathrm{Units}(R) \to \mathrm{Units}(R/I)$ is onto and the kernel is $1 + I$.

EXERCISE 4.2.2. Let R be a PID, π a prime in R, and $e \geq 1$ an integer. This exercise describes the group of units in the principal ideal ring $R/(\pi^e)$ in terms of the additive and multiplicative groups of the field $R/(\pi)$. To simplify notation, write $(\cdot)^*$ for the group of units in a ring. Let $I = (\pi)/(\pi^e)$ be the maximal ideal of $R/(\pi^e)$. Starting with the descending chain of ideals

$$R/(\pi^e) = I^0 \supseteq I^1 \supseteq \cdots \supseteq I^{e-1} \supseteq I^e = (0),$$

for $i = 1, \ldots, e$, define U_i to be the coset $1 + I^i$. Write U_0 for the group of units $(R/(\pi^e))^*$. Prove

$$(R/(\pi^e))^* = U_0 \supseteq U_1 \supseteq \cdots \supseteq U_{e-1} \supseteq U_e = (1)$$

is a series of subgroups satisfying these properties: U_0/U_1 is isomorphic to the multiplicative group $(R/(\pi))^*$, and for $i = 1, \ldots, e-1$, U_i/U_{i+1} is isomorphic to the additive group $R/(\pi)$. To prove this, follow this outline.

(1) To show the U_i form a series of subgroups and U_0/U_1 is isomorphic to $(R/(\pi))^*$, use Exercise 4.2.1 to prove that
$$1 \to U_i \to (R/(\pi^e))^* \to \big(R/(\pi^i)\big)^* \to 1$$
is an exact sequence, for $i = 1, \dots, e$.

(2) Assume $e \geq 2$. Show that $R/(\pi) \cong U_{e-1}$ by the assignment which sends x to the coset represented by $1 + x\pi^{e-1}$. This can be proved directly. By induction on e, conclude that $R/(\pi) \cong 1 + (\pi^{i-1})/(\pi^i)$, for all $i \geq 2$.

(3) Prove that $U_{i-1}/U_i \cong 1 + (\pi^{i-1})/(\pi^i)$, for all $i \geq 2$. This can be proved directly, or by applying the Snake Lemma (Theorem 2.5.2) to the commutative diagram:
$$\begin{tikzcd}
1 \arrow[r] & U_i \arrow[r] \arrow[d] & (R/(\pi^e))^* \arrow[r] \arrow[d] & \big(R/(\pi^i)\big)^* \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & U_{i-1} \arrow[r] & (R/(\pi^e))^* \arrow[r] & \big(R/(\pi^{i-1})\big)^* \arrow[r] & 1
\end{tikzcd}$$

EXERCISE 4.2.3. Let R be a ring and $\mathrm{J}(R) \supseteq B \supseteq A$ a chain of ideals. Prove this generalization of Exercise 4.2.2: $\mathrm{Units}(R) \supseteq 1+B \supseteq 1+A$ is a series of normal subgroups and the quotient group $(1+B)/(1+A)$ is isomorphic to $1 + (B/A)$. (Hint: Show that the image of the natural map $1 + B \to \mathrm{Units}(R/A)$ is $1 + (B/A)$.)

EXERCISE 4.2.4. Let $R = R_1 \oplus \cdots \oplus R_n$ be a direct sum, where each R_i is a commutative local ring. Prove that a finitely generated projective R-module M of constant rank r is a free R-module of rank r.

EXERCISE 4.2.5. Let R be a commutative semilocal ring. Prove:

(1) $R/J(R)$ is isomorphic to a finite direct sum of fields.

(2) If M is a finitely generated projective R-module of constant rank r, then M is a free R-module of rank r. (Hint: Mimic the proof of Proposition 3.4.2.)

EXERCISE 4.2.6. Let R be a ring. Prove that $\mathrm{J}(M_n(R)) = M_n(\mathrm{J}(R))$. (Hint: First show that if S is a simple left R-module, then S^n is a simple left $M_n(R)$-module.)

EXERCISE 4.2.7. Let R be a ring and I a two-sided ideal of R such that $I \subseteq \mathrm{J}(R)$. Let $M, N \in {}_R\mathfrak{M}$ and $\theta : N \to M$ a homomorphism of left R-modules. Let $1 \otimes \theta : R/I \otimes_R N \to R/I \otimes_R M$ be the homomorphism of R/I-modules induced by tensoring with $R/I \otimes_R (\ )$.

(1) Assuming M is finitely generated as an R-module, prove that θ is onto if and only if $1 \otimes \theta$ is onto.

(2) Assuming M and N are finitely generated projective R-modules, prove that θ is an isomorphism if and only if $1 \otimes \theta$ is an isomorphism.

EXERCISE 4.2.8. Prove that $\mathrm{J}(\prod_{i \in I} R_i) = \prod_{i \in I}(\mathrm{J}(R_i))$, where $\{R_i \mid i \in I\}$ is a family of rings.

3. Semisimple Modules and Semisimple Rings

In this section we introduce an important class of artinian rings called semisimple rings. A ring R is semisimple if every left ideal of R is a module direct summand of R. We eventually derive more than five sets of necessary and sufficient conditions for a ring R to be semisimple. Two such sets that are particularly useful are: R is semisimple if and only if every R-module is projective, which is true if and only if R is artian and $\mathrm{J}(R) = (0)$.

THEOREM 4.3.1. *Let R be a ring and M a nonzero R-module. The following are equivalent.*

(1) *$M = \bigoplus_{i\in I} M_i$ is the internal direct sum of a family of simple submodules $\{M_i \mid i \in I\}$.*
(2) *$M = \sum_{i\in I} M_i$ is the sum of a family of simple submodules $\{M_i \mid i \in I\}$.*
(3) *Every submodule of M is a direct summand of M.*

PROOF. (2) clearly follows from (1).

(2) implies (1): Assume $M = \sum_{i\in I} M_i$ and each M_i is a simple submodule of M. By Zorn's Lemma, Proposition 1.2.4, choose a maximal subset $J \subseteq I$ such that the sum $\sum_{i\in J} M_i$ is a direct sum. Assume $\sum_{i\in J} M_i \neq M$. Then there is some $k \in I$ such that M_k is not contained in $\sum_{i\in J} M_i$. Since M_k is simple,

$$\big(\sum_{i\in J} M_i\big) \bigcap M_k = 0.$$

In this case, the sum $\big(\sum_{i\in J} M_i\big) + M_k$ is a direct sum which contradicts the choice of J.

(1) plus (2) implies (3): Then M is an internal direct sum of simple submodules $\{M_i \mid i \in I\}$. Let N be a submodule of M. If $N = M$, then we are done. Assume $N \neq M$. For each $i \in I$, $M_i \cap N$ is a submodule of M_i hence $M_i \cap N = 0$ or $M_i \cap N = M_i$. Then for some $k \in I$ we have $M_k \cap N = 0$. Choose a maximal subset $J \subseteq I$ such that

$$\big(\sum_{i\in J} M_i\big) \bigcap N = 0. \tag{3.1}$$

Let

$$N' = \big(\sum_{i\in J} M_i\big) + N.$$

If $N' = M$, then $M = \big(\sum_{i\in J} M_i\big) \oplus N$ and we are done. Otherwise for some index $k \in I$, $M_k \cap N' = 0$. Consider

$$x \in \big(\sum_{i\in J} M_i + M_k\big) \cap N.$$

Write $x = x_0 + x_k$ where $x_0 \in \sum_{i\in J} M_i$ and $x_k \in M_k$. So $x_k = x - x_0 \in N' \cap M_k = 0$. By (3.1) we see that $x = 0$. Then $J \cup \{k\}$ satisfies (3.1) which contradicts the choice of J.

(3) implies (2): Let $\{M_i \mid i \in I\}$ be the family of all simple submodules of M. Set $N = \sum_i M_i$. Assume $N \neq M$. By (3), $M = N \oplus N'$ for some nonzero submodule N'. To finish the proof, it is enough to show the existence of a simple submodule of N'. Let $x \in N' - (0)$. Being a direct summand of M, N' satisfies (3) (the reader should verify this). Therefore $N' = Rx \oplus N''$. Let L be a maximal left ideal of R such that L contains $\operatorname{annih}_R(x)$. Then R/L is simple. The diagram

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "\alpha"'] & R \arrow[r] \arrow[d, "\beta"'] & R/L \arrow[r] \arrow[d, "\eta"'] & 0 \\
0 \arrow[r] & Lx \arrow[r] & Rx \arrow[r] & Rx/Lx \arrow[r] & 0
\end{tikzcd}$$

commutes. The rows are exact. The vertical maps α and β are onto, therefore η is onto. Since $x \notin Lx$, we know Rx/Lx is not zero. Then η is not the zero map. Since R/L is simple, η is an isomorphism. Applying (3) to Rx gives $Rx = Lx \oplus S$ where $S \cong Rx/Lx$ is a simple R-submodule of Rx. But then N' contains S, so we are done. $\square$

DEFINITION 4.3.2. Let R be a ring and M an R-module. If M satisfies any of the properties of Theorem 4.3.1, then M is called *semisimple*.

THEOREM 4.3.3. *Let R be a ring. The following conditions are equivalent.*

(1) *Every left R-module is projective.*
(2) *Every short exact sequence of left R-modules splits.*
(3) *Every left R-module is semisimple.*
(4) *R is semisimple when viewed as a left R-module.*
(5) *R is artinian and $\mathrm{J}(R) = 0$.*

PROOF. The reader should verify that (3) implies (4) and that the first three statements are equivalent.

(4) implies (1): Let M be a left R-module. Let $I = M$ and $F = R^I$. As in the proof of Proposition 2.1.1, there is an R-module homomorphism $\pi : F \to M$ which is surjective. Because R is semisimple, R is the internal direct sum of simple R-submodules. So F is an internal direct sum of simple R-modules. So F is semisimple and $\ker \pi$ is a direct summand of F. Then $F \cong \ker \pi \oplus M$, hence M is projective.

(4) implies (5): Since $\mathrm{J}(R)$ is a submodule of R, it is an internal direct summand of R. For some left ideal L we have $R = \mathrm{J}(R) \oplus L$. By Lemma 3.2.4, $\mathrm{J}(R) = Re_1$ and $L = Re_2$ and $e_1e_2 = 0$ and $1 = e_1 + e_2$. By Nakayama's Lemma (Theorem 4.2.3), e_2 is a unit in R. Therefore $e_1 = 0$ and $\mathrm{J}(R) = 0$. To show that R is artinian, assume $I_1 \supseteq I_2 \supseteq I_3 \dots$ is a descending chain of ideals. Since R is semisimple as an R-module, I_1 is a direct summand of R, and we can write $R = L_0 \oplus I_1$. Also, I_2 is a direct summand of I_1, so $R = L_0 \oplus L_1 \oplus I_2$. For each index i, I_{i+1} is a direct summand of I_i and we can write $I_i = L_i \oplus I_{i+1}$. Each $L_i = Re_i$ for some idempotent e_i and $\bigoplus_{i=1}^{\infty} L_i$ is a direct summand of R. That is,

$$R = \left(\bigoplus_{i=1}^{\infty} L_i \right) \oplus L$$

for some L. The representation of 1 in the direct sum involves only a finite number of the e_i, and the rest are 0.

(5) implies (4): We show that R is the direct sum of a finite collection of minimal left ideals and apply Theorem 4.3.1 (1). Let L_1 be a minimal left ideal of R. This exists since R is artinian. Since $\mathrm{J}(R) = 0$ it follows from Corollary 4.2.5 that $L_1^2 \neq 0$. By Lemma 3.2.4 (3), there is a left ideal I_1 and $R = L_1 \oplus I_1$. If $I_1 = 0$, then we are done. Otherwise, by the minimum condition, there is a minimal left ideal L_2 of R contained in I_1. Again from Lemma 3.2.4 we have $R = L_2 \oplus J$ for some J. There exists an R-module homomorphism $\pi : R \to L_2$ which splits $L_2 \subseteq R$. The restriction of π to I_1 is therefore a splitting of $L_2 \subseteq I_1$. Therefore, $I_1 = L_2 \oplus I_2$, where $I_2 = \{x \in I_1 \mid \pi(x) = 0\} = I_1 \cap \ker \pi$. Hence $R = L_1 \oplus L_2 \oplus I_2$ where L_1, L_2 are minimal ideals in R. If $I_2 = 0$, then we are done. Otherwise we continue inductively to get $R = L_1 \oplus \cdots \oplus L_n \oplus I_n$ where each L_i is a minimal left ideal. After a finite number of iterations, the process terminates with $I_n = 0$ because R is artinian and $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ is a descending chain of ideals. □

DEFINITION 4.3.4. The ring R is called *semisimple* if R satisfies any of the equivalent conditions of Theorem 4.3.3.

EXAMPLE 4.3.5. Let R be an artinian ring. Then $R/\mathrm{J}(R)$ satisfies Theorem 4.3.3 (5), hence is semisimple.

4. Simple Rings and the Wedderburn-Artin Theorem

A ring R is simple if it is artinian and has no proper two-sided ideal. We show that a semisimple ring is a finite direct sum of simple rings. The main result of this section is the Wedderburn-Artin Theorem which shows that a simple ring is isomorphic to the ring of

n-by-n matrices ring over a division ring. This important theorem plays a fundamental role in the definition of the Brauer group of a field. The interested reader is referred to [**18**]. Results from this section will be applied in Section 5.5 to classify separable algebras over a field.

DEFINITION 4.4.1. A ring R is called *simple* if R is artinian and the only two-sided ideals of R are 0 and R. Since $\mathrm{J}(R)$ is a two-sided ideal, a simple ring satisfies Theorem 4.3.3 (5) hence is semisimple.

EXAMPLE 4.4.2. Let D be a division ring and M a finite dimensional D-vector space. Let $S = \operatorname{Hom}_D(M,M)$. By Exercise 4.1.12, S is artinian. By Corollary 2.8.4 it follows that there is a one-to-one correspondence between two-sided ideals of D and two-sided ideals of S. Since D is a simple ring, it follows that S is a simple ring. We prove the converse of this fact in Theorem 4.4.5.

THEOREM 4.4.3. *Let A be an artinian ring and let R be a semisimple ring.*

(1) Every simple left R-module is isomorphic to a minimal left ideal of R.
(2) R is a finite direct sum of simple rings.
(3) R is simple if and only if all simple left R-modules are isomorphic.
(4) If A is simple, then every nonzero A-module is faithful.
(5) If there exists a simple faithful A-module, then A is simple.

PROOF. (1): Let R be a semisimple ring. By the proof of Theorem 4.3.3 there are idempotents $e_1,\dots,e_n$ such that each Re_i is a minimal left ideal of R and $R = Re_1 \oplus \cdots \oplus Re_n$. Let S be any simple left R-module. Let x be a nonzero element of S. Then for some e_i we have $e_i x \neq 0$. The R-module homomorphism $Re_i \to S$ defined by $re_i \mapsto re_i x$ is an isomorphism because both modules are simple. This proves (1).

(2): Let $S_1,\dots,S_m$ be representatives for the distinct isomorphism classes of simple left R-modules. By (1) there are only finitely many such isomorphism classes. For each i, define

$$R_i = \sum_j \left\{ L_{ij} \mid L_{ij} \text{ is a left ideal of } R \text{ and } L_{ij} \cong S_i \right\}.$$

We proceed in four steps to show that $R = R_1 \oplus \cdots \oplus R_m$ and each R_i is a simple ring.

Step 1: R_i is a two-sided ideal. By definition, R_i is a left ideal of R. Pick any L_{ij}. Let $r \in R$ and consider the R-module homomorphism $\rho_r : L_{ij} \to R$ which is "right multiplication by r". Since L_{ij} is simple, either $\ker \rho_r = L_{ij}$ and $L_{ij} r \subseteq L_{ij}$, or $\ker \rho_r = 0$ and $L_{ij} \cong L_{ij} r$. In the latter case, the left ideal L_{ij} is isomorphic to some L_{ik}. In both cases, $L_{ij} r \subseteq R_i$ which shows $R_i r \subseteq R_i$ and R_i is a two-sided ideal of R.

Step 2: Let L be a minimal left ideal of R contained in R_i. We show that $L \cong S_i$. Since L is idempotent generated, there is some $e \in L$ such that $e^2 = e \neq 0$. Since $e \in L \subseteq R_i$, the R-module homomorphism $\rho_e : R_i \to L$ is nonzero. Since R_i is generated by the ideals L_{ij}, there is some j such that $L_{ij} e \neq 0$. The map $\rho_e : L_{ij} \to L$ is an isomorphism. Therefore $L \cong S_i$.

Step 3: $R = R_1 \oplus \cdots \oplus R_m$. Clearly $R = R_1 + \cdots + R_m$. For contradiction's sake, assume $R_1 \cap (R_2 + \cdots + R_m) \neq 0$. Let L be a minimal left ideal of R contained in $R_1 \cap (R_2 + \cdots + R_m)$. By Step 2, $L \cong S_1$. There is an idempotent e such that $L = Re$. As in Step 2, the map $\rho_e : R_2 + \cdots + R_m \to L$ is nonzero. Hence there exists L_{ik} such that $2 \leq i \leq m$ and $\rho_e : L_{ik} \to L$ is an isomorphism. This is a contradiction, since S_1 and S_i are not isomorphic. Therefore $R_1 \cap (R_2 + \cdots + R_m) = 0$. By induction on m, this step is done.

Step 4: Fix i and show that R_i is simple. By Theorem 4.3.3, R is artinian. Let I be a nonzero two-sided ideal in R_i. To show $I = R_i$, the plan is to show I contains each of the ideals L_{ij}. By Step 3 and Theorem 1.1.8, ideals of R_i are also ideals in R. In particular, I is a two-sided ideal in R. Let L be any minimal left ideal of R contained in I. By Step 2, $L = L_{ik}$ for some k. There exists an idempotent e such that $L_{ik} = Re$. Let L_{ij} be another minimal left ideal in R_i. There is an R-module isomorphism $\phi : I_{ik} \cong I_{ij}$. We have

$$\begin{aligned} L_{ij} &= \operatorname{im} \phi \\ &= \{\phi(re) \mid r \in R\} \\ &= \{\phi(ree) \mid r \in R\} \\ &= \{re\phi(e) \mid r \in R\}. \end{aligned}$$

Since e belongs to the two-sided ideal I, $L_{ij} \subseteq I$. Thus $I = R_i$.

(4): Assume A is simple. Let M be any nonzero left A-module. Let $I = \operatorname{annih}_A(M)$, a two-sided ideal of A. Since $1 \notin I$, it follows that $I \neq A$. Therefore $I = 0$ and M is faithful.

(3): By (2) we can write $R = R_1 \oplus \cdots \oplus R_m$ as a direct sum of simple rings. If all simple left R-modules are isomorphic, then $m = 1$ and R is simple. Now say R is simple and L is a simple left R-module. We know that $m = 1$, otherwise R_1 is a proper two-sided ideal. Then $L \cong L_{1j}$ for some j and all simple left R-modules are isomorphic.

(5): Assume A is artinian and S is a simple faithful left A-module. Since S is simple, $\mathrm{J}(A)S$ is either 0 or S. Since S is simple and faithful, S is nonzero and generated by one element. By Theorem 4.2.3 (3) we know $\mathrm{J}(A)S \neq S$. So $\mathrm{J}(A)S = 0$. Since S is faithful, $\mathrm{J}(A) = 0$. This proves A is semisimple. By (2) $A = A_1 \oplus \cdots \oplus A_n$ where each A_i is a two-sided ideal of A. Assume $n \geq 2$. By (1), we assume without loss of generality that $S \cong S_1$. Then $A_1 S = S$. Since the ideals are two-sided, $A_2 A_1 \subseteq A_1 \cap A_2 = 0$. Therefore $0 = (A_2 A_1)S = A_2(A_1 S) = A_2 S$. So $A_2 \subseteq \operatorname{annih}_A(S)$. This contradiction implies $n = 1$, and A is simple. □

LEMMA 4.4.4. *(Schur's Lemma) Let R be any ring and M a simple left R-module. Then $S = \operatorname{Hom}_R(M,M)$ is a division ring.*

PROOF. Is left to the reader. □

THEOREM 4.4.5. *(Wedderburn-Artin) Let R be a simple ring. Then $R \cong \operatorname{Hom}_D(M,M)$ for a finite dimensional vector space M over a division ring D. The division ring D and the dimension $\dim_D(M)$ are uniquely determined by R.*

PROOF. Since R is semisimple, by the proof of Theorem 4.3.3 there are idempotents $e_1, \ldots, e_n$ such that each $L_i = Re_i$ is a minimal left ideal of R and $R = Re_1 \oplus \cdots \oplus Re_n$ is an R-module direct sum. But R is simple, so $L_1 \cong \ldots \cong L_n$ by Theorem 4.4.3. Set $M = L_1$ and $D = \operatorname{Hom}_R(M,M)$. By Lemma 4.4.4, D is a division ring. Since $L_1 = Re_1$ for some idempotent e_1, M is finitely generated. By Theorem 4.3.3, M is projective. By Lemma 2.1.11, the trace ideal of M is a two-sided ideal of R. Since R is simple, M is a generator over R. By Morita Theory, Corollary 2.8.3 (1), $R \cong \operatorname{Hom}_D(M,M)$. By Corollary 2.8.3 (5), M is a finitely generated D-vector space.

To prove the uniqueness claims, assume D' is another division ring and M' is a finite dimensional D'-vector space and $\operatorname{Hom}_D(M,M) \cong \operatorname{Hom}_{D'}(M',M')$. By Morita Theory, $D' \cong \operatorname{Hom}_R(M',M')$ and M' is an R-progenerator. We know M' is a simple R-module, otherwise M' would have a nontrivial direct summand and $\operatorname{Hom}_R(M',M')$ would contain noninvertible elements. Since R is simple, by Theorem 4.4.3, $M \cong M'$ as R-modules. □

4.1. Central Simple Algebras.

DEFINITION 4.4.6. Let k be a field and A a k-algebra. We say A is a *central simple k-algebra* if these three conditions are met:

(1) A is a simple ring.
(2) A is a central k-algebra.
(3) $\dim_k(A) < \infty$.

EXAMPLE 4.4.7. It follows from Example 4.4.2 that the ring of matrices $M_n(k)$ over a field k is a central simple k-algebra. If A is a central simple k-algebra, then by Theorem 4.4.5 we know $A \cong \operatorname{Hom}_D(E,E)$ where D is a division ring and E is a finite dimensional D-vector space. The reader should verify that $\dim_k(D) < \infty$ and $Z(D) = k$.

PROPOSITION 4.4.8. *Let k be an algebraically closed field and A a central simple k-algebra. Then $A \cong M_n(k)$ for some n.*

PROOF. Let D be the division algebra component of A. Let $\alpha \in D$. Because D is a finite dimensional division algebra over k, $k[\alpha]$ is an algebraic field extension of k. Because k is algebraically closed, $\alpha \in k$. Therefore, $k = D$. □

Theorem 4.4.9 below shows that over a field k, tensor product induces a product on the category of all central simple k-algebras.

THEOREM 4.4.9. *Let k be a field and let A and B be simple k-algebras. If A is a central simple k-algebra, then*

(1) $A \otimes_k B$ is a simple ring.
(2) $Z(A \otimes_k B) = Z(B)$.

PROOF. (1): Let I be a nonzero two-sided ideal in $A \otimes_k B$. Let x be a nonzero element of I. Then there are $a_1, \dots, a_n$ in A and there are k-linearly independent $b_1, \dots, b_n$ in B such that $x = \sum_{i=1}^n a_i \otimes b_i$. Choose x such that n is minimal. Since A is simple, the principal ideal Aa_1A is the unit ideal. Pick $r_1, \dots, r_m, s_1, \dots, s_m$ in A such that $\sum_j r_j a_1 s_j = 1$. Since $(r_j \otimes 1)x(s_j \otimes 1) \in I$ for each j,

$$\begin{aligned}
y &= \sum_j (r_j \otimes 1)\, x\, (s_j \otimes 1) \\
&= \sum_j \Big((r_j \otimes 1) \Big(\sum_i a_i \otimes b_i \Big) (s_j \otimes 1) \Big) \\
&= \sum_j \sum_i (r_j a_i s_j \otimes b_i) \\
&= \sum_i \Big(\Big(\sum_j r_j a_i s_j \Big) \otimes b_i \Big) \\
&= 1 \otimes b_1 + a_2' \otimes b_2 + \cdots + a_n' \otimes b_n
\end{aligned}$$

is an element of I for some $a_2', \dots, a_n'$ in A. For all $a \in A$ we have

$$\begin{aligned}
(a \otimes 1)y - y(a \otimes 1) &= a \otimes b_1 + aa_2' \otimes b_2 + \cdots + aa_n' \otimes b_n \\
&\quad - \big(a \otimes b_1 + a_2' a \otimes b_2 + \cdots + a_n' a \otimes b_n \big) \\
&= (aa_2' - a_2' a) \otimes b_2 + \cdots + (aa_n' - a_n' a) \otimes b_n
\end{aligned}$$

is in I. Because the length n of x was minimal, $(a \otimes 1)y - y(a \otimes 1) = 0$. Because $b_1, \dots, b_n$ are k-linearly independent in B, it follows that $1 \otimes b_1, \dots, 1 \otimes b_n$ are A-linearly independent in $A \otimes_k B$. It follows that $aa'_i = a'_i a$ for all $a \in A$ and all $2 \le i \le n$. That is to say, each a'_i is in $Z(A) = k$. In that case we can write

$$\begin{aligned} y &= 1 \otimes b_1 + 1 \otimes a'_2 b_2 + \cdots + 1 \otimes a'_n b_n \\ &= 1 \otimes (b_1 + a'_2 b_2 + \cdots + a'_n b_n) \\ &= 1 \otimes b \end{aligned}$$

where b is nonzero because $b_1 \neq 0$ and the set $\{b_i\}$ is k-linearly independent. Since B is simple, there exist $u_1, \dots, u_p, v_1, \dots, v_p \in B$ such that $\sum_j u_j b v_j = 1$. Now $y = 1 \otimes b$ is in the ideal I, so

$$\sum_j \big((1 \otimes u_j)(1 \otimes b)(1 \otimes v_j)\big) = 1 \otimes \sum_j u_j b v_j = 1 \otimes 1$$

is in I. This shows $I = A \otimes_k B$.

(2): It is easy to see that $1 \otimes_k Z(B) \subseteq Z(A \otimes_k B)$. Let $x \in Z(A \otimes_k B)$. Assume $x \neq 0$ and write $x = \sum_{i=1}^n a_i \otimes b_i$ where we assume $b_1, \dots, b_n$ are linearly independent over k. For each $a \in A$ we have

$$\begin{aligned} 0 &= (a \otimes 1)x - x(a \otimes 1) \\ &= aa_1 \otimes b_1 + \cdots + aa_n \otimes b_n - (a_1 a \otimes b_1 + \cdots + a_n a \otimes b_n) \\ &= (aa_1 - a_1 a) \otimes b_1 + \cdots + (aa_n - a_n a) \otimes b_n \end{aligned}$$

Since $1 \otimes b_i$ are A-linearly independent in $A \otimes_k B$, we conclude that $aa_i = a_i a$ for each i. That is, each a_i is in $Z(A) = k$. Therefore, $x = 1 \otimes b$. It is now easy to verify that $b \in Z(B)$. □

COROLLARY 4.4.10. *Let k be a field and A a central simple k-algebra. Then* $\dim_k(A) = n^2$ *for some* $n \ge 1$.

PROOF. Let K be an algebraic closure of k. By Theorem 4.4.9, $A \otimes_k K$ is a central simple K-algebra. By Proposition 4.4.8, $A \otimes_k K$ is isomorphic to $M_n(K)$, for some $n \ge 1$. By Theorem 2.3.23, $\dim_k(A) = \dim_K(A \otimes_k K) = n^2$. □

4.2. Exercises.

EXERCISE 4.4.1. Let k be a field and A a finite dimensional k-algebra. Let N be a nilpotent left ideal of A such that $\dim_k(N) \le 2$. Prove that N is commutative. That is, $xy = yx$ for all x and y in N.

EXERCISE 4.4.2. Let k be a field and let A be the subset of $M_2(k)$ consisting of all matrices of the form $\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right)$ where a, b, c are in k.

(1) Show that A is a k-subalgebra of $M_2(k)$, and $\dim_k(A) = 3$.
(2) Show that A is noncommutative.
(3) Let I_1 be the set of all matrices of the form $\left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right)$. Show that I_1 is a maximal left ideal of A and $I = Ae_1$ for an idempotent e_1.
(4) Let I_2 be the set of all matrices of the form $\left(\begin{smallmatrix} 0 & 0 \\ b & c \end{smallmatrix}\right)$. Show that I_2 is a maximal left ideal of A. Show that I_2 is not an A-module direct summand of A.
(5) Determine the Jacobson radical $\mathrm{J}(A)$ and show that A is not semisimple.
(6) Classify $A/\mathrm{J}(A)$ in the manner of Exercise 1.8.1.

EXERCISE 4.4.3. Let k be a field. Let A be the k-subspace of $M_3(k)$ spanned by $1, \alpha, \beta$, where

$$\alpha = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \beta = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

(1) Show that A is a k-subalgebra of $M_3(k)$, and $\dim_k(A) = 3$.
(2) Show that A is commutative if and only if $\operatorname{char} k = 2$.
(3) Determine the Jacobson radical $\mathrm{J}(A)$ and show that A is not semisimple.
(4) Classify $A/\mathrm{J}(A)$ in the manner of Exercise 1.8.1.

EXERCISE 4.4.4. Let k be a field. Let A be the k-subspace of $M_3(k)$ spanned by $1, \alpha, \beta$, where

$$\alpha = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \beta = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

(1) Show that A is a k-subalgebra of $M_3(k)$, and $\dim_k(A) = 3$.
(2) Show that A is noncommutative.
(3) Determine the Jacobson radical $\mathrm{J}(A)$ and show that A is not semisimple.
(4) Classify $A/\mathrm{J}(A)$ in the manner of Exercise 1.8.1.

EXERCISE 4.4.5. Let k be a field and $n \geq 1$. Prove:

(1) Every finitely generated left $M_n(k)$-module is free.
(2) If m does not divide n, then $M_n(k)$ has no k-subalgebra isomorphic to $M_m(k)$.
(3) If $m \mid n$, then $M_n(k)$ contains a k-subalgebra which is isomorphic to $M_m(k)$.

EXERCISE 4.4.6. Let R be a ring, M an R-module and suppose $M = \bigoplus_{i \in I} M_i$ is the internal direct sum of a family of simple R-submodules, for some index set I. Prove that the following are equivalent.

(1) M is artinian.
(2) M is noetherian.
(3) I is finite.

EXERCISE 4.4.7. Let R be a semisimple ring and M an R-module. Prove that M is artinian if and only if M is noetherian.

EXERCISE 4.4.8. Prove the converse of Theorem 4.4.3 (2). That is, a finite direct sum of simple rings is a semisimple ring.

EXERCISE 4.4.9. Let k be a field and $A = M_2(k)$ the ring of all 2-by-2 matrices over k. Let I be the set of all matrices of the form $\left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right)$. Show that I is a left ideal of A. Let $\lambda : A \to \operatorname{Hom}_k(A/I, A/I)$ be the left regular representation of A (see Example 1.1.13). Show that λ is an isomorphism of rings. (Hint: Exercise 1.1.2.)

EXERCISE 4.4.10. Let k be an algebraically closed field and A a finite dimensional k-algebra. Show that if A is a simple ring, then A is isomorphic to $M_n(k)$, for some n. In particular, $\dim_k(A) = n^2$.

5. Commutative Artinian Rings

We begin by proving that any artinian ring R is noetherian. Following that result, our focus is on commutative artinian rings. It is shown that a commutative ring R is artinian if and only if R is noetherian and every prime ideal is maximal. A commutative artinian ring R decomposes into a finite direct sum of local artinian rings. As a corollary, if M is a projective R-module of constant rank r, then M is a free module of rank r.

THEOREM 4.5.1. *Let R be an artinian ring and M an R-module. If M is artinian, then M is noetherian. In particular, R is a noetherian ring.*

PROOF. Let $J = \mathrm{J}(R)$ denote the Jacobson radical of R. Then R/J is a semisimple ring, by Example 4.3.5. By Lemma 4.1.9, since M is artinian, so are the submodules J^nM and the quotient modules $J^nM/J^{n+1}M$, for all $n \geq 0$. By Exercise 1.1.1, the quotient module $J^nM/J^{n+1}M$ is artinian over R/J. By Exercise 4.4.7, $J^nM/J^{n+1}M$ is noetherian as a R/J-module. Again by Exercise 1.1.1, $J^nM/J^{n+1}M$ is noetherian as an R-module. For each $n \geq 0$, the sequence

$$0 \to J^{n+1}M \to J^nM \to \frac{J^nM}{J^{n+1}M} \to 0$$

is exact. By Corollary 4.2.6, for some r, we have $J^{r+1} = (0)$. Taking $n = r$ in the exact sequence, Lemma 4.1.9 implies J^rM is noetherian. A finite induction argument using Lemma 4.1.9 and the exact sequence proves J^nM is noetherian for $n = r, \dots, 1, 0$. □

LEMMA 4.5.2. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. If $\mathfrak{m}$ is the only prime ideal of R, then R is artinian.*

PROOF. By Lemma 3.3.7, $I(V(0)) = \mathrm{Rad}_R(0) = \mathfrak{m}$. Therefore, $\mathfrak{m}^n = (0)$, for some $n \geq 1$. Look at the filtration

$$R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots \supseteq \mathfrak{m}^{n-1} \supseteq (0).$$

Each factor $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is finitely generated as an R-module, hence is finitely generated as a vector space over the field $R/\mathfrak{m}$. By Exercise 1.1.1, the R-submodules of $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ correspond to $R/\mathfrak{m}$-subspaces. By Exercise 4.1.11, $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ satisfies DCC as an $R/\mathfrak{m}$-vector space, hence as an R-module. In particular, $\mathfrak{m}^{n-1}$ satisfies DCC as an R-module. A finite induction argument using Lemma 4.1.9 and the exact sequences

$$0 \to \mathfrak{m}^{i+1} \to \mathfrak{m}^i \to \mathfrak{m}^i/\mathfrak{m}^{i+1} \to 0$$

shows that each R-module $\mathfrak{m}^i$ has the DCC on submodules. In particular, R is artinian. □

PROPOSITION 4.5.3. *Let R be a commutative artinian ring.*

(1) Every prime ideal of R is maximal.
(2) The nil radical $\mathrm{Rad}_R(0)$ is equal to the Jacobson radical $\mathrm{J}(R)$.
(3) There are only finitely many maximal ideals in R.
(4) The nil radical $\mathrm{Rad}_R(0)$ is nilpotent.
(5) If R is simple, then R is a field. If R is semisimple, then R is a finite direct sum of fields.

PROOF. (1): Let P be a prime ideal in R. Then R/P is an artinian integral domain. By Exercise 4.1.6, R/P is a field.

(2): This is Exercise 4.5.1.

(3): Theorem 4.5.1 implies R is noetherian, and Proposition 4.1.14 implies $\operatorname{Spec} R$ has only a finite number of irreducible components. By Corollary 4.1.15, the irreducible components of $\operatorname{Spec} R$ correspond to the minimal primes of R. It follows from Part (1) that every prime ideal in R is minimal. Therefore, $\operatorname{Spec} R$ is finite.

(4): In an artinian ring the Jacobson radical is always nilpotent, by Corollary 4.2.6.

(5): This part is left to the reader. □

PROPOSITION 4.5.4. *Let R be a commutative ring. The following are equivalent.*

(1) R is artinian.
(2) R is noetherian and every prime ideal is maximal ($\dim(R) = 0$, in the notation of Section 9.6.1).
(3) R is an R-module of finite length.

PROOF. By Proposition 4.1.21, it is enough to show (1) and (2) are equivalent.

(1) implies (2): By Theorem 4.5.1, R is noetherian. By Proposition 4.5.3, every prime ideal of R is maximal.

(2) implies (1): By Theorem 4.1.16, R has a decomposition $R = R_1 \oplus \cdots \oplus R_n$ where each R_i has only two idempotents. By Exercise 4.1.1 it suffices to show each R_i is artinian. Therefore, assume $\operatorname{Spec} R$ is connected. By Proposition 1.3.7, $\operatorname{Spec} R$ decomposes into a union of a finite number of irreducible closed subsets. Each prime ideal of R is maximal, so the irreducible components of $\operatorname{Spec} R$ are closed points. Since we are assuming $\operatorname{Spec} R$ is connected, this proves R is a local ring. By Lemma 4.5.2, R is artinian. □

PROPOSITION 4.5.5. *Let R be a commutative noetherian local ring and let $\mathfrak{m}$ be the maximal ideal of R.*

(1) If $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all $n \geq 1$, then R is not artinian.
(2) If there exists $n \geq 1$ such that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, then $\mathfrak{m}^n = 0$ and R is artinian.

PROOF. (1): If R is artinian, then by Proposition 4.5.3 (4) there exists $n > 0$ such that $\mathfrak{m}^n = 0$.

(2) If $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, then by Nakayama's Lemma (Theorem 4.2.3), $\mathfrak{m}^n = 0$. If P is a prime ideal of R, then $\mathfrak{m}^n \subseteq P$. By Exercise 3.3.4, $\mathfrak{m} = \operatorname{Rad}(\mathfrak{m}^n) \subseteq \operatorname{Rad}(P) = P$. This proves that $P = \mathfrak{m}$, so by Proposition 4.5.4, R is artinian. □

THEOREM 4.5.6. *Let R be a commutative artinian ring.*

(1) $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ where each R_i is a local artinian ring.
(2) The rings R_i in Part (1) are uniquely determined up to isomorphism.
(3) If $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ is the complete list of prime ideals in $\operatorname{Spec} R$, then the natural homomorphism $R \to R_{\mathfrak{m}_1} \oplus \cdots \oplus R_{\mathfrak{m}_n}$ is an isomorphism.

PROOF. (1): By Proposition 4.5.3, $\operatorname{Max} R = \operatorname{Spec} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ is a finite set. So the topological space $\operatorname{Spec} R$ has the discrete topology. By Theorem 4.1.16, R can be written as a direct sum $R = R_1 \oplus \cdots \oplus R_r$ where $\operatorname{Spec} R_i$ is connected. Since the topology is discrete, this implies $\operatorname{Spec} R_i$ is a singleton set, hence R_i is a local ring. This also proves $n = r$.

(2): A local ring has only two idempotents, so this follows from Theorem 3.2.5.

(3): Start with the decomposition $R \cong R_1 \oplus \cdots \oplus R_n$ of Part (1) and apply Exercise 3.1.4. □

COROLLARY 4.5.7. *Let R be a commutative artinian ring. If M is a finitely generated projective R module of constant rank r, then M is a free R-module of rank r.*

PROOF. By Theorem 4.5.6, R is the finite direct sum of local rings. By Exercise 4.2.4, M is a free module of rank r. □

COROLLARY 4.5.8. *Let R be a commutative ring and S a commutative R-algebra which is finitely generated and projective as an R-module. Let M be a finitely generated projective S-module. Let $\mathfrak{p}$ be a prime ideal in $\operatorname{Spec} R$ such that $\operatorname{Rank}_{S_{\mathfrak{p}}}(M_{\mathfrak{p}}) = s$ is defined. Then*

$$\operatorname{Rank}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \operatorname{Rank}_{R_{\mathfrak{p}}}(S_{\mathfrak{p}}) \operatorname{Rank}_{S_{\mathfrak{p}}}(M_{\mathfrak{p}})$$

PROOF. Let $k = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ be the residue field of $R_{\mathfrak{p}}$. Then $S \otimes_R k$ is a finite dimensional k-algebra, hence is artinian. By Corollary 4.5.7, $M \otimes_R k = M \otimes_S (S \otimes_R k)$ is a free $S \otimes_R k$-module of constant rank s. Proposition 2.1.13 (5) applies to the trio k, $S \otimes_R k$, $M \otimes_R k$. Applying Proposition 3.4.2 we get the rank formula over the local ring $R_{\mathfrak{p}}$. □

5.1. Exercises.

EXERCISE 4.5.1. Let R be a commutative artinian ring. Prove that the Jacobson radical $\mathrm{J}(R)$ is equal to the nil radical $\mathrm{Rad}_R(0)$.

EXERCISE 4.5.2. Let R be a commutative artinian ring and M a finitely generated free R-module of rank n. Prove that the length of M is equal to $\ell(M) = n\ell(R)$.

EXERCISE 4.5.3. Let R be a commutative ring with the property that for every maximal ideal $\mathfrak{m}$ in R, $V(\mathfrak{m})$ is both open and closed in $\operatorname{Spec} R$. Prove that every prime ideal of R is maximal.

EXERCISE 4.5.4. Let R be a commutative noetherian ring. Recall that a topological space has the discrete topology if "points are open". Prove that the following are equivalent.

(1) R is artinian.
(2) $\operatorname{Spec} R$ is discrete and finite.
(3) $\operatorname{Spec} R$ is discrete.
(4) For each maximal ideal $\mathfrak{m}$ in $\operatorname{Max} R$, the singleton set $\{\mathfrak{m}\}$ is both open and closed in $\operatorname{Spec} R$.

EXERCISE 4.5.5. Let $k_1, \dots, k_m$ be fields and $R = k_1 \oplus \cdots \oplus k_m$. Show that R has exactly m maximal ideals. Prove that if $\sigma_i : R \to k_i$ is the ring homomorphism onto k_i and $\mathfrak{m}_i$ the kernel of σ_i, then the maximal ideals of R are $\mathfrak{m}_1, \dots, \mathfrak{m}_m$.

EXERCISE 4.5.6. Let R be a commutative noetherian semilocal ring. Let I be an ideal which is contained in the Jacobson radical, $I \subseteq \mathrm{J}(R)$. Prove that the following are equivalent.

(1) There exists $\nu > 0$ such that $\mathrm{J}(R)^\nu \subseteq I \subseteq \mathrm{J}(R)$.
(2) R/I is artinian.

EXERCISE 4.5.7. Let R be a commutative noetherian ring, $\mathfrak{m}$ a maximal ideal in R, and $n \geq 1$.

(1) Prove that $R/\mathfrak{m}^n$ is a local artinian ring.
(2) Prove that the natural map $R/\mathfrak{m}^n \to R_\mathfrak{m}/\mathfrak{m}^n R_\mathfrak{m}$ is an isomorphism.

EXERCISE 4.5.8. Let k be a field and $R = k[x_1, \dots, x_n]$. Let $\alpha_1, \dots, \alpha_n$ be elements of k and $\mathfrak{m}$ the ideal in R generated by $x_1 - \alpha_1, \dots, x_n - \alpha_n$.

(1) Show that $\mathfrak{m}$ is a maximal ideal, and the natural map $k \to R/\mathfrak{m}$ is an isomorphism.
(2) Show that $\mathfrak{m}/\mathfrak{m}^2$ is a k-vector space of dimension n.
(3) Show that $\mathfrak{m}R_\mathfrak{m}/\mathfrak{m}^2 R_\mathfrak{m}$ is a k-vector space of dimension n.

EXERCISE 4.5.9. Let k be an algebraically closed field. Show that if A and B are local artinian k-algebras, then $A \otimes_k B$ is a local artinian k-algebra.

EXERCISE 4.5.10. Let k be a field and $R = k[x,y]/(x^n, y^m)$, where $m, n \in \mathbb{N}$. Show that R is a local k-algebra with maximal ideal $\mathfrak{m} = (x,y)$. Show that $\dim_k(R) = nm$.

EXERCISE 4.5.11. Let $R = (\mathbb{Z}/4)[x]/(x^4 + 1)$.

(1) Show that R is a local ring.
(2) Show that the maximal ideal of R is the principal ideal $\mathfrak{m} = (x+1)$.

EXERCISE 4.5.12. Let $f : R \to S$ be a homomorphism of commutative rings and assume S is finitely generated as an R-module. Let $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ be the continuous map of Exercise 3.3.3. For each $P \in \operatorname{Spec} R$, show that the set $(f^\sharp)^{-1}(P)$ is finite. In other words, show that there are only finitely many $Q \in \operatorname{Spec} S$ such that $f^{-1}(Q) = P$. (Hint: Exercise 3.4.3.)

EXERCISE 4.5.13. Let R be a commutative artinian ring. Show that every element of R is either a unit or a zero divisor.

6. Examples

This section is devoted to applications and examples. First we apply the results from the previous sections to study algebras which are three dimensional over a field. Let k be a field and A a k-algebra such that $\dim_k(A) = 3$. We show that if A is semisimple, then either A is a field extension of k, or the direct sum of field extensions of k. If A is noncommutative, then we show that A is isomorphic to the subring of $M_2(k)$ consisting of lower triangular matrices. If A is a commutative local ring, then there are two possibilities for A, depending on whether the Jacobson radical $\mathrm{J}(A)$ contains an element with index of nilpotency greater than 2. The last case is when A is the direct sum of a local ring of dimension two and a copy of k. Our second application is a classification of all finite rings of order p^3, where p is a prime number. Most of the cases that arise in this context fall under the hypotheses of an algebra of dimension three over the finite field $\mathbb{F}_p$. In particular, there is exactly one case where the ring A is noncommutative. In the computation of this example, most of the work is spent on the case where A is a finite ring of order p^3 and characteristic p^2. We show that such a ring A is a commutative $\mathbb{Z}/p^2$-algebra. If $p = 2$, then up to isomorphism there are three distinct possibilities for A, but if p is odd, there are four.

6.1. Three Dimensional Algebras.

6.1. Three Dimensional Algebras. Let k be a field. We apply the results of the previous sections to classify up to isomorphism all three dimensional k-algebras. First we review in Example 4.6.1 below the classification of k-algebras A such that $\dim_k(A) = 2$.

EXAMPLE 4.6.1. Let k be a field and A a finite dimensional k-algebra such that $\dim_k(A) = 2$. By Exercises 1.8.1 and 1.8.2, A is a commutative simple extension of k and there are three possibilities for A. Either A is a field extension of k or A is isomorphic as a k-algebra to a direct sum $k \oplus k$ of two copies of k, or to the local ring $k[x]/(x^2)$.

THEOREM 4.6.2. *Let k be a field and A a finite dimensional k-algebra. If $\dim_k(A) = 3$, then exactly one of the following is true.*

(1) A is a field extension of k of degree 3. A is a simple ring.
(2) A is isomorphic to $k \oplus F$, a direct sum of k and a field extension F/k of degree 2. A is semisimple but not simple.
(3) A is isomorphic to $k \oplus k \oplus k$, a direct sum of three copies of k. In this case, A is semisimple.
(4) A is isomorphic to $\left\{ \begin{bmatrix} x & 0 & 0 \\ y & x & 0 \\ z & 0 & x \end{bmatrix} \mid x, y, z \in k \right\}$*, a subring of the ring of matrices $M_3(k)$, a commutative local ring. If $J = \mathrm{J}(A)$, then $\dim_k(J) = 2$ and $J^2 = (0)$. By Exercise 4.6.1, this ring is isomorphic to the ring $R = k[x,y]/(x^2, xy, y^2)$.*

(5) A is isomorphic to $\left\{ \begin{bmatrix} x & 0 & 0 \\ y & x & 0 \\ z & y & x \end{bmatrix} \mid x,y,z \in k \right\}$*, a subring of the ring of matrices* $M_3(\mathbb{F}_2)$*, a commutative local ring. If* $J = \mathrm{J}(A)$*, then* $\dim_k(J) = 2$ *and* $\dim_k(J^2) = 1$*. There is an element* $u \in J$ *such that* $u^2 \neq 0$*,* $u^3 = 0$*. By Exercise 4.6.2, this ring is isomorphic to the ring* $R = k[x,y]/(x^2 - y, xy, y^2)$*.*

(6) A is isomorphic to $k \oplus k[x]/(x^2)$*, a commutative ring, the Jacobson radical is the principal ideal generated by the ordered pair* $(0,x)$*.*

(7) A is isomorphic to $\left\{ \begin{bmatrix} x & 0 \\ y & z \end{bmatrix} \mid x,y,z \in k \right\}$*, which is a subring of the ring of matrices* $M_2(k)$*, a noncommutative ring. The Jacobson radical is the principal ideal generated by* $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$*. This is the ring of Exercise 4.4.2.*

A finite dimensional k-algebra A is artinian (Exercise 4.1.13). By Corollary 4.2.6, $\mathrm{J}(A)$ is a nilpotent ideal. It follows that every element of $\mathrm{J}(A)$ is nilpotent.

For the remainder of this section, we will use the notation Ring (1), ..., Ring (7) to refer to the seven rings of Theorem 4.6.2. The proof is divided into a series of lemmas.

LEMMA 4.6.3. *Let k be a field and A a finite dimensional k-algebra such that* $\dim_k(A) = 3$.

(1) If $\mathrm{J}(A) = (0)$*, then A is either a field, or a direct sum of fields. Hence A is either a direct sum* $k \oplus k \oplus k$ *of three copies of k, or a direct sum* $k \oplus F$*, where F is a quadratic extension field of k, or A is an extension field of k with degree* 3*. In this case A is isomorphic to exactly one of the rings (1), (2) or (3) of Theorem 4.6.2.*

(2) If $\dim_k \mathrm{J}(A) = 1$*, then* $A/\mathrm{J}(A) \cong k \oplus k$*. In this case, A contains exactly two maximal ideals* $\mathfrak{m}_1$ *and* $\mathfrak{m}_2$*, where* $\dim_k \mathfrak{m}_i = 2$ *and* $\mathrm{J}(A) = \mathfrak{m}_1 \cap \mathfrak{m}_2$*.*

(3) If $\dim_k \mathrm{J}(A) = 2$*, then* $A/\mathrm{J}(A) \cong k$*.*

PROOF. (1): Since A is semisimple, A is a direct sum of simple rings. By Theorem 4.4.5, a simple ring is a ring of matrices over a division ring. Since $\dim_k(A) = 3$, a simple k-algebra is necessarily a division ring D such that $\dim_k(D) = 3$. By Corollary 4.4.10, the dimension of D over the center $Z(D)$ is a square. If D is a simple ring that is a direct summand of A, then $D = Z(D)$, hence D is a field.

(2): By Exercise 2.5.4, if $\mathrm{J}(A)$ has dimension one, then A contains a maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \cong k$. By Corollary 4.2.7 (1), $\mathrm{J}(A)$ is contained in $\mathfrak{m}$. By Proposition 1.5.3, $A/\mathrm{J}(A)$ is not simple. By Example 4.6.1, $A/\mathrm{J}(A)$ is isomorphic to the ring $k \oplus k$. By Exercise 4.5.5, $A/\mathrm{J}(A)$ has exactly two maximal ideals, hence, so does A.

(3): In this case, $A/\mathrm{J}(A)$ is a k-algebra of dimension 1. □

The classification of algebras A such that $\mathrm{J}(A)$ has dimension 2 over k will utilize the following result on two-by-two nilpotent matrices.

LEMMA 4.6.4. *Let k be a field and* $M_2(k)$ *the ring of two-by-two matrices over k. Let U and V be nonzero nilpotent matrices in* $M_2(k)$*. The following are equivalent.*

(1) $\ker U = \ker V$.

(2) $\operatorname{im} U = \operatorname{im} V$.

(3) $U = sV$ *for some* $s \in k^*$.

(4) For every pair $(s,t) \in k^2$*, the matrix* $sU + tV$ *is singular.*

PROOF. (1) and (2) are equivalent: Since U and V are nonzero nilpotent matrices in $M_2(k)$, $\ker U = \operatorname{im} U$ and $\ker V = \operatorname{im} V$.

(1) and (2) imply (3): Let u be an eigenvector for U. If $u_1 \in k^2 - \ker U$, then $B = \{u, u_1\}$ is a basis for k^2. We have $Uu_1 = su$ for some $s \in k^*$. Likewise, since $\ker U = \ker V$, $Vu_1 = tu$ for some $t \in k^*$. On the basis B, we have $tU = sV$. This proves $U = t^{-1}sV$.

(3) implies (4): Say $s \in k^*$ and $U = sV$. For contradiction's sake, assume $aU + bV$ is nonsingular, where $(a,b) \in k^2$. Substituting, $aU + bV = asV + bV = (as+b)V$ is nonsingular. But $(as+b)V$ has rank less than or equal to one, hence is singular.

(4) implies (1): Suppose $\ker U \neq \ker V$. Let u be an eigenvector for U and v an eigenvector for V. Then $B = \{u, v\}$ is a basis for k^2. By the proof of (1) and (2) implies (3), there exist a, b in k^* such that $Uv = au$ and $Vu = bv$. On the basis B, we have $(U+V)(U+V)u = (U+V)bv = abu$ and $(U+V)(U+V)v = (U+V)au = abv$. This proves $U+V$ is invertible and $(U+V)^{-1} = (ab)^{-1}(U+V)$. □

LEMMA 4.6.5. *Let k be a field and A a finite dimensional k-algebra such that* $\dim_k(A) = 3$. *If $J = \mathrm{J}(A)$ and* $\dim_k(J) = 2$*, then A is isomorphic to exactly one of the two rings (4) or (5) of Theorem 4.6.2.*

PROOF. Let $\{u, v\}$ be a k-basis for J. Then u and v are nilpotent. Let $\lambda : A \to \operatorname{Hom}_k(J,J)$ be the left regular representation of A (Example 1.1.13). The image of A under λ is a k-subalgebra $S = \operatorname{im}\lambda$ of $\operatorname{Hom}_k(J,J)$. The endomorphism ring $\operatorname{Hom}_k(J,J)$ and the ring of matrices $M_2(k)$ are isomorphic as k-algebras. The image of J under λ consists of nilpotent matrices. By Lemma 4.6.4, $\dim_k \lambda(J) \leq 1$. Therefore, the kernel of $\lambda : J \to \operatorname{Hom}_k(J,J)$ is not equal to (0). In other words, there exists $w \in J - (0)$ such that $0 = wu = uw = wv = vw = w^2$. We split the rest of the proof into two cases.

Case 1: $\lambda(J) \neq (0)$. Since $\dim_k(J) = 2$ and $\lambda(J) \cong J/(\ker(\lambda) \cap J)$, this means $\ker(\lambda) \cap J = kw$ has dimension one. Then there exists some $u \in J$ such that $u \notin \operatorname{annih}_R(J)$. Thus, $u \notin kw$. Since $\lambda(u)^2 = 0$, we have $u^2 \in kw$. Hence $u^2 = aw$, for some $a \in k$. A basis for J over k is $\{u, w\}$. With respect to this basis, the matrix for $\lambda(u)$ is $\begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix}$. Since $\lambda(u) \neq 0$, this implies $a \neq 0$. Define a k-linear transformation $f : A \to M_3(k)$ on the basis $\{1, u, aw\}$ by

$$f(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad f(u) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad f(aw) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

It is routine to check that f maps the ring A isomorphically onto Ring (5).

Case 2: $\lambda(J) = (0)$. We have $J \subseteq \operatorname{annih}_R(J)$, thus $J^2 = (0)$. As above, a basis for A over k is $\{1, u, v\}$, where $J = ku + kv$. On this basis we define a k-linear transformation $f : A \to M_3(k)$ by

$$f(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad f(u) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad f(v) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

It is routine to check that f maps the ring A isomorphically onto Ring (4). □

LEMMA 4.6.6. *Let k be a field and A a finite dimensional k-algebra such that* $\dim_k(A) = 3$. *If $J = \mathrm{J}(A)$ and* $\dim_k(J) = 1$*, then A is isomorphic to exactly one of the two rings (6) or (7) of Theorem 4.6.2.*

PROOF. Let $v \in J - (0)$. Then $J = kv$. By Lemma 4.6.3, A/J is isomorphic to $k \oplus k$. By Corollary 4.2.8 (2), lift one of the nontrivial idempotents of A/J to an idempotent $e \in A$. Then $\{1, e, v\}$ is a basis for A as a k-vector space. Let $\lambda : A \to \operatorname{Hom}_k(J,J)$ be the left regular representation. The ring $\operatorname{Hom}_k(J,J)$ is isomorphic to the field k, hence has only two idempotents. Therefore, either $\lambda(e)=0$, or $\lambda(e)=1$. Thus ev is either 0 or v. Likewise, ve is either 0 or v. There are four mutually exclusive cases.

Case 1: $ev=ve=0$. Then $A=k1+ke+kv$ is clearly a commutative ring and A is the internal direct sum $A=Ae\oplus A(1-e)$. So $Ae=ke$ is isomorphic as a ring to k by the assignment $e\mapsto 1$. Moreover, $v(1-e)=v$, $(1-e)v=v$. The assignment $1-e\mapsto 1$ and $v\mapsto x$ induces an isomorphism of rings from $A(1-e)=k(1-e)+kv$ to $k[x]/(x^2)$. Hence, A is isomorphic to Ring (6).

Case 2: $ev=ve=v$. Then $(1-e)v=0$, $v(1-e)=0$. It follows at once that this is Case 1, with the roles of e and $1-e$ reversed. Hence, A is isomorphic to Ring (6).

Case 3: $ev=0$ and $ve=v$. Then $(1-e)v=v$ and $v(1-e)=0$. On the basis $\{1,e,v\}$ define a k-linear transformation $\phi : A\to M_2(k)$:

$$\phi(1)=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad \phi(v)=\begin{bmatrix}0&0\\1&0\end{bmatrix},\quad \phi(e)=\begin{bmatrix}1&0\\1&0\end{bmatrix}.$$

It is routine to check that $\phi(e)\phi(v)=0$, $\phi(v)\phi(e)=\phi(v)$ and that ϕ maps A isomorphically onto Ring (7).

Case 4: $ev=v$, $ve=0$. With the roles of e and $1-e$ reversed, this is Case 3. The ring A is isomorphic to Ring (7).

□

6.2. Finite Rings of Order p^3**.** Throughout this section p is a fixed prime number. The goal of this section is to classify in a systematic way all finite rings of order p^3. In Theorem 4.6.8 we show that if p is odd, then up to isomorphism there are twelve different rings of order p^3. If $p=2$, we show that there are eleven different rings of order eight.

EXAMPLE 4.6.7. We know from [**19**, Exercise 5.5.26] that up to isomorphism there are exactly four different rings of order p^2.

(1) $\mathbb{Z}/p^2$. This ring has order p^2 and characteristic p^2.
(2) $(\mathbb{Z}/p)[x]/(x^2)$. This ring has order p^2, characteristic p, is a local ring, and has nontrivial Jacobson radical.
(3) $\mathbb{Z}/p\oplus\mathbb{Z}/p$. This ring has order p^2, characteristic p, trivial Jacobson radical, and is not a field.
(4) $\mathbb{F}_{p^2}$, the unique field of order p^2, which exists by Theorem 1.8.7.

THEOREM 4.6.8. *Let R be a finite ring of order p^3. Then R is isomorphic to exactly one of the following rings.*

(1) $\mathbb{Z}/p^3$, the ring of integers modulo p^3, a local ring with characteristic p^3. The Jacobson radical is $\{0,p,2p,\dots,(p-1)p\}$, which has order p^2.
(2) $\mathbb{F}_{p^3}$, the field of order p^3 and characteristic p, a simple ring.
(3) $\mathbb{F}_{p^2}\oplus\mathbb{F}_p$, the direct sum of the field of order p^2 and the field of order p. The characteristic is p. This is a semisimple ring which is not simple.
(4) $\mathbb{F}_p\oplus\mathbb{F}_p\oplus\mathbb{F}_p$, the direct sum of three copies of the field of order p. The characteristic is p. This is a semisimple ring which is not simple.
(5) $\left\{\begin{bmatrix}x&0&0\\y&x&0\\z&0&x\end{bmatrix}\mid x,y,z\in\mathbb{F}_p\right\}$, a subring of the ring of matrices $M_3(\mathbb{F}_p)$, a commutative local ring with characteristic p. The Jacobson radical, J, has order p^2, and $J^2=(0)$. By Exercise 4.6.1, this ring is isomorphic to the ring $R=\mathbb{F}_p[x,y]/(x^2,xy,y^2)$.

(6) $\left\{ \begin{bmatrix} x & 0 & 0 \\ y & x & 0 \\ z & y & x \end{bmatrix} \mid x,y,z \in \mathbb{F}_p \right\}$*, a subring of the ring of matrices* $M_3(\mathbb{F}_p)$*, a commutative local ring with characteristic* p*. The Jacobson radical,* J*, has order four, and* J^2 *has order two. There is an element* $b \in J$ *such that* $b^2 \neq 0$*,* $b^3 = 0$*. By Exercise 4.6.2, this ring is isomorphic to the ring* $R = \mathbb{F}_p[x,y]/(x^2 - y, xy, y^2)$*.*

(7) $\mathbb{F}_p \oplus \mathbb{F}_p[x]/(x^2)$*, a commutative ring with characteristic* p*. The Jacobson radical is the principal ideal generated by the ordered pair* $(0,x)$*.*

(8) $\left\{ \begin{bmatrix} x & 0 \\ y & z \end{bmatrix} \mid x,y,z \in \mathbb{F}_p \right\}$*, which is a subring of the ring of matrices* $M_2(\mathbb{F}_p)$*, a noncommutative ring with characteristic* p*. The Jacobson radical is the principal ideal generated by* $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$*.*

(9) $\mathbb{Z}/p^2 \oplus \mathbb{Z}/p$*, the direct sum of the local ring* $\mathbb{Z}/p^2$ *and the field* $\mathbb{Z}/p$*, the Jacobson radical is* $\{0, p, 2p, \dots, (p-1)p\}$*, the characteristic is* p^2*.*

(10) $\mathbb{Z}/p^2[x]/(px, x^2)$*, the polynomial ring* $\mathbb{Z}/p^2[x]$ *modulo the ideal* (px, x^2)*, a local ring with characteristic* p^2*. The maximal ideal* $\mathfrak{m}$ *is generated by* $\{p, x\}$*, where* $pv = 0$*,* $x^2 = 0$*, and* $\mathfrak{m}^2 = (0)$*. The additive group* $(\mathfrak{m}, +)$ *is an elementary* p*-group of order* p^2*.*

(11) $\mathbb{Z}/p^2[x]/(px, x^2 - p)$*, the polynomial ring* $\mathbb{Z}/p^2[x]$ *modulo the ideal* $(px, x^2 - p)$*, a local ring with characteristic* p^2*. The maximal ideal* $\mathfrak{m}$ *is principal, generated by* $\{x\}$*, where* $pv = 0$*,* $x^2 = p$*, and* $\mathfrak{m}^2 = \{0, p, 2p, \dots, (p-1)p\}$*. The additive group* $(\mathfrak{m}, +)$ *is an elementary* p*-group of order* p^2*.*

(12) This case does not occur if $p = 2$*.* $\mathbb{Z}/p^2[x]/(px, x^2 - ap)$*, the polynomial ring* $\mathbb{Z}/p^2[x]$ *modulo the ideal* $(px, x^2 - ap)$*,* a *is any quadratic nonresidue modulo* p*. A local ring with characteristic* p^2*, the maximal ideal* $\mathfrak{m}$ *is principal, generated by* $\{x\}$*, where* $pv = 0$*,* $x^2 = ap$*, and* $\mathfrak{m}^2 = \{0, p, 2p, \dots, (p-1)p\}$*. The additive group* $(\mathfrak{m}, +)$ *is an elementary* p*-group of order* p^2*. In this ring* p *is not a square.*

For the remainder of this section, we will use the notation Ring (1), …, Ring (12) to refer to the twelve rings of Theorem 4.6.8. Rings (2) – (8) all have characteristic p and these seven fall under the hypotheses of Theorem 4.6.2. The only ring of order p^3 that has characteristic p^3 is $\mathbb{Z}/p^3$, which is Ring (1). To complete the proof of Theorem 4.6.8, it suffices to classify all rings of order p^3 that have characteristic p^2. The rings of characteristic p^2 in Theorem 4.6.8 are Rings (9) – (12). We show in Lemma 4.6.12 below that if p is odd, then a ring A of order p^3 and characteristic p^2 is isomorphic to exactly one of the Rings (9) – (12). If $p = 2$, then we show A is isomorphic to one of the Rings (9) – (11).

For the rest of this section, A denotes a finite ring of order p^3, characteristic p^2, and C denotes the image of the natural map $\mathbb{Z} \to A$. So C is isomorphic to $\mathbb{Z}/p^2$. If M is an additive abelian group, then in Lemma 4.6.9 below, $\lambda_p : M \to M$ is the "multiplication by p" map. We write pM for the image and $M(p)$ for the kernel of λ_p.

LEMMA 4.6.9. *Let* A *be a finite ring of order* p^3 *and characteristic* p^2*. Let* C *be the canonical subring of order* p^2*, the image of the natural map* $\mathbb{Z} \to A$*.*

(1) A *is a commutative ring and generated as a* C*-algebra by any element* $v \in A - C$*.*

(2) The abelian group $(A, +)$ *is isomorphic to* $\mathbb{Z}/p^2 \oplus \mathbb{Z}/p$*.*

(3) Denote by $A(p)$ *the subgroup of* $(A, +)$ *annihilated by* p*. Then* $A(p)$ *is isomorphic to* $\mathbb{Z}/p \oplus \mathbb{Z}/p$*.*

(4) Denote by pA the ideal generated by p. Then pA is equal to the ideal pC and has order p.

PROOF. (1): Since C is central, given any $v \in A - C$, the assignment $x \mapsto v$ defines an evaluation homomorphism $C[x] \to A$. The image is the commutative subring $C[v]$. The index of $(C,+)$ in $(A,+)$ is prime. By Lagrange's Theorem, Theorem 1.1.1, the order of $C[v]$ is necessarily p^3.

(2): This follows from the Basis Theorem for Finite Abelian Groups (Theorem 1.7.16), since $(A,+)$ has order p^3 and exponent p^2.

(3) and (4): These follow immediately from (2). Notice that the ideal pC is actually an A-module contained in C and is equal to $C : A$, the conductor from A to C (see Exercise 1.1.8). □

LEMMA 4.6.10. *If A is a finite ring of order p^3 and characteristic p^2, then exactly one of the following is true.*

(1) A is a local ring.
(2) A is isomorphic to $\mathbb{Z}/p^2 \oplus \mathbb{Z}/p$.

PROOF. By Lemma 4.6.9, A is commutative. Since A is finite, A is artinian. By Theorem 4.5.6, A is a direct sum of local artinian rings. If A is not a local ring, then $A = A_1 \oplus A_2$. Since A has characteristic p^2, either A_1 or A_2 has characteristic p^2 and the other has order p. By Example 4.6.7, one of the direct summands is isomorphic to $\mathbb{Z}/p^2$ and the other is isomorphic to $\mathbb{Z}/p$. □

In Lemma 4.6.11 (4), we denote by U_p the group of units modulo p. The homomorphism $\pi^2 : U_p \to U_p$ is defined by $u \mapsto u^2$. We write U_p^2 for the image of π^2. Since U_p is a cyclic group of order $p-1$ (Theorem 1.8.7), it follows that $[U_p : U_p^2] = 2$, if p is odd.

LEMMA 4.6.11. *Let p be an odd prime number and i an integer such that* $\gcd(i,p) = 1$. *Consider the quotient ring*

$$A_i = \mathbb{Z}/p^2[x]/(px, x^2 - ip).$$

In the following, cosets in the ring A_i are written without brackets or any extra adornment.

(1) A_i is a local ring of order p^3 and characteristic p^2. The Jacobson radical $J = \mathrm{J}(A_i)$ is equal to the principal ideal (x) and $(J,+)$ is an elementary p-group of order p^2.
(2) J^2 is equal to the principal ideal (p), which has order p.
(3) The set $\{\alpha^2 \mid \alpha \in J\}$ is equal to the subset $\{u^2 ip \mid u \in \mathbb{Z}\}$ of (p) and has order $(p+1)/2$.
(4) If j is an integer such that $\gcd(j,p) = 1$, then the rings A_i and A_j are isomorphic if and only if the cosets of i and j in the factor group U_p/U_p^2 are equal.

PROOF. (1) and (2): This is Exercise 4.6.3.

(3): Since $J^2 = (p)$, the set $\{\alpha^2 \mid \alpha \in J\}$ is a subset of (p). The additive group $(J,+)$ is an elementary p-group of rank 2, and $\{p,x\}$ is a basis. A typical element $\alpha \in J$ is of the form $\alpha = ux + vp$, where u and v are integers. Since $px = 0$, $p^2 = 0$, and $x^2 = ip$, we have $\alpha^2 = u^2 ip$. If $p \mid u$, then $\alpha^2 = 0$. If $\gcd(u,p) = 1$, then $u^2 i$ is in the coset of i in U_p/U_p^2. Since $[U_p : U_p^2] = 2$, this implies there are $(p-1)/2 + 1 = (p+1)/2$ squares α^2 in J.

(4): If i and j are not congruent modulo U_p^2, then by (3), the rings A_i and A_j are not isomorphic. Conversely, assume $i = ju^2 + kp$ for some integers u and k such that $\gcd(u,p) = 1$. Define $\phi : A_i \to A_j$ by $\phi(x) = ux$. Note that $\phi(x^2 - ip) = (ux)^2 - ip =$

$u^2jp - ip = (i-kp)p - ip = 0$. From this it is routine to check that ϕ is well defined, and ϕ is an isomorphism. $\square$

LEMMA 4.6.12. *Let A be a finite ring of order p^3 and characteristic p^2. If $p = 2$, then A is isomorphic to exactly one of the Rings (9), (10), or (11) of Theorem 4.6.8. If p is odd, then A is isomorphic to exactly one of the Rings (9), (10), (11), or (12).*

PROOF. By Lemma 4.6.10, if A is not a local ring, then A is isomorphic to Ring (9). Assume from now on that A is a local ring with maximal ideal $J = \mathrm{J}(A)$. By Lemma 4.6.9, $A(p)$ is a maximal ideal. Therefore, $J = A(p)$. Then $(J,+)$ is an elementary p-group of order p^2. Let $v \in J - (p)$. By Lemma 4.6.9, a basis for $(J,+)$ is the set $\{p, v\}$, and A is generated as a C-algebra by v. By Corollary 4.2.6, either $J^2 = (0)$, or $J^2 = (p)$. We now consider these two mutually exclusive cases.

Case 1: Assume $J^2 = (0)$. Then $v^2 = 0$. Define a homomorphism from Ring (10) to A by the assignment $x \mapsto v$. It is immediate that this is an isomorphism.

Case 2: Assume $J^2 = (p)$. Then $v^2 = ip$ for some integer i such that $\gcd(i, p) = 1$. As in Lemma 4.6.11, let $A_i = \mathbb{Z}/p^2[x]/(px, x^2 - ip)$. Define a homomorphism from A_i to A by the assignment $x \mapsto v$. It is immediate that this is an isomorphism. If $p = 2$, then $(p) = \{0, p\}$. In this case there is only one choice for i, and A is isomorphic to Ring (11). If p is odd, then by Lemma 4.6.11, A is isomorphic to exactly one of Ring (11) or (12). $\square$

6.3. Exercises.

EXERCISE 4.6.1. Let k be a field and $k[x,y]$ the polynomial ring over k in two variables. Consider the quotient ring $R = k[x,y]/(x^2, xy, y^2)$. In the following, cosets in the ring R are written without brackets or any extra adornment. Prove:

(1) R is a local ring with maximal ideal $\mathfrak{m} = Rx + Ry$.
(2) R has Krull dimension 0.
(3) $\dim_k(R) = 3$. (Hint: a basis for R over k is $1, x, y$.)
(4) R is isomorphic to the subring $\left\{ \begin{bmatrix} \alpha & 0 & 0 \\ \beta & \alpha & 0 \\ \gamma & 0 & \alpha \end{bmatrix} \mid \alpha, \beta, \gamma \in k \right\}$ of $M_3(k)$. (Hints: map x to $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, and y to $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.)

EXERCISE 4.6.2. Let k be a field and $k[x,y]$ the polynomial ring over k in two variables. Consider the quotient ring $R = k[x,y]/(x^2 - y, xy, y^2)$. In the following, cosets in the ring R are written without brackets or any extra adornment. Prove:

(1) R is a local ring with maximal ideal $\mathfrak{m} = Rx + Ry$.
(2) R has Krull dimension 0.
(3) $\dim_k(R) = 3$. (Hint: a basis for R over k is $1, x, y$.)
(4) R is isomorphic to the subring $\left\{ \begin{bmatrix} \alpha & 0 & 0 \\ \beta & \alpha & 0 \\ \gamma & \beta & \alpha \end{bmatrix} \mid \alpha, \beta, \gamma \in k \right\}$ of $M_3(k)$. (Hints: map x to $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, and y to $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.)

EXERCISE 4.6.3. Let p be a prime number and i an integer such that $\gcd(i, p) = 1$. Consider the quotient ring $R = \mathbb{Z}/p^2[x]/(px, x^2 - ip)$. In the following, cosets in the ring R are written without brackets or any extra adornment. Prove:

(1) R has order p^3 and characteristic p^2.
(2) Denote by (x) the principal ideal generated by x. Then (x) has order p^2 and (x) is equal to $\operatorname{Rad}_R(0)$, the nil radical of R.
(3) R is a local ring, the maximal ideal is (x).
(4) The ideals (x^2) and (p) are equal and they both have order p.
(5) Find the invariants of the finite abelian groups $(R,+)$ and $(Rx,+)$. That is, find the elementary divisors (Theorem 1.7.16).

CHAPTER 5

Separable Algebras, Definition and First Properties

This chapter is an introduction to the theory of separable algebras over commutative rings. Most of the material in this chapter appears in [**18**, Chapter 4]. In Section 5.1 we have the definition of a separable algebra over a commutative ring R. Many of the standard examples of separable R-algebras are presented. A localization of R is separable, as is a nonzero homomorphic image of R and the ring of n-by-n matrices over R. If G is a finite group such that the order of G is invertible in R, then the group ring $R(G)$ is separable over R. We show that separability is preserved under a change of base, and separability is transitive in the sense that a separable algebra over a separable algebra is separable. If k is a field, then a separable k-algebra is a finite direct sum of matrix algebras over finite dimensional k-division algebras such that the center of each division algebra appearing is a separable extension field of k. We do not prove it here, but an R-algebra A is R-separable if and only if A is separable over its center $Z(A)$, and $Z(A)$ is R-separable (see [**18**, Theorem 7.1.11]).

1. Separable Algebra, the Definition

In this section the notion of a separable algebra over a commutative ring is defined. The basic properties of separable algebras are studied. Most of the material in this section first appeared in [**7**], including the definition of separability.

An extension of fields F/k is separable if every element of F is the root of a separable polynomial over k. This definition does not generalize to an algebra A over a commutative ring R. Instead the definition of a separable algebra is based on a certain module structure of the ring A over the enveloping algebra $A \otimes_R A^o$ which is induced by the multiplication map $x \otimes y \mapsto xy$.

DEFINITION 5.1.1. Let R be a commutative ring and A an R-algebra. A *two-sided A/R-module* is a left A right A bimodule M such that the two induced R-actions are equal. That is, for all $a, b \in A$, $r \in R$, $x \in M$:

$$\begin{aligned} (ax)b &= a(xb), \text{ and} \\ rx = (r \cdot 1)x &= x(r \cdot 1) = xr. \end{aligned} \tag{1.1}$$

The *enveloping algebra* of A is $A^e = A \otimes_R A^o$. Then A^e is an R-algebra. If M is a left A^e-module, then we can make M into a two-sided A/R-module by

$$\begin{aligned} ax &= a \otimes 1 \cdot x, \\ xa &= 1 \otimes a \cdot x. \end{aligned} \tag{1.2}$$

Conversely, any two-sided A/R-module can be turned into a left A^e-module in the same way. Since A is an R-algebra, A is a two-sided A/R-module. Hence, by (1.2), A is a left A^e-module. By Example 1.1.13, the left regular representation of A^e as a ring of R-module endomorphisms of A induces an R-algebra homomorphism

$$\varphi : A^e \to \operatorname{Hom}_R(A,A) \tag{1.3}$$

where an element α of A^e is mapped to the element $\varphi(\alpha)$ of $\operatorname{Hom}_R(A,A)$ which is "left multiplication by α". Specifically, if $\alpha = \sum a_i \otimes b_i$, then for any $x \in A$, $\varphi(\alpha)(x) = \alpha \cdot x = \sum_i a_i x b_i$. The map φ will be called the *enveloping homomorphism* of A. The ring A^e is a left A^e-module, and the assignment $x \mapsto x \cdot 1$ defines an A^e-module epimorphism

$$\begin{aligned} A^e &\xrightarrow{\mu} A \\ a \otimes b &\mapsto ab. \end{aligned} \tag{1.4}$$

Denote by $J_{A/R}$ the kernel of μ. Then $J_{A/R}$ is an A^e-submodule of A^e, hence is a left ideal. The sequence

$$0 \to J_{A/R} \to A^e \xrightarrow{\mu} A \to 0 \tag{1.5}$$

is an exact sequence of A^e-modules. When A is commutative, μ is a homomorphism of R-algebras (see Exercise 2.3.11). See Example 5.5.2 for an example of a noncommutative algebra A over a field k such that μ is not a homomorphism of rings and $J_{A/k}$ is not a two-sided ideal. Notice that $\mu(a \otimes 1 - 1 \otimes a) = 0$ so $a \otimes 1 - 1 \otimes a \in J_{A/R}$. In Exercise 5.1.3 the reader is asked to prove that $J_{A/R}$ is generated by elements of the form $a \otimes 1 - 1 \otimes a$.

PROPOSITION 5.1.2. *Let R be a commutative ring and A an R-algebra. The following are equivalent.*

(1) A is projective as a left A^e-module.
(2) The sequence

$$0 \to J_{A/R} \to A^e \xrightarrow{\mu} A \to 0$$

of left A^e-modules is split exact.
(3) There is an element $e \in A^e$ such that $\mu(e) = 1$ and $J_{A/R}e = 0$.
(4) There is an idempotent $e \in A^e$ such that $J_{A/R}$ is equal to the principal left ideal in A^e generated by $1 - e$.

PROOF. Follows from Exercise 3.2.1. □

DEFINITION 5.1.3. Let R be a commutative ring and A an R-algebra. If A satisfies any of the equivalent properties of Proposition 5.1.2, then we say A is a *separable* R-algebra. Notice that the same element e works for both (3) and (4). The element $e \in A^e$ is called a *separability idempotent* for A. If A is commutative, then a separability idempotent is unique, if it exists (Exercise 5.1.1).

DEFINITION 5.1.4. Let R be a commutative ring and A an R-algebra. If M is a two-sided A/R-module, define

$$M^A = \{x \in M \mid ax = xa, \forall a \in A\}.$$

This R-submodule of M is called the centralizer of A in M.

The rest of this section focuses on a proof that A is R-separable if and only if the assignment $M \mapsto M^A$ defines an exact functor from the category of left A^e-modules to the category of left R-modules.

LEMMA 5.1.5. *Let R be a commutative ring, A an R-algebra, and M an A^e-module. Then*

$$\begin{aligned}\operatorname{Hom}_{A^e}(A,M) &\xrightarrow{\cong} M^A\\ f &\mapsto f(1)\end{aligned}$$

is an isomorphism of R-modules. If $g\colon M \to N$ is an A^e-module homomorphism, then the diagram

$$\begin{tikzcd}\operatorname{Hom}_{A^e}(A,M) \arrow[r, "g\circ(\cdot)"] \arrow[d] & \operatorname{Hom}_{A^e}(A,N) \arrow[d] \\ M^A \arrow[r, "g"] & N^A\end{tikzcd}$$

commutes. The functors $\operatorname{Hom}_{A^e}(A,\cdot)$ and $(\cdot)^A$ are naturally isomorphic and both are left exact.

PROOF. Let $f \in \operatorname{Hom}_{A^e}(A,M)$. Then for $a \in A$,

$$\begin{aligned}a\cdot f(1) &= a\otimes 1\cdot f(1)\\ &= f(a\otimes 1\cdot 1)\\ &= f(a)\\ &= f(1\otimes a\cdot 1)\\ &= 1\otimes a\cdot f(1)\\ &= f(1)\cdot a.\end{aligned}$$

So $f(1) \in M^A$. Conversely, say $x \in M^A$. Define $\rho_x\colon A \to M$ to be "right multiplication by x", $\rho_x(a) = ax$. See that ρ_x is A^e-linear:

$$\begin{aligned}\rho_x(b\otimes c\cdot a) &= \rho_x(bac)\\ &= (bac)x\\ &= (b\otimes c\cdot a)x\\ &= b\otimes c\cdot(a\otimes 1\cdot x)\\ &= b\otimes c\cdot(ax)\\ &= b\otimes c\cdot \rho_x(a).\end{aligned}$$

Since $\rho_x(1) = x$ and $\rho_{f(1)}(x) = xf(1) = f(x)$, these are inverses of each other. The rest of the proof is left to the reader. □

COROLLARY 5.1.6. $\operatorname{Hom}_{A^e}(A,A) \cong Z(A)$ *under the correspondence* $f \mapsto f(1)$.

PROOF. Take $M = A$ in Lemma 5.1.5 and note that $A^A = Z(A)$. □

COROLLARY 5.1.7. *Let $(0\colon J_{A/R}) = \{x \in A^e \mid yx = 0, \forall y \in J_{A/R}\}$ be the right annihilator of $J_{A/R}$ in A^e. Then $\operatorname{Hom}_{A^e}(A,A^e) \cong (0\colon J_{A/R})$. If A is R-separable, then $\mu(0\colon J_{A/R}) = Z(A)$.*

PROOF. Take $M = A^e$ in Lemma 5.1.5. Then

$$\begin{aligned}\operatorname{Hom}_{A^e}(A,A^e) &\cong \left(A^e\right)^A\\ &= \{x \in A^e \mid (a\otimes 1 - 1\otimes a)x = 0,\ \forall a \in A\}\\ &= (0\colon J_{A/R}).\end{aligned}$$

If A is R-separable, then A is A^e-projective. Since

$$A^e \xrightarrow{\mu} A \to 0$$

is exact, it follows from Proposition 2.4.5 that

$$\operatorname{Hom}_{A^e}(A, A^e) \xrightarrow{\mu\circ()} \operatorname{Hom}_{A^e}(A, A) \to 0$$

is exact. By Lemma 5.1.5, $\mu(0 : J_{A/R}) = Z(A)$. □

COROLLARY 5.1.8. *An R-algebra A is separable if and only if $(\cdot)^A$ is a right exact functor.*

PROOF. By Proposition 2.4.5, the functor $\operatorname{Hom}_{A^e}(A, \cdot)$ is right exact if and only if A is a projective A^e-module. □

1.1. Exercises.

EXERCISE 5.1.1. If S is a commutative separable R-algebra, then the separability idempotent is unique. (Hint: Lemma 3.3.12.)

EXERCISE 5.1.2. Let R be a commutative ring.

(1) R is a separable R-algebra.
(2) If $W \subseteq R$ is a multiplicative set, then the localization R_W is a separable R-algebra.
(3) If $I \subseteq R$ is a nonunit ideal, then R/I is a separable R-algebra.

EXERCISE 5.1.3. Let $\mu : A \otimes_R A^o \to A$ be as in Eq. (1.4) Prove that $J_{A/R}$, the kernel of μ, is the left ideal in $A \otimes_R A^o$ generated by the set $\{a \otimes 1 - 1 \otimes a \mid a \in A\}$.

EXERCISE 5.1.4. Let R be a commutative ring.

(1) Let $R \oplus R$ be the ring direct sum of two copies of R. Let $e_1 = (1, 0)$ and $e_2 = (0, 1)$ be the orthogonal idempotents in $R \oplus R$. Use Exercise 5.1.3 to show that $e = e_1 \otimes e_1 + e_2 \otimes e_2$ is a separability idempotent. Hence, $R \oplus R$ is separable over R.
(2) Let $R^n = R \oplus \cdots \oplus R$ be the ring direct sum of n copies of R. Show that R^n is separable over R. (Hint: $e = \sum_{i=1}^n e_i \otimes e_i$ is a separability idempotent, where $e_1, \ldots, e_n$ are the orthogonal idempotents in R^n.)

EXERCISE 5.1.5. Show that $\mathbb{C}$ is separable over $\mathbb{R}$. (Hint: Use Exercise 5.1.3 to show that $\frac{1}{2}(1 \otimes 1 - i \otimes i)$ is a separability idempotent.)

EXERCISE 5.1.6. Let $\mathbb{H} = \mathbb{R}1 + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij$ be the ring of real quaternions. As an $\mathbb{R}$-vector space $\mathbb{H}$ is spanned by the four linearly independent elements $1, i, j, ij$. Multiplication in $\mathbb{H}$ is determined by the rules:

$$i^2 = j^2 = (ij)^2 = -1, \quad ij = -ji.$$

Show that $\mathbb{H}$ is a separable $\mathbb{R}$-algebra. (Hint: $e = \frac{1}{4}(1 \otimes 1 - i \otimes i - j \otimes j - ij \otimes ij)$ is a separability idempotent.)

EXERCISE 5.1.7. If A is a separable R-algebra and e is a separability idempotent, then $(A \otimes_R A^o)e = (A \otimes_R 1)e = (1 \otimes_R A^o)e$.

EXERCISE 5.1.8. Prove the following generalization of Lemma 5.1.5. Let R be a commutative ring, A an R-algebra, and S a commutative R-subalgebra of A. If M is a left $S \otimes_R A^o$-module, then the assignment $f \mapsto f(1)$ induces an isomorphism of R-modules

$\operatorname{Hom}_{S\otimes_R A^o}(A,M) \cong M^S$. If $g\colon M \to N$ is a homomorphism of left $S\otimes_R A^o$-modules, then the diagram

$$\begin{tikzcd}
\operatorname{Hom}_{S\otimes_R A^o}(A,M) \arrow[r, "g\circ(\cdot)"] \arrow[d] & \operatorname{Hom}_{S\otimes_R A^o}(A,N) \arrow[d] \\
M^S \arrow[r, "g"] & N^S
\end{tikzcd}$$

commutes. The functors $\operatorname{Hom}_{S\otimes_R A^o}(A,\cdot)$ and $(\cdot)^S$ are naturally isomorphic and both are left exact.

2. Examples of Separable Algebras

In this section three standard examples of separable algebras are presented. First we show that the ring of n-by-n-matrices over a commutative ring R is a separable R-algebra. Secondly, we show that if G is a finite group of order n and n is invertible in R, then the group ring $R(G)$ is a separable R-algebra. In our third example we show that if 2 is invertible in R and I is an R-module with the property that $I\otimes_R I \cong R$, then $S = R\oplus I$ can be turned into a separable R-algebra.

More examples appear in the exercises (Sections 5.1.1 and 5.4.1).

EXAMPLE 5.2.1. Let R be a commutative ring and let $M_n(R)$ be the ring of n-by-n matrices over R. Let e_{ij} be the elementary matrix having a single 1 in position (i,j) and 0 elsewhere. Notice that

$$e_{k\ell}e_{ij} = \begin{cases} e_{kj} & \text{if } \ell = i \\ 0 & \text{otherwise.} \end{cases}$$

Fix j and define

$$e = \sum_{i=1}^{n} e_{ij}\otimes e_{ji}$$

in the enveloping algebra of $M_n(R)$. Then

$$\begin{aligned}
\mu(e) &= \sum_i e_{ij}e_{ji} \\
&= \sum_i e_{ii} \\
&= 1.
\end{aligned}$$

For any k and l,

$$\begin{aligned}
(e_{kl}\otimes 1 - 1\otimes e_{kl})e &= \sum_i (e_{kl}e_{ij}\otimes e_{ji} - e_{ij}\otimes e_{ji}e_{kl}) \\
&= e_{kj}\otimes e_{jl} - e_{kj}\otimes e_{jl} \\
&= 0.
\end{aligned}$$

Since the e_{kl} generate $M_n(R)$ as an R-module, Exercise 5.1.3 shows that $J_{A/R}e = 0$. By Proposition 5.1.2 we see that $M_n(R)$ is a separable R-algebra and e is a separability idempotent.

EXAMPLE 5.2.2. Let G be a finite multiplicative group and R a commutative ring. Suppose G has order n and assume $n = n\cdot 1$ is a unit in R. Starting with the identity element, let $G = \{1 = \sigma_1, \sigma_2, \dots, \sigma_n\}$ be an enumeration of the elements of G. Let $R(G) = R \cdot 1 \oplus R \cdot \sigma_2 \oplus \cdots \oplus R \cdot \sigma_n$ be the group algebra (Example 1.1.4). Let

$$e = \frac{1}{n} \sum_{\sigma \in G} \sigma \otimes \sigma^{-1}$$

which is an element in the enveloping algebra $\left[R(G)\right]^e$. Then

$$\mu(e) = \frac{1}{n} \sum_{\sigma \in G} \sigma\sigma^{-1} = \frac{1}{n} \sum_{\sigma \in G} 1 = 1.$$

If we fix any $\tau \in G$, then as sets we have $G = \{\sigma\tau | \sigma \in G\}$, hence

$$\begin{aligned}(\tau \otimes 1)e &= \frac{1}{n} \sum_{\sigma \in G} \tau\sigma \otimes \sigma^{-1} \\ &= \frac{1}{n} \sum_{\rho} \rho \otimes \rho^{-1}\tau \\ &= \frac{1}{n} \sum_{\rho} \rho \otimes \tau * \rho^{-1} \\ &= (1 \otimes \tau)e.\end{aligned}$$

(We write $x * y = yx$ as the product in the opposite algebra.) The group algebra $R(G)$ is generated over R by the basis elements $\tau \in G$. This together with Exercise 5.1.3 and Proposition 5.1.2 shows that e is a separability idempotent for $R(G)$ and the group algebra $R(G)$ is a separable R-algebra. For the converse of this result see Exercise 5.5.3.

EXAMPLE 5.2.3. Let R be an integral domain and assume $2 = 1 + 1$ is a unit in R. In this example, we see that an element of order two in the Picard group gives rise to a separable R-algebra. Let $I \subseteq R$ an ideal which is an invertible R-module (I is projective and has rank one). Suppose $I^2 = R\alpha$ is principal. In this case, there is an isomorphism of R-modules $\phi\colon I^2 \to R$ defined by $\phi(x) = \alpha^{-1}x$. The multiplication map $R \otimes_R R \to R$ of Exercise 2.3.11 induces an R-module homomorphism $\psi\colon I \otimes_R I \to I^2$. Since ψ is onto and $I^2 \cong R$, ψ splits. But I^2 is free of rank one, so by counting ranks it follows that ψ is is an isomorphism of R-modules. By Lemma 3.6.5, $I \cong I^*$. It follows that in the Picard group, $|I|$ has order 1 or 2. Let $S = R \oplus I$ as R-modules. We turn S into a commutative R-algebra using ϕ to define a multiplication operation:

$$(a \oplus b)(c \oplus d) = (ac + \phi(bd)) \oplus (ad + cb).$$

The reader should verify that this multiplication rule is associative, commutative, distributes over addition, and that $1 \oplus 0$ is the identity element.

We show S is separable by constructing a separability idempotent in S^e. By assumption, there exist elements $a_1, \dots, a_n, b_1, \dots, b_n$ in I and $\sum_i a_i b_i = \alpha$. In S define two sequences

$$x_1 = 0 \oplus a_1, \dots, x_n = 0 \oplus a_n, x_{n+1} = 1 \oplus 0$$

and

$$y_1 = 0 \oplus b_1, \dots, y_n = 0 \oplus b_n, y_{n+1} = 1 \oplus 0.$$

Notice that

$$\begin{aligned}\sum_{i=1}^{n+1} x_i y_i &= x_1 y_1 + \cdots + x_n y_n + x_{n+1} y_{n+1} \\ &= \big(\phi(a_1 b_1) + \cdots + \phi(a_n b_n) + 1\big) \oplus 0 \\ &= (\phi(a_1 b_1 + \cdots + a_n b_n) + 1) \oplus 0 \\ &= (1+1) \oplus 0 \\ &= 2 \oplus 0\end{aligned}$$

In the enveloping algebra S^e, define

$$e = \frac{1}{2} \sum_{i=1}^{n+1} x_i \otimes y_i.$$

By the above,

$$\mu(e) = \frac{1}{2} \sum_i x_i y_i = 1 \oplus 0 = 1.$$

By Exercise 5.1.3, $J_{S/R}$ is generated by elements of the form $x \otimes 1 - 1 \otimes x$, where $x \in S = R \oplus I$. Since $a \otimes 1 - 1 \otimes a = 0$, if $a \in R$, it follows that $J_{S/R}$ is generated by elements of the form $x \otimes 1 - 1 \otimes x$, where $x \in 0 \oplus I$. Notice that $(0 \oplus I)^2 \subseteq R \oplus 0$. Therefore, if $x \in 0 \oplus I$, then

$$\begin{aligned}x \otimes 1 \cdot e &= \frac{1}{2} \left(\sum_{j=1}^{n} x x_j \otimes y_j + x \otimes 1 \right) \\ &= \frac{1}{2} \left(\sum_{j=1}^{n} 1 \otimes x x_j y_j + x \otimes 1 \right) \\ &= \frac{1}{2} \left(1 \otimes \left(\sum_{j=1}^{n} x_j y_j \right) \cdot 1 \otimes x + x \otimes 1 \right) \\ &= \frac{1}{2} (1 \otimes x + x \otimes 1)\end{aligned}$$

which by a similar argument is equal to $1 \otimes x \cdot e$. Then $J_{S/R} e = (0)$. By Proposition 5.1.2, e is a separability idempotent for S and S is separable over R. This example is a small part of Kummer Theory, the interested reader is referred to [**18**, Section 12.9] for additional results.

3. Separable Algebras Under Change of Base Ring

There are two main results in this section, both of which are due to M. Auslander and O. Goldman, [**7**]. Proposition 5.3.1, which is actually very general, implies that tensor product induces a product on the category of all separable R-algebras. It also implies that the property of an algebra being separable is preserved under a change of base ring. Proposition 5.3.3 and its corollaries are particular types of "Descent Theorems". They have the form, "If A becomes separable under a suitable change of base, then A is separable." We prove in Theorem 10.1.10 below a faithfully flat descent theorem for separability.

PROPOSITION 5.3.1. *Let R be a commutative ring and S_1 and S_2 commutative R-algebras. Let A_1 be a separable S_1-algebra and A_2 a separable S_2-algebra. Then $A_1 \otimes_R A_2$ is separable over $S_1 \otimes_R S_2$.*

PROOF. We show that $(\cdot)^{A_1 \otimes_R A_2}$ is an exact functor on two-sided $A_1 \otimes_R A_2/S_1 \otimes_R S_2$-modules and then apply Corollary 5.1.8. Start with an exact sequence

$$M \xrightarrow{f} N \to 0$$

of two-sided $A_1 \otimes_R A_2/S_1 \otimes_R S_2$-modules. The diagram of ring homomorphisms

$$\begin{tikzcd} A_1 \arrow[r] & A_1 \otimes_R A_2 \\ S_1 \arrow[u] \arrow[r] & S_1 \otimes_R S_2 \arrow[u] \end{tikzcd}$$

commutes so M and N can be turned into two-sided A_1/S_1-modules. Since A_1 is separable over S_1, the sequence

$$(M)^{A_1} \xrightarrow{f} (N)^{A_1} \to 0$$

is exact. From Exercise 2.3.10 the diagram

$$\begin{tikzcd} & A_1 \otimes_R A_2 & \\ A_1 \arrow[ur, "\rho_1"] & & A_2 \arrow[ul, "\rho_2"'] \\ & R \arrow[ul] \arrow[ur] & \end{tikzcd}$$

commutes and $\operatorname{im}(\rho_1)$ commutes with $\operatorname{im}(\rho_2)$. So we turn M^{A_1} and N^{A_1} into two-sided A_2/S_2-modules. Since A_2 is separable over S_2, the sequence

$$\left(M^{A_1}\right)^{A_2} \xrightarrow{f} \left(N^{A_1}\right)^{A_2} \to 0$$

is exact. As a ring $A_1 \otimes_R A_2$ is generated by the images of ρ_1 and ρ_2. So $\left(M^{A_1}\right)^{A_2} \subseteq M^{A_1 \otimes_R A_2}$. Conversely, $M^{A_1 \otimes_R A_2} \subseteq M^{A_1 \otimes_R 1} \cap M^{1 \otimes_R A_2} = \left(M^{A_1}\right)^{A_2}$. $\square$

COROLLARY 5.3.2. *Let A be a separable R-algebra and S a commutative R-algebra. Then $A \otimes_R S$ is a separable S-algebra.*

PROOF. Take $A = A_1$, $R = S_1$, $S = S_2 = A_2$ in Proposition 5.3.1. $\square$

PROPOSITION 5.3.3. *(Descent of Separable Algebras) Let R be a commutative ring and S_1 and S_2 commutative R-algebras. Let A_1 be any S_1-algebra and A_2 any S_2-algebra such that $A_1 \otimes_R A_2$ is separable over $S_1 \otimes_R S_2$. If A_2 is faithful as an R-module and $R \cdot 1$ is an R-module direct summand of A_2, then A_1 is separable over S_1.*

PROOF. We show that $(\cdot)^{A_1}$ is right exact and apply Corollary 5.1.8. Let M be a two-sided A_1/S_1-module. The reader should verify that $M \otimes_R A_2$ is then a two-sided $A_1 \otimes_R A_2/S_1 \otimes_R S_2$-module. By our hypothesis, the sequence of natural maps $0 \to R \to A_2$ splits. That is, $A_2 = L \oplus R \cdot 1$ as R-modules and there is an isomorphism

$$M \otimes_R A_2 = M \otimes_R (L \oplus R \cdot 1) \cong (M \otimes_R L) \oplus (M \otimes_R R \cdot 1).$$

The reader should verify that in fact $M \otimes_R R \cdot 1$ is a two-sided A_1/S_1-module direct summand of $M \otimes_R A_2$, hence there is a projection

$$M \otimes_R A_2 \xrightarrow{\pi} M \otimes_R R \cdot 1 \tag{3.1}$$

of two-sided A_1/S_1-modules. Apply the functor $(\cdot)^{A_1}$ to (3.1) to get the R-module homomorphism

$$(M \otimes_R A_2)^{A_1} \xrightarrow{\pi} (M \otimes_R R \cdot 1)^{A_1}.$$

Since $\big(M \otimes_R A_2\big)^{A_1 \otimes_R A_2} \subseteq (M \otimes_R A_2)^{A_1}$, the map π restricted to $\big(M \otimes_R A_2\big)^{A_1 \otimes_R A_2}$ takes values in $(M \otimes_R R \cdot 1)^{A_1}$. Using the fact that A_2 is R-faithful, the reader should verify that $M^{A_1} \otimes_R R \cdot 1 = (M \otimes_R R \cdot 1)^{A_1}$ and the sequence

$$\big(M \otimes_R A_2\big)^{A_1 \otimes_R A_2} \xrightarrow{\pi} M^{A_1} \otimes_R R \cdot 1 \to 0 \tag{3.2}$$

is exact. Consider an arbitrary exact sequence

$$M \xrightarrow{f} N \to 0 \tag{3.3}$$

of two-sided A_1/S_1-modules. Combine (3.2) with (3.3) to get the diagram

$$\begin{tikzcd} \big(M \otimes_R A_2\big)^{A_1 \otimes_R A_2} \arrow[r, "f \otimes 1"] \arrow[d, "\pi"] & \big(N \otimes_R A_2\big)^{A_1 \otimes_R A_2} \arrow[r] \arrow[d, "\pi"] & 0 \\ M^{A_1} \otimes_R R \cdot 1 \arrow[r, "f \otimes 1"] & N^{A_1} \otimes_R R \cdot 1 \arrow[r] & 0 \end{tikzcd} \tag{3.4}$$

which commutes. The functor $(\cdot) \otimes_R A_2$ is always right exact, and by assumption the functor $(\cdot)^{A_1 \otimes_R A_2}$ is right exact. Therefore the top row of (3.4) is exact. By (3.2), π is onto, which implies the bottom row of (3.4) is exact. Since $R \to R \cdot 1$ is an isomorphism, $f : M^{A_1} \to N^{A_1}$ is onto. □

COROLLARY 5.3.4. *Let A_1 and A_2 be R-algebras such that A_2 is faithful over R, and $R \cdot 1$ is an R-module direct summand of A_2. If $A_1 \otimes_R A_2$ is separable over R, then A_1 is separable over R.*

PROOF. Take $S_1 = S_2 = R$ in Proposition 5.3.3. □

COROLLARY 5.3.5. *Let S be a commutative faithful R-algebra such that $R \cdot 1$ is an R-module direct summand of S. Let A be an R-algebra such that $A \otimes_R S$ is S-separable.*

(1) A is R-separable.
(2) If the image of $R \otimes_R S \to A \otimes_R S$ is equal to the center of $A \otimes_R S$, then $R \cdot 1$ is equal to the center of A.

PROOF. For the first part, take $A_1 = A$, $A_2 = S_2 = S$ and $S_1 = R$ in Proposition 5.3.3. For the second part, notice that

$$1 \otimes_R S = Z(A \otimes_R S) = \big(A \otimes_R S\big)^{A \otimes_R S}$$

maps onto $A^A = Z(A)$ by the proof of Proposition 5.3.3. But the projection map π is the splitting map to $R \to S$ which has image $R \cdot 1$. Hence $1 \otimes S$ projects onto $1 \otimes R \cong R \cdot 1$. □

REMARK 5.3.6. Say A is an R-algebra with structure homomorphism $\theta : R \to Z(A)$. If I is an ideal in R and $I \subseteq \ker \theta$, then θ factors through R/I so A is an R/I-algebra and $A \otimes_R A^o = A \otimes_{R/I} A^o$ so A is R-separable if and only if A is R/I-separable.

PROPOSITION 5.3.7. *Say A is a separable R-algebra and I is a two-sided ideal of A. Then A/I is a separable R-algebra. Moreover,*

$$Z(A/I) = \frac{Z(A) + I}{I}$$

PROOF. Let M be a two-sided $(A/I)/R$-module. Then M can be viewed as a two-sided A/R-module using the natural homomorphism $\eta : A \to A/I$. Then $M^A = M^{A/I}$. Then A/I is R-separable by Corollary 5.1.8. Now

$$A \to A/I \to 0$$

is an exact sequence of two-sided A/R-modules. Since A is R-separable,

$$A^A \to (A/I)^A \to 0$$

is exact. So $Z(A/I)$ is the image under η of $Z(A)$. □

COROLLARY 5.3.8. *Let A_1 be an R_1-algebra and A_2 an R_2-algebra, where R_1 and R_2 are commutative rings. Then $A_1 \oplus A_2$ is a separable $R_1 \oplus R_2$-algebra if and only if both A_1 and A_2 are separable over R_1 and R_2 respectively.*

PROOF. Follows from Corollary 5.1.8 and Proposition 5.3.7. □

4. Homomorphisms of Separable Algebras

We prove three fundamental theorems on separable algebras. The first (Theorem 5.4.1) is a theorem of permanence which says that if A is R-separable and M is an A-module which is R-projective, then M is A-projective. In Theorem 5.4.2 we prove that separability is transitive. The third (Theorem 5.4.3) is a general result, more technical than the rest, and applies to any homomorphism of R-algebras $\theta : A \to B$ such that A is R-separable.

THEOREM 5.4.1. *Let R be a commutative ring and A a separable R-algebra. By the structure homomorphism $\theta : R \to A$, any left A-module M inherits the structure of a left R-module.*

(1) Let

$$0 \to L \to N \xrightarrow{\eta} M \to 0$$

be any exact sequence of left A-modules. If the sequence is split exact in ${}_R\mathfrak{M}$, then it is split exact in ${}_A\mathfrak{M}$.

(2) Let M be a left A-module. If M is R-projective, then M is A-projective.

PROOF. By Proposition 2.1.1, (2) follows from (1). Suppose there exists an R-module homomorphism $\psi : M \to N$ with $\eta\psi = 1_M$. Since both N and M are left A-modules, Lemma 2.4.1 shows that $\mathrm{Hom}_R(M,N)$ can be given the structure of a left A^e-module under the operation induced by

$$\left[(x \otimes y) \cdot f\right](m) = x \cdot f(y \cdot m),$$

where $x \otimes y \in A \otimes_R A^o$, $f \in \mathrm{Hom}_R(M,N)$, and $m \in M$. Since A is R-separable, let $e \in A^e$ be a separability idempotent for A. Define $\psi' = e \cdot \psi$. That is, if $e = \sum_i x_i \otimes y_i$, and $m \in M$ then

$$\psi'(m) = \sum_i x_i \psi(y_i m).$$

Since η is an A-module homomorphism and $\mu(e) = 1$, we have

$$\begin{aligned}
\eta\psi'(m) &= \eta\left(\sum_i x_i \psi(y_i m)\right) \\
&= \sum_i x_i \eta \cdot \psi(y_i m) \\
&= \sum_i x_i y_i m \\
&= m
\end{aligned}$$

for all $m \in M$. Since $J_{A/R}e = 0$, we have

$$\begin{aligned}(a \otimes 1 - 1 \otimes a)\psi' &= (a \otimes 1 - 1 \otimes a)e \cdot \psi \\ &= 0,\end{aligned}$$

for all $a \in A$. It follows that

$$\begin{aligned}a\psi'(m) &= a \otimes 1 \cdot \psi'(m) \\ &= 1 \otimes a \cdot \psi'(m) \\ &= \psi'(am),\end{aligned}$$

for all $a \in A$, $m \in M$. □

THEOREM 5.4.2. *Let S be a commutative R-algebra and let A be an S-algebra. Then A is also an R-algebra.*

(1) (Separable over Separable is Separable) If S is separable over R and A is separable over S, then A is separable over R.
(2) If A is separable over R, then A is separable over S.
(3) If A is separable over R and A is an S-progenerator, then S is separable over R.

PROOF. (1): Any two-sided A/R-module M is also a two-sided S/R-module. Given any $x \in M^S$, $a \in A$ and $s \in S$, the equations

$$\begin{aligned}s \cdot (a \cdot x) &= a \cdot (s \cdot x) \\ &= a \cdot (x \cdot s) \\ &= (a \cdot x) \cdot s\end{aligned}$$

show that $ax \in M^S$. It follows that M^S is a two-sided A/S-module, with $\left(M^S\right)^A = M^A$. For any two-sided A/R-modules M and N, if

$$M \xrightarrow{f} N \to 0$$

is exact then, by Corollary 5.1.8 applied to the separable R-algebra S, it follows that

$$M^S \xrightarrow{f} N^S \to 0$$

is exact. But $\left(M^S\right)^A = M^A$ and $\left(N^S\right)^A = N^A$. By Corollary 5.1.8 applied to the separable S-algebra A, it follows that

$$M^A \xrightarrow{f} N^A \to 0$$

exact. Hence A is R-separable, which proves (1).

(2): In the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & J_{A/R} \arrow[r] \arrow[d] & A \otimes_R A^o \arrow[r, "\mu"] \arrow[d] & A \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & J_{A/S} \arrow[r] & A \otimes_S A^o \arrow[r, "\mu"] & A \arrow[r] & 0
\end{tikzcd}$$

all of the vertical maps are onto (Exercise 2.3.16). A separability idempotent for A/R maps to a separability idempotent for A/S.

(3): By part (2), A is separable over S. Since A is S-projective, so is A^o. The reader should verify (for example, by an argument involving dual bases) that $A \otimes_R A^o$ is projective over $S \otimes_R S$. Because A is separable over R, A is projective as a left $A \otimes_R A^o$-module under the μ-action. By Proposition 2.1.13, it follows that A is projective as a left $S \otimes_R S$-module.

By Proposition 3.5.6, $S \cdot 1$ is an S-module direct summand of A, so we can write $A = S \oplus L$ for some L. It follows that S is also an $S \otimes_R S$-module direct summand of A under the μ-action. Hence S is $S \otimes_R S$-projective and S is R-separable. $\square$

Let R be a commutative ring and $\theta : A \to B$ an R-algebra homomorphism. Consider the commutative diagram

$$\begin{tikzcd} A \otimes_R B^0 \arrow[rr, "\gamma"] \arrow[dr, "\theta\otimes 1"'] & & B \\ & B \otimes_R B^o \arrow[ur, "\mu"'] & \end{tikzcd} \tag{4.1}$$

where γ is defined to be the R-algebra homomorphism $\theta \otimes 1$, followed by the left $B \otimes_R B^o$-module homomorphism μ. Therefore, all of the terms in (4.1) can be viewed as left $A \otimes_R B^o$-modules. Notice that $\gamma(x \otimes y) = \theta(x)y$, hence the left $A \otimes_R B^o$-module action on B is given by $(a \otimes b) \cdot x = \theta(a)xb$. We emphasize that γ is not a homomorphism of rings unless the image of θ is a subring of the center of B.

THEOREM 5.4.3. *Let R be a commutative ring and $\theta : A \to B$ an R-algebra homomorphism. If A is R-separable, then the following are true.*

1. *The sequence of left $A \otimes_R B^o$-modules*
$$A \otimes_R B^o \xrightarrow{\gamma} B \to 0$$
is split exact. The kernel of γ is idempotent generated, and B is projective as a left $A \otimes_R B^o$-module.
2. *If B is a flat left R-module, then B is a flat left A-module.*
3. *If B is a projective left R-module, then B is a projective left A-module.*
4. *If A is commutative, $\operatorname{im}(\theta) \subseteq Z(B)$, and B is R-separable, then B is A-separable.*

PROOF. (1): Since A is R-separable, there is a split exact sequence

$$0 \to J_{A/R} \to A^e \xrightarrow{\mu} A \to 0 \tag{4.2}$$

of left A^e-modules. The R-algebra homomorphism $1 \otimes \theta : A^e \to A \otimes_R B^o$ allows us to view $A \otimes_R B^o$ as a left $A \otimes_R B^o$ right A^e-bimodule. Applying the functor $(A \otimes_R B^o)_{A^e}(\,)$ to sequence (4.2) yields the split exact sequence

$$0 \to (A \otimes_R B^o) \otimes_{A^e} J_{A/R} \to (A \otimes_R B^o) \otimes_{A^e} A^e \xrightarrow{1\otimes\mu} (A \otimes_R B^o)_{A^e} A \to 0 \tag{4.3}$$

of left $A \otimes_R B^o$-modules. By Lemma 2.3.13, the middle term in (4.3) is isomorphic to $A \otimes_R B^o$. Define $\phi : B \to (A \otimes_R B^o) \otimes_{A^e} A$ by $x \mapsto 1 \otimes x \otimes 1$. The reader should verify that ϕ is onto. Notice $a \otimes b \cdot \phi(x) = a \otimes b \cdot 1 \otimes x \otimes 1 = a \otimes xb \otimes 1 = 1 \otimes xb \otimes a = 1 \otimes \theta(a)xb \otimes 1 = \phi(a \otimes b \cdot x)$, so ϕ is a well defined $A \otimes_R B^o$-module epimorphism. To see that ϕ is one-to-one, look at the $\mathbb{Z}$-module homomorphisms

$$B \xrightarrow{\phi} (A \otimes_R B^o)_{A^e} A \xrightarrow{\theta\otimes 1\otimes\theta} (B \otimes_R B^o)_{A^e} B \xrightarrow{\xi} (B \otimes_R B^o)_{B^e} B \xrightarrow{\cong} B \tag{4.4}$$

where ξ is from Exercise 2.3.16, and the last isomorphism is Lemma 2.3.13. In (4.4), the composite map is the identity on B. This shows ϕ is an isomorphism, hence the last term in (4.3) is isomorphic to B. The reader should verify that γ is the map induced by $1 \otimes \mu$, and that

$$0 \to \ker(\gamma) \to A \otimes_R B^o \xrightarrow{\gamma} B \to 0$$

is a split exact sequence of left $A \otimes_R B^o$-modules. The kernel of γ is idempotent generated, by Lemma 3.2.4. This proves (1).

(2): Since B is a flat left R-module, $A \otimes_R B^o$ is a flat left A-module (Theorem 2.3.23). By Exercise 2.3.6, a projective module is flat. Part (1) and Exercise 3.5.9 imply that B is a flat left A-module.

(3): This can be proved using the method of Part (2). Alternatively, this follows from Theorem 5.4.1.

(4): This is Theorem 5.4.2(2). □

Let A be a ring and $Z(A)$ the center of A. The next three results are concerned with the tower of subrings of A:

$$R \subseteq S \subseteq Z(A) \subseteq A. \tag{4.5}$$

COROLLARY 5.4.4. *As in Eq.* (4.5)*, let R and S be subrings of the center of A. Then any two of the following statements imply the third.*

(1) S is a separable R-algebra and a finitely generated projective R-module.
(2) A is a separable S-algebra and a finitely generated projective S-module.
(3) A is a separable R-algebra and a finitely generated projective R-module.

PROOF. (1) and (2) implies (3): Apply Proposition 2.1.13 and Theorem 5.4.2(1).

(1) and (3) implies (2): Since A is a finitely generated R-module, A is a finitely generated S-module. Since A is projective over R and S is separable over R, by Theorem 5.4.1, A is projective over S. Since A is separable over R, by Theorem 5.4.2(2), A is separable over S.

(2) and (3) implies (1): By Theorem 5.4.2(3), S is separable over R. By Proposition 3.5.6, $S \cdot 1$ is a S-module direct summand of A. Therefore, the R-module S is isomorphic to a direct summand of the R-progenerator A. This shows that S is a finitely generated projective R-module. □

The following finiteness criterion for a separable R-algebra is due to O. Villamayor and D. Zelinsky ([**59**]).

PROPOSITION 5.4.5. *Let R be a commutative ring and A a separable R-algebra which is projective as an R-module. Then A is finitely generated as an R-module.*

PROOF. Since A and A^o are identical as R-modules, it is enough to show A^o is finitely generated. Let $\{f_i, a_i\}$ be a dual basis for A^o over R with $a_i \in A^o$ and $f_i \in \operatorname{Hom}_R(A^o, R)$. For every $a \in A^o$, $f_i(a) = 0$ for almost all i and

$$a = \sum_i f_i(a) a_i.$$

Identify $A \otimes_R R$ with A, and consider $1_A \otimes f_i$ as an element of $\operatorname{Hom}_A(A^e, A)$. The set $\{1_A \otimes f_i, 1 \otimes a_i\}$ forms a dual basis for A^e as a projective left A-module. That is,

$$u = \sum_i (1_A \otimes f_i)(u) \cdot (1 \otimes a_i)$$

for all $u \in A^e$. Applying the multiplication map μ and setting $u = (1 \otimes a)e$ where e is a separability idempotent for A over R, we obtain

$$\begin{aligned} a &= \mu\big((1 \otimes a)e\big) \\ &= \sum_i \Big[(1_A \otimes f_i)\big((1 \otimes a)e\big)\Big] \cdot a_i \end{aligned} \tag{4.6}$$

for each $a \in A^o$. Since

$$\begin{aligned}(1_A \otimes f_i)\big((1 \otimes a)e\big) &= (1_A \otimes f_i)\big((a \otimes 1)e\big)\\ &= (a \otimes 1)\big((1_A \otimes f_i)(e)\big)\end{aligned}$$

the set of subscripts i for which $(1_A \otimes f_i)\big((1 \otimes a)e\big)$ is not equal to zero is contained in the finite set of subscripts for which $(1_A \otimes f_i)(e)$ is not equal to zero. This latter set is independent of a. Therefore the summation (4.6) may be taken over a fixed finite set. Writing

$$e = \sum_j x_j \otimes y_j \;,$$

we have from (4.6) that

$$\begin{aligned}a &= \sum_{i,j} x_j f_i(y_j a) a_i\\ &= \sum_{i,j} f_i(y_j a) x_j a_i\end{aligned}$$

for each $a \in A^o$. This shows that the finite set $\{x_j a_i\}$ generates A^o over R. □

Corollary 5.4.6 is attributed to F. DeMeyer.

COROLLARY 5.4.6. *Assume A is a separable R-algebra which as an R-module is faithful and projective. Then*

(1) A is an R-module progenerator.
(2) If S is a commutative separable R-subalgebra of A, then S is an R-module progenerator.

PROOF. (1): By Corollary 2.2.4, a finitely generated projective and faithful R-module is an R-progenerator. Therefore, this follows from Proposition 5.4.5.

(2): We identify R with $R \cdot 1$. By Proposition 3.5.6, R is an R-module direct summand of S. Since A is finitely generated over R, A is finitely generated over S. By Theorem 5.4.1, A is a finitely generated projective S-module. Since A is faithful over S, A is an S-progenerator. By Proposition 3.5.6, S is an S-module direct summand of A. So S is finitely generated projective and faithful over R. □

COROLLARY 5.4.7. *Let S and A be separable R-algebras and $f : S \to A$ an R-algebra homomorphism. Assume the image of f is a commutative R-subalgebra of A, and A is an R-module progenerator. The following are true:*

(1) The diagram of R-algebra homomorphisms

$$\begin{tikzcd} R \arrow[r, "\alpha"] \arrow[dr, "\beta"'] & f(S) \arrow[r, "\subseteq"] & A \\ & S \arrow[u] \arrow[ur, "f"'] & \end{tikzcd}$$

commutes.

(2) α and β are one-to-one.
(3) The kernel of f is idempotent generated.
(4) If S is commutative and connected, then f is a monomorphism.

PROOF. By Proposition 3.5.6, α is one-to-one. By Proposition 5.3.7, the image of f is a commutative separable R-subalgebra of A. By Corollary 5.4.6, $f(S)$ is an R-progenerator. By Theorem 5.4.1, $f(S)$ is projective over S. By Exercise 3.2.1, the kernel of f is idempotent generated. The rest is left to the reader. □

Let A be an R-algebra with structure homomorphism $\theta : R \to A$. A *section* to θ is an R-algebra homomorphism $\sigma : A \to R$ such that $\sigma\theta$ is the identity map on R. If A is R-separable, then in Corollary 5.4.8 below we show that a section $\sigma : A \to R$ is determined by a particular type of central idempotent in A.

COROLLARY 5.4.8. *Let R be a commutative ring and A a separable R-algebra. Then*

(1) There is a one-to-one correspondence between the set of all R-algebra homomorphisms $\sigma : A \to R$, and the set of all central idempotents e in A such that the composite mapping

$$R \to Re \to Ae$$

is one-to-one and onto. In this case $\sigma(e) = 1$ and $\sigma(x)e = xe$ for all $x \in A$.

(2) Suppose R is connected, $\sigma_1, \dots, \sigma_n$ are distinct R-algebra homomorphisms from A to R, and $e_1, \dots, e_n$ are the corresponding idempotents. Then
   (a) $\sigma_j(e_i) = 0$ if $i \neq j$, and
   (b) $e_ie_j = 0$, if $i \neq j$.

PROOF. (1): Let $\theta : R \to A$ be the structure homomorphism. Let e be a central idempotent in A and $\pi : A \to Ae$ the canonical projection map. The diagram

$$\begin{tikzcd} R \arrow[r, "\alpha"] \arrow[d, "\theta"'] & Re \arrow[d, "\subseteq"] \\ A \arrow[r, "\pi"] & Ae \end{tikzcd}$$

of R-algebra homomorphisms commutes, where $\alpha(x) = xe$. If $Re = Ae$ and α is one-to-one, then $\alpha^{-1}\pi$ is an R-algebra homomorphism.

Conversely, assume $\sigma : A \to R$ is an R-algebra homomorphism. By Theorem 5.4.1, σ makes R into a projective A-module. By Exercise 3.2.1 $\ker\sigma$ is an A-module direct summand of A, hence $\ker\sigma = Ae_0$ for some idempotent $e_0 \in A$. Since $\ker\sigma$ is a two-sided ideal of A, $e = 1 - e_0$ is a central idempotent by Theorem 1.1.8. The rest is left to the reader.

(2): Since R is connected, $\sigma_j(e_i)$ is equal to either 0 or 1. Suppose $\sigma_j(e_i) = 1$. Then for every $x \in A$, $\sigma_j(x) = \sigma_j(x)\sigma_j(e_i) = \sigma_j(xe_i) = \sigma_j(\sigma_i(x)e_i) = \sigma_i(x)\sigma_j(e_i) = \sigma_i(x)$ which implies $i = j$. This proves (a). Lastly, $\sigma_j(x)e_j = xe_j$ for all $x \in A$ implies $\sigma_j(e_i)e_j = e_ie_j$. This proves (b). $\square$

4.1. Exercises.

EXERCISE 5.4.1. Let $f : R \to S$ be a homomorphism of commutative rings. Let $q \in \operatorname{Spec} S$ and $p = f^{-1}(q)$. If S is a separable R-algebra, then S_q is a separable R_p-algebra.

EXERCISE 5.4.2. Let R be a commutative ring. Let A_1 and A_2 be R-algebras. Prove that $A_1 \oplus A_2$ is separable over R if and only if A_1 and A_2 are separable over R.

EXERCISE 5.4.3. Let k be any field and x an indeterminate.

(1) Show that $A = k[x]/(x^2)$ is not separable over k. (Hint: Show that A^e is a local ring. What are the candidates for e?)
(2) Show that $k[x]/(x^n)$ is k-separable if and only if $n = 1$.
(3) Suppose $f \in k[x]$ is a nonconstant polynomial such that each irreducible factor of f has degree one. Show that $k[x]/(f)$ is separable over k if and only if f has no repeated roots.

(4) Suppose $f \in k[x]$ is a nonconstant polynomial and F is a splitting field for f over k. Show that $k[x]/(f)$ is separable over k if and only if f has no repeated roots in F.

EXERCISE 5.4.4. Let k be a field and $k[x]$ the polynomial ring over k in one variable. Show that $A = k[x]$ is not separable over k. (Hint: Show that A^e is an integral domain.)

EXERCISE 5.4.5. Let R be a commutative ring. Show that $A = R[x]$ is not separable over R.

EXERCISE 5.4.6. Let $A = \mathbb{Z}[i]$ be the ring of gaussian integers. Then up to isomorphism A is equal to $\mathbb{Z}[x]/(x^2+1)$. Show that A is not separable over $\mathbb{Z}$. (Hints: Use Corollary 5.3.2. Take $S = \mathbb{Z}/2$ and apply the argument of Exercise 5.4.3 to show $A \otimes \mathbb{Z}/2$ is not separable over the field $\mathbb{Z}/2$. We say that A *ramifies* at the prime 2.)

EXERCISE 5.4.7. Let R be an integral domain in which $2 = 1+1$ is a unit. Let a be a unit of R and define $S = R[\sqrt{a}]$ to be R with the square root of a adjoined. That is, $S = R[x]/(x^2 - a)$.

(1) Show that S is a faithfully flat R-algebra. (Hint: Example 1.6.10 (2).)
(2) Show that the $\sqrt{a} \mapsto -\sqrt{a}$ induces an R-algebra automorphism $\sigma\colon S \to S$. (Hint: Exercise 1.1.7.)
(3) The trace map $T\colon S \to R$ is defined by $T(z) = z + \sigma(z)$. Show that T is an R-module homomorphism and the image of T is R. Show that the kernel of T is the R-submodule generated by $\sqrt{a}$. Conclude that $S \cong R \cdot 1 \oplus R\sqrt{a}$ as R-modules.
(4) If $\mathfrak{m}$ is any maximal ideal in S, then $\mathfrak{m}$ does not contain the R-submodule $R\sqrt{a}$.
(5) Show that S is a separable R-algebra. (Hint: $e = \frac{1}{2}(1 \otimes 1 + \sqrt{a} \otimes \frac{1}{\sqrt{a}})$ is a separability idempotent.)

EXERCISE 5.4.8. Let R be an integral domain in which 2 is a unit. Let $a \in R$ and $S = R[\sqrt{a}] = R[x]/(x^2 - a)$.

(1) If $a = b^2$ and b is a unit in R, then $S \cong R \oplus R$ as R-algebras.
(2) If a is not a unit in R, then S is not separable over R.

EXERCISE 5.4.9. Let the Cartesian plane $\mathbb{R}^2$ have the usual metric space topology. Let X be the x-axis and $\pi\colon \mathbb{R}^2 \to X$ the standard projection map defined by $\pi(x,y) = x$.

(1) Let $S = \mathbb{R}[x,y]/(x^2 - y^2)$ and $R = \mathbb{R}[x]$. Show that S is faithfully flat over R, but is not separable.

    Geometrically, S corresponds to two intersecting lines and R corresponds to the x-axis. In $\mathbb{R}^2$ let Y denote the two lines $x = \pm y$. The projection $\pi\colon Y \to X$ of Y onto the x-axis is two-to-one everywhere except at the origin, hence is not a local homeomorphism.
(2) Let $S = \mathbb{R}[x,y]/(x^2 + y^2 - 1)$. Show that S is faithfully flat over $R = \mathbb{R}[x]$, but is not separable.

    Geometrically, S corresponds to a circle of radius 1 and R corresponds to the x-axis. In $\mathbb{R}^2$ let Y denote the circle $x^2 + y^2 = 1$. The projection $\pi\colon Y \to X$ of Y onto the x-axis is two-to-one everywhere except at the points where $x = \pm 1$, hence is not a local homeomorphism.

EXERCISE 5.4.10. Let R be an integral domain in which 2 is a unit. Assume $i \in R$ such that $i^2 = -1$. Let α and β be units of R. Define an R algebra A by the following rules. As an R-module, A is the free R-module on the basis $1, u, v, uv$:

$$A = R \cdot 1 + R \cdot u + R \cdot v + R \cdot uv.$$

Multiplication in A is determined by the relations

$$u^2 = \alpha, v^2 = \beta, uv = -vu.$$

(1) Show that A is a separable R-algebra. (Hint: $e = \frac{1}{4}(1 \otimes 1 + u \otimes u^{-1} + v \otimes v^{-1} + uv \otimes (uv)^{-1})$ is a separability idempotent.)
(2) Assume $\alpha = a^2$ and $\beta = b^2$ for some a, b in R. Show that A is isomorphic to the ring $M_2(R)$ of two-by-two matrices over R. (Hint: Define the map $A \to M_2(R)$ on generators by

$$u \mapsto \begin{bmatrix} 0 & -ia \\ ia & 0 \end{bmatrix}, \quad v \mapsto \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix}.$$

Show that this definition extends to A.)
(3) If $R = \mathbb{C}$, then $A \cong M_2(\mathbb{C})$ for every choice of α and β.

EXERCISE 5.4.11. Let S be a commutative separable R-algebra. For $n \geq 1$, let $T^n_R(S) = S \otimes_R S \otimes_R \cdots \otimes_R S$ be the tensor product of n copies of S. View $T^n_R(S)$ as an S-algebra by the homomorphism $\rho : S \to T^n_R(S)$, where $\rho(s) = s \otimes 1 \otimes \cdots \otimes 1$. Let $\mu : T^n_R(S) \to S$ be the product map, where $\mu(x_1 \otimes \cdots \otimes x_n) = x_1 \cdots x_n$.

(1) Show that μ is an S-algebra homomorphism and the kernel of μ is idempotent generated.
(2) Show that there is an idempotent $e \in T^n_R(S)$ such that $Se = (S \otimes_R 1 \otimes_R \cdots \otimes_R 1)e = T^n_R(S)e$.

5. Separable Algebras over a Field

The goal of this section is to prove a structure theorem that classifies separable algebras over a given field k. First we show in Section 5.5.1 that A is a central separable k-algebra if and only if A is a central simple k-algebra. The main results on separable k-algebras are Theorem 5.5.7 and its corollaries. Given the connection between central simple and central separable, these results are generalizations of the Wedderburn-Artin Theorem. When k is infinite and A is commutative, we prove that A is generated as a k-algebra by a primitive element. If k is a field and A is a central simple k-algebra, then the Skolem-Noether Theorem shows that any k-algebra automorphism of A is an inner automorphism.

The theorems and their proofs appearing below are from various sources, including [**16**], [**36**], [**49**], [**52**], [**33**], and [**18**].

5.1. Central Simple Equals Central Separable. Let k be a field. As in Definition 4.4.6, a k-algebra A is central simple in case $k = Z(A)$, $\dim_k(A)$ is finite, and A is a simple ring.

PROPOSITION 5.5.1. *Let k be a field and A a finite dimensional k-algebra. Then A is a central simple k-algebra if and only if the enveloping homomorphism $\varphi : A^e \to \operatorname{Hom}_k(A,A)$ of Eq.*(1.3) *is an isomorphism.*

PROOF. If A is a central simple k-algebra, then so is A^o. By Proposition 4.4.9 it follows that A^e is a central simple k-algebra. Therefore φ is one-to-one and counting dimensions over k proves that φ is onto. Conversely, suppose that φ is an isomorphism. Since $\operatorname{Hom}_k(A,A)$ is isomorphic to a ring of matrices $M_n(k)$, it is a central simple k-algebra by Example 4.4.2. If I is a two-sided ideal of A, then $I \otimes_k A^o$ is an ideal in A^e. So I is either (0) or A. If $\alpha \in Z(A)$, then $\alpha \otimes 1 \in Z(A^e)$ so $\varphi(\alpha \otimes 1) \in k$. Since φ is a k-algebra isomorphism, $\alpha \otimes 1 \in k \cdot 1 \otimes 1$. It follows that $\alpha \in k$. □

EXAMPLE 5.5.2. Let k be a field and A a finite dimensional central simple k-algebra. Assume $\dim_k(A) = n \geq 2$. Consider the exact sequence

$$0 \to J_{A/k} \to A \otimes_k A^o \xrightarrow{\mu} A \to 0$$

of Eq. (1.5), where μ is the multiplication map defined by $a \otimes b \mapsto ab$. In this example we show that μ is not a ring homomorphism and $J_{A/k}$ is not a two-sided ideal. By Proposition 5.5.1, the enveloping algebra $A^e = A \otimes_k A^o$ is isomorphic to the endomorphism ring $\operatorname{Hom}_k(A,A)$. Therefore, A^e is a central simple k-algebra, by Example 4.4.2. This implies A^e is a simple ring. Since the multiplication map μ is always onto, we have $\dim_k J_{A/k} = \dim_k(A^e) - \dim_k(A) = n^2 - n > 0$. Since A^e is a simple ring, this implies $J_{A/k}$ is not a two-sided ideal. It follows that μ is not a homomorphism of rings.

COROLLARY 5.5.3. *Let A be a separable k-algebra where k is a field. Then A is a finite dimensional k-vector space.*

PROOF. This follows immediately from Proposition 5.4.5. □

COROLLARY 5.5.4. *Let k be a field and A a k-algebra. Then A is a central simple k-algebra if and only if A is a central separable k-algebra.*

PROOF. Assume A is a central simple k-algebra. Let K be an algebraic closure of k. Then by Theorem 4.4.9, $A \otimes_k K$ is a central simple K-algebra. By Proposition 4.4.8, $A \otimes_k K \cong M_n(K)$ for some n. By Example 5.2.1, $A \otimes_k K$ is a central separable K-algebra. By Corollary 5.3.5, A is a separable k-algebra. Conversely assume A is a central separable k-algebra. Then $Z(A) = k$ and by Corollary 5.5.3, A is finite dimensional over k. Any left A-module is a k-vector space, hence is projective as a k-module. By Theorem 5.4.1, every left A-module is projective. By Theorem 4.3.3, A is semisimple. By Theorem 4.4.3, A is a finite direct sum of simple rings. Since the center of A is the field k, it follows that A is simple. □

5.2. A Separable Field Extension is a Separable Algebra.

THEOREM 5.5.5. *Let k be a field and A a k-algebra. The following are equivalent.*

(1) A is a separable k-algebra.
(2) A is finite dimensional over k and if K/k is any field extension of k, then $A \otimes_k K$ is semisimple.

PROOF. (1) implies (2): By Corollary 5.5.3, A is finite dimensional over k. By Corollary 5.3.2, $A \otimes_k K$ is a separable K-algebra. Every $A \otimes_k K$-module is free over K. By Theorem 5.4.1, every $A \otimes_k K$-module is projective. By Theorem 4.3.3, $A \otimes_k K$ is semisimple.

(2) implies (1): Let $\bar{k}$ be the algebraic closure of k. By Theorem 4.4.3(2), $A \otimes_k \bar{k} = R_1 \oplus \cdots \oplus R_n$ is a direct sum of a finite number of simple rings R_i. Each R_i is finite dimensional over $\bar{k}$. By Theorem 4.4.5, the center of R_i is a finite extension field of $\bar{k}$. Since $\bar{k}$ is algebraically closed, the center of R_i is $\bar{k}$. By Corollary 5.5.4, each R_i is central separable over $\bar{k}$. Therefore $A \otimes_k \bar{k}$ is separable over $\bar{k} \oplus \cdots \oplus \bar{k}$. By Exercise 5.1.4, $\bar{k} \oplus \cdots \oplus \bar{k}$ is separable over $\bar{k}$. By Theorem 5.4.2 (1), $A \otimes_k \bar{k}$ is separable over $\bar{k}$. By Corollary 5.3.5, A is separable over k. □

PROPOSITION 5.5.6. *Let k be a field and F a finite dimensional extension field of k. Then F is a separable k-algebra if and only if F/k is a separable field extension.*

PROOF. Assume F is a separable field extension of k. Then $F = k(u_1,\dots,u_m)$ where each u_i is separable over k. By Theorem 5.4.2 (1), it is enough to assume $F = k[x]/(f(x))$ is a simple extension and prove that F is a separable k-algebra. Let K/k be a splitting field for $f(x)$. In $K[x]$ we have the factorization $f(x) = (x-\alpha_1)\dots(x-\alpha_n)$ where the roots α_i are distinct. The Chinese Remainder Theorem shows that $F \otimes_k K \cong K[x]/(f(x))$ is isomorphic to a direct sum of n copies of K. By Exercise 5.1.4, $F \otimes_k K$ is separable over K. By Corollary 5.3.5, F is a separable k-algebra.

Conversely assume F/k is not a separable extension of fields and let S be the separable closure of k in F (see [**19**, Theorem 5.4.2], for example). Let p be the characteristic of k. Since F/S is purely inseparable, there exists $u \in F$, $n \geq 1$, and $\alpha \in S$ such that the irreducible polynomial of u over S is $\operatorname{Irr.poly}_S(u) = x^{p^n} - \alpha$. Consider the element $t = u \otimes 1 - 1 \otimes u$ in $F \otimes_S F$. It is easy to see that t is nonzero and that $t^{p^n} = 0$. The Jacobson radical of $F \otimes_S F$ contains t, so $F \otimes_S F$ is not a semisimple ring (Theorem 4.3.3). By Theorem 5.5.5, F is not a separable S-algebra. By Theorem 5.4.2 (2), F is not a separable k-algebra. □

THEOREM 5.5.7. *Let k be a field and A a k-algebra. Then A is a separable k-algebra if and only if A is isomorphic to a finite direct sum of matrix rings $M_{n_i}(D_i)$ where each D_i is a finite dimensional k-division algebra such that the center $Z(D_i)$ is a finite separable extension field of k.*

PROOF. If A is separable over k, then by Theorem 5.5.5, A is semisimple. It follows from Theorem 4.4.3(2) that $A = A_1 \oplus \cdots \oplus A_m$ is a direct sum of a finite number of simple rings A_i. By Exercise 5.4.2, A_i is separable over k, for each i. By Theorem 4.4.5, $A_i \cong M_{n_i}(D_i)$ where D_i is a finite dimensional k-division algebra. The center of A_i is $Z(D_i)$ and by Theorem 5.4.2(3), $Z(D_i)$ is separable over k. By Proposition 5.5.6, $Z(D_i)/k$ is a finite separable field extension.

For the converse, suppose K/k is a finite separable field extension and D is a finite dimensional K-central division algebra. Then by Example 4.4.2 and Theorem 4.4.9, $M_n(D) \cong \operatorname{Hom}_K(K^{(n)}, K^{(n)}) \otimes_K D$ is K-central simple. By Corollary 5.5.4, $M_n(D)$ is K-central separable. By Proposition 5.5.6 and Theorem 5.4.2 (1), $M_n(D)$ is separable over k. The part about direct sums follows from Exercise 5.4.2. □

Corollaries 5.5.9 and 5.5.10 are generalizations of the Primitive Element Theorem for a separable extension of fields, which is stated here for reference.

THEOREM 5.5.8. *If F/k is a finite dimensional separable extension of fields, then there is a separable element $u \in F$ such that $F = k(u)$.*

PROOF. [**19**, Theorem 5.2.14]. □

COROLLARY 5.5.9. *Let k be a field and A a commutative k-algebra. Then the following are true.*

(1) A is separable over k if and only if A is isomorphic to a finite direct sum of fields $K_1 \oplus \cdots \oplus K_n$ where each K_i is a finite separable extension field of k.

(2) If k is infinite and A is separable over k, then there is a monic polynomial $f(x) \in k[x]$ such that $\gcd(f, f') = 1$ and A is isomorphic to $k[x]/(f(x))$ as a k-algebra. There is a primitive element $\alpha \in A$ such that A is generated as a k-algebra by α.

PROOF. (1): Follows from Theorem 5.5.7.

(2): By Part (1), there is a k-algebra isomorphism $A \cong K_1 \oplus \cdots \oplus K_n$, where each K_i is a separable extension field of k. By Theorem 5.5.8, $K_i \cong k[x]/(p_i(x))$, for some irreducible monic separable polynomial $p_i(x) \in k[x]$. By induction, assume $n \geq 2$ and there is a monic polynomial $f(x)$ such that $\gcd(f, f') = 1$ and $K_2 \oplus \cdots \oplus K_n$ is isomorphic to $k[x]/(f(x))$ as a k-algebra. Let F be a splitting field for $f(x)p_1(x)$. Let $\{u_1, \ldots, u_r\}$ be all the roots of $f(x)p_1(x)$ in F. Assume $p_1(u_1) = 0$. Since k is infinite, pick $a \in k$ such that a is not in the set $\{0, u_2 - u_1, \ldots, u_r - u_1\}$. So $p_1(x-1)$ is a monic irreducible separable polynomial in $k[x]$ and $a + u_1$ is a root of $p_1(x-a)$ but not a root of $f(x)$. Therefore, $p_1(x-a)$ does not divide $f(x)$. Hence $p_1(x-a)f(x)$ is a separable polynomial. By the Chinese Remainder Theorem, Theorem 1.1.7,

$$\frac{k[x]}{(p_1(x-a)f(x))} \to \frac{k[x]}{(p_1(x-a))} \bigoplus \frac{k[x]}{(f(x))}$$

is an isomorphism. But the k-algebra on the right is isomorphic to A. $\square$

Corollary 5.5.10 is a kind of "Primitive Element Theorem" for commutative separable algebras over a finite field which is due to T. McKenzie ([**43**]).

COROLLARY 5.5.10. *If k is a finite field and A is a commutative separable k-algebra, then there is a monic polynomial $f(x) \in k[x]$ such that* $\gcd(f, f') = 1$ *and A is isomorphic to a k-subalgebra of* $k[x]/(f(x))$.

PROOF. By Corollary 5.5.9 (1), there is a k-algebra isomorphism $A \cong K_1 \oplus \cdots \oplus K_n$, where each K_i is a separable extension field of k. Let $d_i = \dim_k(K_i)$, and $d = \operatorname{lcm}(d_1, \ldots, d_n)$. By [**19**, Exercise 5.5.24] there exists a polynomial $f(x) \in k[x]$ such that $\gcd(f, f') = 1$ and $k[x]/(f(x))$ is isomorphic to the direct sum $F \oplus \cdots \oplus F$ of n copies of the field F, where $\dim_k(F) = dm$, for some $m \geq 1$. By Theorem 1.8.7, F contains a subfield isomorphic to K_i, and we can embed A into $k[x]/(f(x))$. $\square$

5.3. The Skolem-Noether Theorem.

THEOREM 5.5.11. *(Skolem-Noether) Let A be a central simple k-algebra. Let B and $\tilde{B}$ be two simple k-subalgebras of A and $\varphi : B \to \tilde{B}$ a k-algebra isomorphism. Then φ extends to an inner automorphism of A. That is, there exists an invertible $u \in A$ such that $\varphi(x) = uxu^{-1}$, for all $x \in B$.*

PROOF. By Theorem 4.4.5, if M is a minimal left ideal of A, then $D = \operatorname{Hom}_A(M, M)$ is a division ring, and $A \cong \operatorname{Hom}_D(M, M)$. For $a \in A$, let $\lambda_a : M \to M$ be "left multiplication by a". For all $x \in M$, $d \in D$, $b \in B$, we have $\lambda_d \lambda_b x = \lambda_b \lambda_d x$. Therefore, we can make M into a left $D \otimes_k B$-module by $d \otimes b \cdot x = dbx$. Using φ, define a second left $D \otimes_k B$-module structure on M by $d \otimes b \cdot x = d\varphi(b)x$. Denote this module by ${}_{\varphi}M$. By Theorem 4.4.9, $D \otimes_k B$ is a simple ring. It follows from Theorem 4.3.1 and Theorem 4.4.3 that V and ${}_{\varphi}M$ are isomorphic $D \otimes_k B$-modules. Therefore, there exists an isomorphism $\theta \in \operatorname{Hom}_k(M, M)$ satisfying:

$$\theta(d \otimes b \cdot x) = d \otimes b \cdot \theta(x) = d\varphi(b)\theta(x).$$

For $b = 1$, this implies $\theta(dx) = d\theta(x)$, so $\theta \in \operatorname{Hom}_D(M, M) = A$. That is, $\theta = \lambda_u$, for some invertible $u \in A$. The equation above becomes

$$u(db)x = d\varphi(b)ux.$$

If $d = 1$, this becomes: $ubx = \varphi(b)ux$. Since M is a faithful module (Theorem 4.4.3), this proves $\varphi(b) = ubu^{-1}$. $\square$

COROLLARY 5.5.12. *Let k be a field and A a central simple k-algebra. If $\theta : A \to A$ is a k-algebra homomorphism, then θ is an inner automorphism of A.*

PROOF. Since A is simple, the kernel of θ is the zero ideal, hence θ is one-to-one. The image of θ has dimension $\dim_k(A)$, hence θ is onto. □

5.4. Exercises.

EXERCISE 5.5.1. Let k be a field and $f \in k[x]$ a monic polynomial. Let $S = k[x]/(f)$. Show that S/k is separable if and only if $\gcd(f, f') = 1$. For a generalization of this result, see Proposition 5.6.2.

EXERCISE 5.5.2. Let k be a field and G a finite group of order $[G:1]$.

(1) (Maschke's Theorem) If $[G:1]$ is invertible in k, then the group algebra $k(G)$ is semisimple.
(2) This exercise contains an outline of a proof of the converse to Maschke's Theorem. In the group algebra $k(G)$, let $t = \sum_{\sigma \in G} \sigma$ and $I = k(G)t$ be the left ideal generated by t.
  (a) Show that I is equal to kt.
  (b) Show that if the characteristic of k divides $[G:1]$, then $I^2 = 0$. Conclude that I is not a $k(G)$-module direct summand of $k(G)$.
  (c) Show that if the group algebra $k(G)$ is semisimple, then $[G:1]$ is invertible in k.

EXERCISE 5.5.3. The purpose of this exercise is to prove the converse of Example 5.2.2. Let R be a commutative ring and G a finite group of order $[G:1]$. Show that if the group algebra $R(G)$ is separable over R, then $[G:1]$ is invertible in R. (Hint: If $\mathfrak{m}$ is a maximal ideal in R which contains $[G:1]$, then by Exercise 5.5.2, the group algebra $(R/\mathfrak{m})(G)$ is not semisimple.)

EXERCISE 5.5.4. Let $\theta : R \to S$ be a local homomorphism of local rings and assume θ makes S into a separable R-algebra. Let $\mathfrak{m}$ be the maximal ideal of R, $\mathfrak{n}$ the maximal ideal of S, and $R/\mathfrak{m} \to S/\mathfrak{n}$ the corresponding extension of residue fields. Then $\mathfrak{m}S = \mathfrak{n}$, $S \otimes_R R/\mathfrak{m} = S/\mathfrak{n}$, and $R/\mathfrak{m} \to S/\mathfrak{n}$ is a finite separable extension of fields.

EXERCISE 5.5.5. This exercise generalizes Exercises 5.4.7 (5) and 5.4.8 (2). Let $n \geq 2$ be an integer and R a commutative ring. Prove the following for $S = R[x]/(x^n - a)$.

(1) S is free of rank n as an R-module with basis $1, x, \dots, x^{n-1}$.
(2) If na is a unit of R, then x is a unit of S and S is a separable R-algebra. (Hint: $e = \frac{1}{n} \sum_{i=0}^{n-1} x^i \otimes x^{-i}$ is a separability idempotent.)
(3) If n is not a unit of R, then S is not separable over R.
(4) If a is not a unit of R, then S is not separable over R.

6. Commutative Separable Algebras

In this section we study R-algebras that are separable and commutative. References for the material in this section are [**52**] and [**33**]. If S is a commutative ring and R is a subring of S, then we say S/R is an *extension of commutative rings*.

DEFINITION 5.6.1. Let R be a commutative ring. A monic polynomial $f(x)$ in $R[x]$ is called *separable* in case $R[x]/(f(x))$ is separable over R. If S/R is an extension of commutative rings, and $b \in S$, then we say b is a *separable element* in S in case there is a separable polynomial $f(x) \in R[x]$ and $f(b) = 0$.

Proposition 5.6.2, a generalization of Exercise 5.5.1, provides a useful Jacobian Criterion for a polynomial to be separable. The proof we give below is from [**52**, Proposition 2.16]. See Proposition 10.2.7 for a more general version that applies when the extension S/R is not necessarily a simple extension.

PROPOSITION 5.6.2. *Let R be a commutative ring and $f(x)$ a monic polynomial in $R[x]$. Let $I = (f(x), f'(x))$ be the ideal of $R[x]$ generated by $f(x)$ and the formal derivative, $f'(x)$. Let $S = R[x]/(f(x))$. Then the following are true.*

(1) S is a free R-module. $\operatorname{Rank}_R(S) = \deg(f(x))$.
(2) S is separable over R if and only if the ideal I is the unit ideal.

PROOF. (1): This is Example 1.6.10 (2).

(2): Assume I is not the unit ideal of $R[x]$. By (1), $R[x]/I$ is a finitely generated R-module. By Nakayama's Lemma (Corollary 2.2.2), there is a maximal ideal $\mathfrak{m}$ in R such that

$$(R[x]/I) \otimes_R (R/\mathfrak{m}) = \frac{(R/\mathfrak{m})[x]}{(f, f')}$$

is nonzero. Let $k = R/\mathfrak{m}$. Then in $k[x]$, (f, f') is not the unit ideal. By Exercise 5.5.1, $S \otimes_R k$ is not separable over k. By Corollary 5.3.2, S is not separable over R.

Now we prove the converse of (2). In $R[x,y]$, $y - x$ is monic in y and linear, so the Division Algorithm applies. Upon dividing $f(y) - f(x)$ by $y - x$ one finds the remainder is 0. We can write $f(y) = f(x) + (y-x)q(x,y)$. Compute the derivative with respect to y: $f'(y) = q(x,y) + (y-x)q_y(x,y)$. By assumption, there are $u(y), v(y) \in R[y]$ such that

$$\begin{aligned} 1 &= f(y)u(y) + f'(y)v(y) \\ &= \big(f(x) + (y-x)q(x,y)\big)u(y) + (q(x,y) + (y-x)q_y(x,y))v(y) \qquad (6.1) \\ &= (y-x)\big(q(x,y)u(y) + q_y(x,y)v(y)\big) + f(x)u(y) + q(x,y)v(y) \end{aligned}$$

Under the mapping $R[x,y] \to S[y]$, all of the polynomials above represent elements in $S[y]$. Consider the principal ideals $A = (y-x)$, $B = (q(x,y))$ in $S[y]$. By (6.1), A and B are comaximal in $S[y]$. By Exercise 1.1.9, $A \cap B = AB$. But in $S[y]$ the equation $f(y) = (y-x)q(x,y)$ holds. The Chinese Remainder Theorem, Theorem 1.1.7, implies

$$\frac{S[y]}{(f(y))} \xrightarrow{\phi_1 \oplus \phi_2} \frac{S[y]}{(y-x)} \bigoplus \frac{S[y]}{(q(x,y))} \qquad (6.2)$$

is an isomorphism. To interpret the map $\mu : S \otimes_R S \to S$ of Eq.(1.4), it is convenient to write the generators of the three copies of S as x, y, and z. Then $\mu(x \otimes 1) = \mu(1 \otimes y) = z$. The diagram

$$\begin{tikzcd} S \otimes_R S \arrow[r, "\mu"] \arrow[d] & S \arrow[d] \\ \frac{R[x]}{(f(x))} \otimes_R \frac{R[y]}{(f(y))} \arrow[r, "\mu"] \arrow[d] & \frac{R[z]}{(f(z))} \arrow[d] \\ S \otimes_R \frac{R[y]}{(f(y))} \arrow[r, "\phi_1"] & \frac{S[y]}{(y-x)} \end{tikzcd}$$

commutes, the vertical maps are isomorphisms. As we have already seen in (6.2), the kernel of ϕ_1 is idempotent generated. $\square$

6.1. Algebras over Local Rings. Given a local ring R with residue field k, Corollary 5.6.3 shows that a separable finite simple field extension $k(u)/k$ lifts to an extension of local rings S/R where S is a commutative separable R-algebra that is generated by a primitive element and as an R-module is finitely generated and faithfully flat. The proof given below is from [**52**, Corollary 2.17]. See Section 11.5.2 for similar existence theorems in the larger category of all faithfully flat local R-algebras S.

COROLLARY 5.6.3. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field k. Let F be a finite dimensional commutative k-algebra such that $\dim_k(F) = n$. Assume F is generated as a k-algebra by a primitive element u. Then there is a commutative faithful R-algebra S satisfying the following.*

(1) S is a free R-module of rank n.
(2) S is generated as an R-algebra by a primitive element a.
(3) $S \otimes_R k$ is isomorphic to F.
(4) If F is a field, then S is a local ring and $\mathfrak{m}S$ is the maximal ideal of S.
(5) If F/k is a separable extension, then S/R is separable.

PROOF. Let $\theta : k[x] \to F$ be defined by $x \mapsto u$. Let $f \in k[x]$ be the monic polynomial that generates the kernel of θ. Since θ is onto, f has degree n. Lift f to a monic polynomial $g \in R[x]$. Set $S = R[x]/(g)$.

(1): This is Example 1.6.10 (2).

(2): Take a to be the image of x.

(3): This follows from $S \otimes_R k = k[x]/(f) = F$.

(4): If F is a field, then by (3), it follows that $\mathfrak{m}S$ is a maximal ideal of S. By Exercise 2.2.14, S is a local ring.

(5): Under the map $R[x] \to k[x]$, the ideal (g, g') in $R[x]$ restricts to the ideal (f, f') in $k[x]$. Since F/k is separable, Proposition 5.6.2 implies $(f, f') = k[x]$. Since $R[x]/(g, g')$ is a finitely generated R-module, Nakayama's Lemma (Corollary 2.2.2) implies $(g, g') = R[x]$. Proposition 5.6.2 implies S/R is separable. $\square$

COROLLARY 5.6.4. *Let $\theta : R \to S$ be a local homomorphism of local rings such that S is a separable R-algebra and finitely generated as an R-module. Then S is a homomorphic image of $R[x]$. That is, S is generated as an R-algebra by a primitive element a.*

PROOF. Let $\mathfrak{m}$ be the maximal ideal of R, and k the residue field. By Exercise 5.5.4, $\mathfrak{m}S$ is equal to the maximal ideal of S, and $S/\mathfrak{m}S$ is a finite separable extension field of k. By Theorem 5.5.8, $S/\mathfrak{m}S = k(u)$ is a simple extension. Define $\phi : R[x] \to S$ by $x \mapsto a$, where $a \in S$ is a preimage of u. Then $R[x] \otimes_R k \to S \otimes_R k$ is onto, S is generated as an R-module by $\operatorname{im}(\phi)$ and $\mathfrak{m}S$, and Nakayama's Lemma (Corollary 2.2.5) implies ϕ is onto. $\square$

If the residue field of R is infinite, then Corollary 5.6.5, which is from [**33**, Lemma 3.1], shows that it is not necessary to assume S is local.

COROLLARY 5.6.5. *Let R be a local ring with infinite residue field k. If S is a separable R-algebra which is finitely generated as an R-module, then S is a homomorphic image of $R[x]$. That is, S is generated as an R-algebra by a primitive element a.*

PROOF. By Corollary 5.5.9, there is a monic separable polynomial $f \in k[x]$ such that $\gcd(f, f') = 1$ and $k[x]/(f) \cong S \otimes_R k$. The rest of the proof is as in Corollary 5.6.4. $\square$

6.2. Separability and the Trace. Let F/k be a finite dimensional separable extension of fields. In Definition 1.8.5 the trace map $T_k^F : F \to k$ is defined and some of its important properties are derived in Lemma 1.8.6. In this section we generalize this definition. For an extension of commutative rings S/R such that S is finitely generated and projective as an R-module, we derive necessary and sufficient conditions in terms of the trace map for S to be R-separable. Theorem 5.6.7, which is fundamental, and its proof are from [**16**, Theorem 3.2.1].

DEFINITION 5.6.6. Let A be any R-algebra. Let M be a left A-module which as an R-module is finitely generated and projective. Let $x_1,\dots,x_m \in M$ and $f_1,\dots,f_m \in \operatorname{Hom}_R(M,R)$ be a dual basis for the R-module M. Define $T_R^{A,M} : A \to R$ by the rule

$$T_R^{A,M}(x) = \sum_{i=1}^{m} f_i(xx_i).$$

The reader should verify that $T_R^{A,M} \in \operatorname{Hom}_R(A,R)$. We call $T_R^{A,M}$ the *trace from A to R afforded by M*. By Exercise 5.6.1, $T_R^{A,M}$ is independent of the choice of a dual basis for M. When $M = A$, we simplify the notation and write T_R^A. The reader should verify that $T_R^R(x) = x$ for all $x \in R$.

THEOREM 5.6.7. *Let S/R be an extension of commutative rings. Then S is finitely generated as an R-module, projective, and separable over R if and only if there exists an element $T \in \operatorname{Hom}_R(S,R)$ and elements $x_1,\dots,x_n$, $y_1,\dots,y_n$ in S satisfying*

(1) $\displaystyle\sum_{j=1}^{n} x_j y_j = 1$, *and*

(2) $\displaystyle\sum_{j=1}^{n} x_j T(y_j x) = x$ *for all* $x \in S$.

Moreover, the map T is always equal to T_R^S, the trace map from S to R.

PROOF. Assume S is a finitely generated R-module, projective, and separable over R. Pick a dual basis $\{a_1,\dots,a_m\}$, $\{f_1,\dots,f_m\}$ for the R-module S. The trace map from S to R is given by

$$T_R^S(x) = \sum_{j=1}^{m} f_j(xa_j)$$

for all $x \in S$. Since S is a finitely generated, projective extension of R, by Theorem 2.3.23, $S \otimes S$ is a finitely generated projective extension of $S \otimes 1$. A dual basis for $S \otimes S$ over $S \otimes 1$ is $\{1 \otimes a_1,\dots,1 \otimes a_m\}$, $\{1 \otimes f_1,\dots,1 \otimes f_m\}$ and the trace map from $S \otimes S$ to $S \otimes 1$ is equal to $T_{S\otimes 1}^{S\otimes S} = 1 \otimes T_R^S$. Since S is a separable extension of R, $S \otimes S$ is a separable extension of $S \otimes 1$, by Corollary 5.3.2. Let e be a separability idempotent for S over R. Under the homomorphism μ of Proposition 5.1.2, $(S \otimes 1)e \cong S \otimes 1$. By Proposition 5.1.2, as $S \otimes S$-modules, we have $S \otimes S \cong J_{A/R} \oplus (S \otimes 1)e \cong J_{A/R} \oplus (S \otimes 1)$. Exercise 5.6.2 allows us to write the trace from $S \otimes S$ to $S \otimes 1$ as the sum

$$T_{S\otimes 1}^{S\otimes S} = T_{S\otimes 1}^{J_{A/R}} + T_{S\otimes 1}^{S\otimes 1},$$

where $T_{S\otimes 1}^{J_{A/R}}$ is the restriction of the trace map to $J_{A/R}$ and $T_{S\otimes 1}^{S\otimes 1}$ is the restriction to $(S \otimes 1)e$. To compute $T_{S\otimes 1}^{S\otimes 1}$, use the dual basis $\{e,\sigma\}$ where $\sigma : (S \otimes 1)e \to S \otimes 1$ is the isomorphism defined by $\sigma(e) = 1$. For any $x \in S$,

$$\begin{aligned} T_{S\otimes 1}^{S\otimes S}((x\otimes 1)e) &= T_{S\otimes 1}^{J_{A/R}}((x\otimes 1)e) + T_{S\otimes 1}^{S\otimes 1}((x\otimes 1)e) \\ &= T_{S\otimes 1}^{S\otimes 1}((x\otimes 1)e) \\ &= x \otimes 1. \end{aligned}$$

Now let $x \in S$ and let $e = \sum_{j=1}^{n} x_j \otimes y_j$. Then (1) follows from $\mu(e) = \sum_{j=1}^{n} x_j y_j = 1$ and (2) follows from applying μ to both sides of

$$\begin{aligned} x \otimes 1 &= T_{S\otimes 1}^{S\otimes S}((x \otimes 1) \cdot e) \\ &= T_{S\otimes 1}^{S\otimes S}((1 \otimes x) \cdot e) \\ &= \left(1 \otimes T_R^S\right) \left(\sum_{j=1}^{n} x_j \otimes y_j x \right) \\ &= \sum_{j=1}^{n} x_j \otimes T_R^S(y_j x). \end{aligned}$$

Conversely, suppose we are given $T \in \operatorname{Hom}_R(S,R)$ and elements $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ in S satisfying (1) and (2). The reader should verify that the assignment $s \mapsto T(y_j s)$ defines an element $T(y_j \cdot)$ in $\operatorname{Hom}_R(S,R)$. The set $\{x_1, \ldots, x_n\}$, $\{T(y_1 \cdot), \ldots, T(y_n \cdot)\}$ forms a dual basis for S over R. Therefore S is a finitely generated, projective R-module. Define an element in $S \otimes_R S$ by $e = \sum_{j=1}^{n} x_j \otimes y_j$. If μ is as in Proposition 5.1.2, $\mu(e) = \sum_{j=1}^{n} x_j y_j = 1$. For any $x \in S$,

$$\begin{aligned} (1 \otimes x)e &= \sum_{j=1}^{n} x_j \otimes y_j x \\ &= \sum_{j=1}^{n} \sum_{i=1}^{n} x_j \otimes x_i T(y_i y_j x) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} x_j T(y_j y_i x) \otimes x_i \\ &= \sum_{i=1}^{n} x y_i \otimes x_i. \end{aligned}$$

If $x = 1$, then we see $e = \sum_{j=1}^{n} x_j \otimes y_j = \sum_{i=1}^{n} y_i \otimes x_i$. It follows that $(1 \otimes x)e = (x \otimes 1)e$ and by Proposition 5.1.2, S is separable over R.

Lastly, the set $\{x_1, \ldots, x_n\}$, $\{T(y_1 \cdot), \ldots, T(y_n \cdot)\}$ is a dual basis for S over R, so by Exercise 5.6.1,

$$T_R^S(x) = \sum_{j=1}^{n} T(y_j x x_j) = T(x \sum_{j=1}^{n} x_j y_j) = T(x).$$

□

Assume S/R is an extension of commutative rings. As we saw in Example 1.1.13, there is an R-algebra embedding $\theta \colon S \to \operatorname{Hom}_R(S,S)$ given by $\alpha \mapsto \ell_\alpha$ where ℓ_α is "left multiplication by α". Using Lemma 2.4.1, we turn $\operatorname{Hom}_R(S,R)$ into a right S-module. In fact, for every $f \in \operatorname{Hom}_R(S,R)$ and $\alpha \in S$, $f\alpha$ is defined to be $f \circ \ell_\alpha$.

COROLLARY 5.6.8. *Let S/R be an extension of commutative rings such that S is a finitely generated projective R-module. Then S is separable over R if and only if the trace map T_R^S from S to R is a free right S-module generator of* $\operatorname{Hom}_R(S,R)$.

PROOF. Assume S/R is a separable extension of R which is a finitely generated projective R-module. Let $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ be elements in R guaranteed by Theorem 5.6.7.

For any $f \in \operatorname{Hom}_R(S,R)$ and any $x \in S$

$$\begin{aligned} f(x) &= \sum_{j=1}^{n} f\big(x_j T_R^S(y_j x)\big) \\ &= \sum_{j=1}^{n} T_R^S(y_j x) f(x_j) \\ &= T_R^S\big(\sum_{j=1}^{n} y_j x f(x_j)\big). \end{aligned}$$

Let $\alpha = \sum_{j=1}^{n} f(x_j) y_j$. Then $f(x) = T_R^S(\alpha x)$, for all $x \in S$, which shows that $f = T_R^S \circ \ell_\alpha$. If $T_R^S \alpha = 0$ in $\operatorname{Hom}_R(S,R)$, then by Theorem 5.6.7(2),

$$0 = \sum_{j=1}^{n} x_j T_R^S(y_j \alpha) = \alpha.$$

This shows that the assignment $\alpha \mapsto T_R^S \alpha$ defines an S-module isomorphism $S \cong \operatorname{Hom}_R(S,R)$.

Conversely suppose $x_1, \dots, x_m$, $f_1, \dots, f_m$ is a dual basis for S over R. Assuming T_R^S generates $\operatorname{Hom}_R(S,R)$ as an S-module, there exist $y_1, \dots, y_m$ in S such that $f_j = T_R^S \circ \ell_{y_j}$. We prove that (1) and (2) of Theorem 5.6.7 are satisfied. For any $x \in S$,

$$x = \sum_{j=1}^{m} f_j(x) x_j = \sum_{j=1}^{m} x_j T_R^S(y_j x)$$

which is (2). For any $z \in S$

$$\begin{aligned} T_R^S\Big(\big(1 - \sum_{j=1}^{m} x_j y_j\big) z\Big) &= T_R^S(z) - T_R^S\Big(\sum_{j=1}^{m} x_j y_j z\Big) \\ &= \sum_{j=1}^{m} f_j(z x_j) - T_R^S\Big(\sum_{j=1}^{m} x_j y_j z\Big) \\ &= \sum_{j=1}^{m} T_R^S(y_j z x_j) - T_R^S\Big(\sum_{j=1}^{m} x_j y_j z\Big) \\ &= T_R^S\Big(\sum_{j=1}^{m} y_j x_j z\Big) - T_R^S\Big(\sum_{j=1}^{m} x_j y_j z\Big) \\ &= 0. \end{aligned}$$

Since T_R^S is a free generator of $\operatorname{Hom}_R(S,R)$, we conclude that $\displaystyle\sum_{j=1}^{m} x_j y_j = 1$ which is (1). $\square$

COROLLARY 5.6.9. *If S is a separable extension of R which is a finitely generated projective R-module, and T_R^S is the trace map from S to R, then there is an element $c \in S$ with $T_R^S(c) = 1$. Moreover $R \cdot c$ is an R-module direct summand of S.*

PROOF. By hypothesis, S is finitely generated projective and faithful as an R-module. By Corollary 2.2.4, S is an R-progenerator module. There exist elements $f_1, \dots, f_n$ in $\operatorname{Hom}_R(S,R)$ and $x_1, \dots, x_n$ in S with $1 = \sum_{j=1}^{n} f_j(x_j)$. By Corollary 5.6.8, for each j there is a unique element $a_j \in S$ such that $f_j(x) = T_R^S(a_j x)$ for all $x \in S$. Set $c = \sum_{j=1}^{n} a_j x_j$. Then $T_R^S(c) = 1$. The R-module homomorphism $R \to S$ which is defined by $1 \mapsto c$ is split by the trace map $T_R^S \colon S \to R$. $\square$

6.3. Twisted Form of the trivial extension. Let R be a commutative ring and $n \geq 1$. We write R^n for the direct sum $R \oplus \cdots \oplus R$. By Exercise 5.1.4, R^n is separable over R. We call R^n the *trivial* commutative separable extension of R of rank n. An R-algebra S is said to be a *twisted form of* R^n if there is a faithfully flat R-algebra T and an isomorphism of T-algebras $S \otimes_R T \cong R^n \otimes_R T$. Proposition 5.6.10 gives a criterion for separability in terms of twisted forms of R^n. The proof given below is based on [**52**, Proposition 2.18].

PROPOSITION 5.6.10. *Let S be a commutative R-algebra. The following are equivalent.*

(1) S is a separable R-algebra and an R-module progenerator of constant rank n.
(2) There is a commutative separable R-algebra T which is an R-module progenerator of constant rank $n!$ and $S \otimes_R T \cong T^n$ as T-algebras.
(3) There is a faithfully flat R-algebra T such that $S \otimes_R T \cong T^n$ as T-algebras.

PROOF. (1) implies (2): Let $e \in S \otimes_R S$ be a separability idempotent. Then $S \otimes_R S = (S \otimes_R S)e \oplus (S \otimes_R S)(1-e)$ and $(S \otimes_R S)e \cong S$. Using Exercise 5.4.2 one can check that $(S \otimes_R S)(1-e)$ is separable over S and is an S-module progenerator of constant rank $n-1$. By Proposition 3.4.5, $S \otimes_R S$ is an S-module progenerator of rank $n-1$. If $n = 1$, then we take $T = S$. Otherwise, inductively, there is a commutative separable S-algebra T which is an S-module progenerator of rank $(n-1)!$ such that $(S \otimes_R S)(1-e) \otimes_S T \cong T^{n-1}$. The reader should verify that T is a separable R-algebra, an R-module progenerator of rank $n!$, and $S \otimes_R T \cong T^n$.

(2) implies (3): By Proposition 3.5.6, T is faithfully flat.

(3) implies (1): We are given that T is faithfully flat over R and $S \otimes_R T \cong T^n$. Using this and Lemma 3.5.12, the reader should verify that S is an R-module which is a progenerator of constant rank n. A projective dual basis for S over R gives rise to a dual basis for $S \otimes_R T$, so the trace $T_T^{S \otimes_R T}$ is $T_R^S \otimes 1$. By Proposition 3.5.9, we see that $T_R^S \otimes 1$ is a free right $S \otimes_R T$-module generator of $\operatorname{Hom}_R(S,R) \otimes_R T$. Using the fact that T is faithfully flat over R, the reader should verify that T_R^S is a free right S-module generator for $\operatorname{Hom}_R(S,R)$. Corollary 5.6.8 implies S is separable over R. $\square$

6.4. The Trivial Galois Extension of a Field. In this section we derive some results on separable field extensions that will be used in the proof of Dirichlet's Unit Theorem, Section 12.8.2.

EXAMPLE 5.6.11. Let R be a commutative ring and G a finite group of order $n = [G : 1]$. As in Section 5.6.3, let $S = \bigoplus_{\sigma \in G} Re_\sigma$ be the trivial commutative separable extension of R of rank n. For $\tau \in G$, let $\lambda_\tau : G \to G$ be "left multiplication by τ". Using λ we make S into a left $\mathbb{Z}G$-module. The G-action is defined on the basis $\{e_\sigma \mid \sigma \in G\}$ by $\lambda_\tau(e_\sigma) = e_{\tau\sigma}$. Denote by S_λ the R-algebra S with the left $\mathbb{Z}G$-module defined using λ. Following [**18**, Example 12.2.5], we call S_λ the *trivial, or split, G-Galois extension of R*. Now let $\rho_\tau : G \to G$ be "right multiplication by τ^{-1}". Using ρ we define another $\mathbb{Z}G$-module structure on S. This G-action is defined on the basis $\{e_\sigma \mid \sigma \in G\}$ by the rule $\rho_\tau(e_\sigma) = e_{\sigma\tau^{-1}}$. Denote by S_ρ the R-algebra S with the left $\mathbb{Z}G$-module defined using ρ. The two $\mathbb{Z}G$-actions we have just defined on the R-algebra S are isomorphic. To see this, define $h : S_\lambda \to S_\rho$ on the basis $\{e_\sigma \mid \sigma \in G\}$ by $h(e_\sigma) = e_{\sigma^{-1}}$. For $\tau \in G$ we have $h(\lambda_\tau e_\sigma) = h(e_{\tau\sigma}) = e_{\sigma^{-1}\tau^{-1}}$ which is equal to $\rho_\tau h(e_\sigma) = \rho_\tau e_{\sigma^{-1}} = e_{\sigma^{-1}\tau^{-1}}$. Although it is not required for our purposes here, the interested reader is referred to Chapter 12 of [**18**] for an introduction to Galois Theory of commutative rings.

Now we establish some notation that will be in effect for the remainder of this section. Let F/k be a Galois extension of fields with finite group $G = \operatorname{Aut}_k(F)$ of order $n = [G:1]$. By Theorem 5.5.8, there exists a separable element $u \in F$ such that $F = k(u)$. Let $f = \operatorname{Irr.poly}_k(u)$ be the irreducible polynomial for u over k. Let $\bar{k}$ be any splitting field for f containing k. In Proposition 5.6.12 we show that $F \otimes_k \bar{k}$ is a trivial G-Galois extension of $\bar{k}$. The rings defined so far make up the following commutative diagram. Each arrow is a one-to-one homomorphism of rings.

$$\begin{tikzcd}
 & & F \otimes_k \bar{k} = \frac{\bar{k}[x]}{(f)} \\
F = k(u) = \frac{k[x]}{(f)} \arrow[urr, "\phi"] & & \bar{k} \arrow[u] \\
k \arrow[u] \arrow[urr] & &
\end{tikzcd}$$

PROPOSITION 5.6.12. *Let F/k be a Galois extension of fields with finite group $G = \operatorname{Aut}_k(F)$. Suppose $F = k(u)$, $f = \operatorname{Irr.poly}_k(u)$ and $\bar{k}$ is a splitting field for f containing k. Then $F \otimes_k \bar{k}$ is a trivial G-Galois extension of $\bar{k}$.*

PROOF. We know from Exercise 1.8.3 that in the polynomial ring $\bar{k}[x]$, the polynomial f has the splitting $f = \prod_{\sigma \in G}(x - \sigma(u))$. By the Chinese Remainder Theorem, Theorem 1.1.7,

$$F \otimes_k \bar{k} = \frac{\bar{k}[x]}{(f)} = \bigoplus_{\sigma \in G} \frac{\bar{k}[x]}{(x - \sigma(u))} = \bigoplus_{\sigma \in G} \bar{k} e_\sigma \tag{6.3}$$

where $\{e_\sigma \mid \sigma \in G\}$ are the idempotents in $F \otimes_k \bar{k}$ corresponding to the direct sum decomposition. For each $\sigma \in G$, the projection map $\pi_\sigma : \bigoplus_{\sigma \in G} \bar{k} e_\sigma \to \bar{k} e_\sigma$ is a ring homomorphism. The ring homomorphism

$$\phi : F \to F \otimes_k \bar{k} = \bigoplus_{\sigma \in G} \bar{k} e_\sigma$$

is one-to-one and

$$\phi(u) = \sum_{\sigma \in G} \sigma(u) e_\sigma. \tag{6.4}$$

Let $\alpha \in F$ be an arbitrary element of F. If $n = [G:1]$, there are unique $a_0, \dots, a_{n-1}$ in k such that $\alpha = \sum_{i=0}^{n-1} a_i u^i$. Hence

$$
\begin{aligned}
\phi(\alpha) &= \sum_{i=0}^{n-1} a_i (\phi(u))^i \\
&= \sum_{i=0}^{n-1} a_i \left(\sum_{\sigma \in G} \sigma(u) e_\sigma \right)^i \\
&= \sum_{i=0}^{n-1} \left(\sum_{\sigma \in G} a_i (\sigma(u))^i e_\sigma \right) \\
&= \sum_{\sigma \in G} \left(\sum_{i=0}^{n-1} a_i (\sigma(u))^i \right) e_\sigma \\
&= \sum_{\sigma \in G} \sigma(\alpha) e_\sigma .
\end{aligned}
\tag{6.5}
$$

For each $\tau \in G$, the diagram

$$
\begin{tikzcd}
F \arrow[r, "\tau"] \arrow[d, "\phi"'] & F \arrow[d, "\phi"'] \\
F \otimes_k \bar{k} \arrow[r, "\tau \otimes 1"] & F \otimes_k \bar{k}
\end{tikzcd}
$$

commutes and $\tau \otimes 1$ is a $\bar{k}$-algebra automorphism. Therefore the G-action on F extends to a G-action on $F \otimes_k \bar{k}$. Notice that

$$
\begin{aligned}
\phi(\tau(u)) &= \sum_{\sigma \in G} \sigma(\tau(u)) e_\sigma \\
&= \sum_{\gamma \in G} \gamma(u) e_{\gamma\tau^{-1}} .
\end{aligned}
\tag{6.6}
$$

Let $\rho_\tau : F \otimes_k \bar{k} \to F \otimes_k \bar{k}$ be the "left multiplication by $\tau \otimes 1$" homomorphism. Comparing (6.4) and (6.6) we see that the G-action on the ring $\bigoplus_{\sigma \in G} \bar{k} e_\sigma$ is defined on the basis $\{e_\sigma \mid \sigma \in G\}$ by the rule $\rho_\tau(e_\sigma) = e_{\sigma\tau^{-1}}$. By Example 5.6.11, this shows that $F \otimes_k \bar{k}$ together with the G-action inherited from F is isomorphic to the trivial G-Galois extension of $\bar{k}$. $\square$

From (6.5) we see that the composite map $\phi_\sigma = \pi_\sigma \phi$ is one-to-one and factors through $\sigma : F \to F$. The diagram

$$
\begin{tikzcd}
F \arrow[r, "\phi_\sigma"] \arrow[d, "\sigma"'] & \bar{k} e_\sigma \\
F \arrow[r, "\subseteq"] & \bar{k} \arrow[u, "\cong"']
\end{tikzcd}
$$

commutes.

6.5. Exercises.

EXERCISE 5.6.1. In Definition 5.6.6 the trace map from A to R afforded by M, $T_R^{A,M}$, was defined using a dual basis for M. Prove that the function $T_R^{A,M}$ is independent of the choice of dual basis for M.

EXERCISE 5.6.2. Let A be an R-algebra and M a left A-module which is a finitely generated projective R-module. If $M = M_1 \oplus M_2$ as A-modules, prove that

$$T_R^{A,M} = T_R^{A,M_1} + T_R^{A,M_2}.$$

EXERCISE 5.6.3. Let A be an R-algebra which is finitely generated and free as an R-module. Show that the trace mapping T_R^S defined in Exercise 1.7.2 is equal to the trace mapping defined in Definition 5.6.6.

EXERCISE 5.6.4. Let k be a field and A a finite dimensional k-algebra. Suppose $\alpha \in A$ and $\operatorname{min.poly}_k(\alpha) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 + a_0$ is irreducible in $k[x]$. Prove that $T_k^A(\alpha) = ra_{m-1}$ for some integer r.

EXERCISE 5.6.5. Let S be a commutative faithful R-algebra which is a finitely generated free R-module of rank n. Let $\lambda_1, \dots, \lambda_n$ be a free basis for S over R. For each i, let $\pi_i \in \operatorname{Hom}_R(S, R)$ be the projection onto the coefficient of λ_i.

(1) The trace map is given by $T_R^S(z) = \sum_{i=1}^n \pi_i(z\lambda_i)$.
(2) The following are equivalent.
   (a) S is separable over R.
   (b) There exist $\mu_1, \dots, \mu_n$ in S such that $T_R^S \cdot \mu_i = \pi_i$.
(3) If S/R is separable, then the elements $\mu_1, \dots, \mu_n$ appearing in (2) make up a free R-basis for S and $T_R^S(\mu_i\lambda_j) = \delta_{ij}$ (Kronecker's delta).

EXERCISE 5.6.6. Let R be a commutative ring and P a finitely generated projective R-module. By Lemma 2.8.1, $\theta_R : P^* \otimes_R P \to \operatorname{Hom}_R(P, P)$ is an isomorphism of R-modules, where $\theta_R(f \otimes p)(x) = f(x)p$.

(1) Define $T : P^* \otimes_R P \to R$ by $T(f \otimes p) = f(p)$. Show that T is an R-module homomorphism.
(2) Assume P is free and finitely generated. Show that the map T induces a map $T : \operatorname{Hom}_R(P, P) \to R$ which is equal to the trace map of Exercise 1.7.2 and the trace map of Definition 5.6.6.

EXERCISE 5.6.7. Let S be a commutative faithful R-algebra which is finitely generated and projective as an R-module. Let A be a faithful S-algebra which is finitely generated and projective as an S-module. Prove the following generalization of Exercise 1.7.4 (1): For every $a \in A$, $T_R^A(a) = T_R^S\left(T_S^A(a)\right)$.

EXERCISE 5.6.8. Let R be a connected commutative ring and S a commutative separable R-algebra that as an R-module is a progenerator of rank n. Then there exists a commutative R-algebra T that satisfies:

(1) T is connected.
(2) T is separable over R.
(3) T is an R-module progenerator.
(4) $S \otimes_R T \cong T^n$.

(Hints: Start with the algebra T constructed in Proposition 5.6.10. By Exercise 3.4.6, $\operatorname{Spec} T$ has only finitely many connected components. Show that T can be replaced with one of its connected components.)

CHAPTER 6

The Integral Closure of a Commutative Ring

If A is an algebra over a field k, then an element $\alpha \in A$ is said to be algebraic over k if there exists a nonzero polynomial $p(x) \in k[x]$ such that $p(\alpha) = 0$. If α is algebraic over k, then the minimal polynomial of α is the monic polynomial $p(x)$ of minimal degree such that $p(\alpha) = 0$. If A is an R-algebra, where R is a commutative ring, then this chapter focuses on those algebraic elements $\alpha \in A$ such that α is the root of a monic polynomial $p(x) \in R[x]$. In this case, we say α is integral over R. We say A is an integral R-algebra if every $\alpha \in A$ is integral over R. Because we do not assume R is a field, elements of A that are algebraic over R are not necessarily integral over R. For example, $\mathbb{Q}$ is algebraic over $\mathbb{Z}$, but if $\alpha \in \mathbb{Q}$ and α is integral over $\mathbb{Z}$, then $\alpha \in \mathbb{Z}$. We say $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. In Section 6.1 we prove that the integral closure of R in A exists. A highlight of this section is Theorem 6.1.13 which gives sufficient conditions such that the integral closure of an integral domain R in a finite extension of its quotient field is a finitely generated R-module. In Section 6.2 we prove that a polynomial ring over a commutative noetherian ring R is a noetherian ring. Since the homomorphic image of a noetherian ring is noetherian, this implies that a commutative ring S is noetherian if and only if there is a commutative noetherian ring R such that S is a finitely generated R-algebra. This is the Hilbert Basis Theorem. We prove Hilbert's Nullstellensatz, in two forms. It says that if k is an algebraically closed field and $p(x_1, \dots, x_n)$ is a polynomial of positive degree in $k[x_1, \dots, x_n]$, then there exists a $(\alpha_1, \dots, \alpha_n) \in k^n$ such that $p(\alpha_1, \dots, \alpha_n) = 0$. In other words, over an algebraically closed field, $p(x_1, \dots, x_n)$ has a nontrivial set of zeros. In Section 6.3 there is a proof of the so-called Going Up and Going Down Theorems. These important theorems are concerned with the correspondence between the prime ideals in a commutative ring R and prime ideals in a commutative integral extension S of R.

1. Integral Extensions

1.1. Integral elements. Let R be a commutative ring and A an R-algebra. An element $a \in A$ is said to be *integral* over R in case there exists a monic polynomial $p \in R[x]$ such that $p(a) = 0$. If every element of A is integral over R, then we say A is *integral* over R. The reader should verify that any homomorphic image of R is integral over R. The R-algebra A comes with a structure homomorphism $\theta : R \to Z(A)$. Assume θ is one-to-one, or equivalently, A is a faithful R-module. Then we identify R with $\theta(R)$ which is a subring of A. In this case, if every element of A is integral over R, we say A/R is an *integral extension*. If no element of $A - R$ is integral over R, then we say R is *integrally closed* in A.

If A is an R-algebra which is R-faithful, and $a \in A$, then the R-subalgebra of A generated by a is denoted $R[a]$. Since $R \subseteq Z(A)$, $R[a]$ is commutative, and the substitution homomorphism $R[x] \to A$ defined by $x \mapsto a$ is an R-algebra homomorphism with image $R[a]$.

EXAMPLE 6.1.1. Let R be a commutative ring. Let $A = M_n(R)$, the ring of n-by-n matrices over R. Let $M \in M_n(R)$ and let $p(x) = \text{char. poly}_M(x)$ be the characteristic polynomial of M. Then $p(x)$ is a monic polynomial of degree n in $R[x]$. By Cayley-Hamilton (Theorem 1.7.7) we know $p(M) = 0$. This shows A is integral over R.

In Proposition 6.1.2 we derive some useful necessary and sufficient conditions for an element to be integral.

PROPOSITION 6.1.2. *Let A be a faithful R-algebra, and $a \in A$. The following are equivalent.*

(1) a is integral over R.
(2) $R[a]$ is a finitely generated R-module.
(3) There is an R-subalgebra B of A such that $R[a] \subseteq B \subseteq A$ and B is a finitely generated R-module.
(4) There exists a faithful $R[a]$-module which is finitely generated as an R-module.

PROOF. (1) implies (2): Since a is integral over R, there exist elements $r_0, r_1, \dots, r_{n-1}$ in R such that $a^n = r_0 + r_1 a + \cdots + r_{n-1} a^{n-1}$. Let B be the R-submodule of $R[a]$ generated by $1, a, a^2, \dots, a^{n-1}$. Then we have shown that $a^n \in B$. Inductively assume $k > 0$ and that $a^i \in B$ for all i such that $0 \le i \le n+k-1$. It follows that $a^{n+k} = r_0 a^k + r_1 a^{k+1} + \cdots + r_{n-1} a^{n+k-1}$ is also in B, hence $B = R[a]$.

(2) implies (3): For B take $R[a]$.

(3) implies (4): Since B contains $R[a]$ as a subring, B is a faithful $R[a]$-module.

(4) implies (1): Let M be a faithful $R[a]$-module. There are ring homomorphisms

$$R[a] \xrightarrow{\alpha} \operatorname{Hom}_{R[a]}(M,M) \xrightarrow{\beta} \operatorname{Hom}_R(M,M)$$

where α is the left regular representation of Example 1.1.13. Since M is faithful, α is one-to-one. Since $R[a]$ is an R-algebra, β is one-to-one. If $u \in R[a]$, then by Exercise 1.7.5, $\beta\alpha(u)$ satisfies a monic polynomial $p \in R[x]$. Therefore, every $u \in R[a]$ is integral over R. $\square$

If R is a subring of a commutative ring A, then Theorem 6.1.3 shows the existence of the integral closure of R in A.

THEOREM 6.1.3. *Let A be a commutative faithful R-algebra.*

(1) If $a_1, \dots, a_n \in A$ are integral over R, then $R[a_1, \dots, a_n]$ is a finitely generated R-module.
(2) Let S be the set of all $a \in A$ such that a is integral over R. Then S is an R-subalgebra of A. We say that S is the integral closure of R in A.
(3) (Integral over Integral is Integral) Let $R \subseteq S \subseteq A$ be three rings such that A is integral over S and S is integral over R. Then A is integral over R.
(4) Let S be the integral closure of R in A. Then S is integrally closed in A.

PROOF. (1): By Proposition 6.1.2 (2), $R[a_1]$ is a finitely generated R-module. Set $S = R[a_1, \dots, a_{n-1}]$. Then a_n is integral over S, so $S[a_n]$ is a finitely generated S-module. Inductively assume S is a finitely generated R-module. By Proposition 2.1.13, $S[a_n] = R[a_1, \dots, a_n]$ is a finitely generated R-module.

(2): Given $x, y \in S$, by Part (1) it follows that $R[x,y]$ is a finitely generated R-module of A. By Proposition 6.1.2, S contains $x+y$, $x-y$, xy. Since $R \subseteq S$, S is an R-algebra.

(3): Let $a \in A$ and $p \in S[x]$ a monic polynomial such that $p(a) = 0$. Suppose $p = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1} + x^n$. Set $T = R[s_0, \dots, s_{n-1}]$. Then T is a finitely generated R-module and $p \in T[x]$, so a is integral over T. It follows that $T[a]$ is finitely generated over T. By Proposition 2.1.13, $T[a] = R[s_0, \dots, s_{n-1}, a]$ is a finitely generated R-module. Therefore a is integral over R.

(4): By the proof of Part (3), if $a \in A$ is integral over S, then a is integral over R. $\square$

If A is an integral R-algebra, then in Lemma 6.1.4 we derive useful necessary and sufficient conditions for A to be a division ring.

LEMMA 6.1.4. *Let A be a faithful integral R-algebra.*

(1) If $x \in R - (0)$, then x is invertible in A if and only if x is invertible in R.
(2) If A is a division ring, then R is a field.
(3) If R is a field and A has no zero divisors, then A is a division ring.

PROOF. (1): Assume $x \in R - (0)$ and $x^{-1} \in A$. Then x^{-1} is integral over R. There exist $n \geq 1$ and $r_i \in R$ such that

$$x^{-n} + r_{n-1}x^{1-n} + \dots + r_1 x^{-1} + r_0 = 0.$$

Multiply by x^{n-1} and get

$$x^{-1} + r_{n-1} + r_{n-2}x + \dots + r_1 x^{n-2} + r_0 x^{n-1} = 0$$

which shows $x^{-1} \in R$. We identify R with a subring of A, so the converse is obvious.

(2): This follows straight from (1).

(3): This follows from Exercise 1.8.6. $\square$

1.2. Integrally Closed Domains. If R is an integral domain with quotient field K, then we say R is *integrally closed* if R is integrally closed in K.

PROPOSITION 6.1.5. *If R is a unique factorization domain (UFD) with quotient field K, then R is integrally closed in K.*

PROOF. Let $n/d \in K$ where $n, d \in R$ and we assume $\gcd(n,d) = 1$. Suppose $p(x) = x^m + r_{m-1}x^{m-1} + \dots + r_1 x + r_0$ is a monic polynomial in $R[x]$ and $p(n/d) = 0$. It follows from the Rational Root Theorem (for example, see [**19**, Theorem 3.7.1]) that d is a unit of R. That is, $n/d \in R$. $\square$

EXAMPLE 6.1.6. Applying Proposition 6.1.5, we list some examples.

(1) The ring of integers $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.
(2) If k is a field, then the ring of polynomials $k[x]$ is integrally closed.
(3) If R is a UFD, then the polynomial ring $R[x_1, \dots, x_n]$ is integrally closed.
(4) If D is a square free integer and $D \equiv 1 \pmod 4$, then the ring $\mathbb{Z}[\sqrt{D}]$ is an integral domain that is not integrally closed. (See [**19**, Example 3.7.9], for example.)

In Lemma 6.1.7 and Corollary 6.1.8 we see that the property of being integrally closed is preserved by localization.

LEMMA 6.1.7. *Suppose $R \subseteq T$ is an extension of commutative rings and S is the integral closure of R in T. If W is a multiplicative set in R, then S_W is the integral closure of R_W in T_W.*

PROOF. By Exercise 6.1.1, $S_W = R_W \otimes_R S$ is integral over R_W. Suppose $t/w \in T_W$ is integral over R_W. Let

$$\left(\frac{t}{w}\right)^n + \frac{r_{n-1}}{w_{n-1}}\left(\frac{t}{w}\right)^{n-1} + \dots \frac{r_1}{w_1}\frac{t}{w} + \frac{r_0}{w_0}$$

be an integral dependence relation where each $r_i \in R$ and $w_i \in W$. Let $d = w_0 \dots w_{n-1}$ and multiply through by $(dw)^n$ to get an integral dependence relation for dt over R. Then $dt \in S$, so $t/w = (dt)/(dw) \in S_W$. □

COROLLARY 6.1.8. *Let R be an integral domain with quotient field K.*

(1) If Λ is a commutative K-algebra, and S is the integral closure of R in Λ, then the image of the natural map $K \otimes_R S \to \Lambda$ is equal to the integral closure of K in Λ.
(2) If L/K is a finite dimensional extension of fields and S is the integral closure of R in L, then L is equal to the quotient field of S.

PROOF. (1): Apply Lemma 6.1.7 with $T = \Lambda$ and multiplicative set $W = R - (0)$. By Lemma 3.1.4 (6), S_W is isomorphic to $K \otimes_R S$. Part (2) is a special case of Part (1). □

Proposition 6.1.9 shows that an integral domain is integrally closed if and only if it is integrally closed when localized at each prime ideal.

PROPOSITION 6.1.9. *Let R be an integral domain with quotient field K. The following are equivalent.*

(1) R is integrally closed in K.
(2) For each $P \in \operatorname{Spec} R$, R_P is integrally closed in K.
(3) For each $P \in \operatorname{Max} R$, R_P is integrally closed in K.

PROOF. Let S be the integral closure of R in K. Then R is integrally closed if and only if $R \to S$ is onto. By Lemma 6.1.7, S_P is the integral closure of R_P in K for each $P \in \operatorname{Spec} R$. The rest follows from Exercise 3.5.1. □

If R is a UFD with quotient field K , then a primitive polynomial $f \in R[x]$ is irreducible in $R[x]$ if and only if f is irreducible in $K[x]$. This is usually called Gauss' Lemma (see, for example, [**19**, Theorem 3.7.4]). Lemma 6.1.10 is a generalization to the case where R is an integral domain that is integrally closed in its quotient field.

LEMMA 6.1.10. *(Gauss' Lemma) Let R be an integrally closed integral domain with quotient field K. Let $f \in R[x]$ be a monic polynomial, and suppose there is a factorization $f = gh$, where g, h are monic polynomials in $K[x]$. Then both g and h are in $R[x]$.*

PROOF. By Proposition 1.8.1, let L/K be an extension of fields such that L is a splitting field for f over K. By Theorem 6.1.3 (2), let S be the integral closure of R in L. Since f splits in $L[x]$, so does g. Write $g = \prod(x - \alpha_i)$. Each α_i is a root of f, hence is integral over R, hence lies in S. This shows that every coefficient of g is in S. So each coefficient of g is in $S \cap K$ which is equal to R since R is integrally closed in K. So $g \in R[x]$. The same argument applies to h. □

The rest of this section consists of three important applications of Gauss' Lemma.

THEOREM 6.1.11. *Let R be an integrally closed integral domain with quotient field K. Let A be a finite dimensional K-algebra. An element $\alpha \in A$ is integral over R if and only if* $\operatorname{min.poly}_K(\alpha) \in R[x]$.

PROOF. Let $f = \operatorname{min.poly}_K(\alpha) \in K[x]$. Assume α is integral over R. Then there exists a monic polynomial $g \in R[x]$ such that $g(\alpha) = 0$. In this case, f divides g in $K[x]$. There is a factorization $g = fh$ for some monic polynomial $h \in K[x]$. By Gauss' Lemma 6.1.10, both f and h lie in $R[x]$. □

COROLLARY 6.1.12. *Let R be an integral domain which is integrally closed in its quotient field K. Let L/K be a finite separable field extension and let S be the integral closure of R in L. Then the trace and norm functions from L to K restrict to trace and norm functions from S to R. That is, $T_K^L : S \to R$, and $N_K^L : S \to R$.*

PROOF. Let $\alpha \in S$ and $f = \min.\operatorname{poly}_K(\alpha)$. By Theorem 6.1.11, we know that $f \in R[x]$. By Lemma 1.8.4 (3), the characteristic polynomial of $\ell_\alpha : L \to L$ is a power of f. Since $T_K^L(\alpha)$ and $N_K^L(\alpha)$ are coefficients of $\operatorname{char.poly}_K(\ell_\alpha)$, they are elements of R. □

Theorem 6.1.13 is motivated by an important finiteness question. Start with an integrally closed integral domain R with quotient field K, let L/K be a finite dimensional extension of fields, and let S be the integral closure of R in L. We ask whether S is finitely generated as an R-module or not. This important theorem shows that the answer is yes, if L/K is separable and if R is noetherian.

THEOREM 6.1.13. *Let R be an integral domain which is integrally closed in its quotient field K. Let L/K be a finite separable field extension and let S be the integral closure of R in L. There exist bases $\{\lambda_1, \dots, \lambda_n\}$ and $\{\mu_1, \dots, \mu_n\}$ for L/K such that $R\lambda_1 + \cdots + R\lambda_n \subseteq S \subseteq R\mu_1 + \cdots + R\mu_n$. If R is noetherian, then S is a finitely generated R-module.*

PROOF. Our proof is based on [**4**, Theorem 5.17]. Every $\lambda \in L$ is algebraic over K. There is an equation $r_m\lambda^m + \cdots + r_1\lambda + r_0 = 0$, where each r_i is in R. Multiply by r_m^{m-1} to get $(r_m\lambda)^m + \cdots + r_1 r_m^{m-2}(r_m\lambda) + r_0 r_m^{m-1} = 0$. This shows that $r_m\lambda$ is integral over R, hence is in S. There exists a basis $\lambda_1, \dots, \lambda_n$ for L/K such that each λ_i is in S. By Lemma 1.8.6 (3), there is a K-basis $\mu_1, \dots, \mu_n$ for L such that $T_K^L(\mu_i\lambda_j) = \delta_{ij}$ (the Kronecker delta function). Let s be an arbitrary element of S. View s as an element of L and write $s = \alpha_1\mu_1 + \cdots + \alpha_n\mu_n$, where each $\alpha_i \in K$. Since $\lambda_i \in S$, we have $s\lambda_i \in S$. By Corollary 6.1.12, $T_K^L(s\lambda_i) \in R$. Then

$$T_K^L(s\lambda_i) = T_K^L\Big(\sum_{j=1}^n \alpha_j\lambda_i\mu_j\Big) = \sum_{j=1}^n T_K^L(\alpha_j\lambda_i\mu_j) = \sum_{j=1}^n \alpha_j T_K^L(\lambda_i\mu_j) = \alpha_i$$

shows that each α_i is in R. It follows that $S \subseteq R\mu_1 + \cdots + R\mu_n$. If R is noetherian, then by Corollary 4.1.12, S is a finitely generated R-module. □

In the terminology of Definition 12.1.2, Theorem 6.1.13 says that if L/K is a finite separable extension, then S is an R-lattice in L. When R is a finitely generated algebra over a field, see Theorem 10.3.11 for a stronger version of Theorem 6.1.13.

1.3. Exercises.

EXERCISE 6.1.1. Let A be an integral R-algebra and S a commutative R-algebra. Show that $S \otimes_R A$ is an integral S-algebra.

EXERCISE 6.1.2. Let A be an integral faithful R-algebra and I a two-sided ideal in A. Show that A/I is an integral $R/(I \cap R)$-algebra.

EXERCISE 6.1.3. Let R be a commutative ring and $A = R[x]$ the polynomial ring in one variable over R. Show that R is integrally closed in A if and only if $\operatorname{Rad}_R(0) = (0)$.

EXERCISE 6.1.4. Let S be a commutative faithfully flat R-algebra. Prove:

(1) If S is an integral domain, then R is an integral domain.

(2) If S is an integrally closed integral domain, then R is an integrally closed integral domain. (Hint: If K is the quotient field of R, show that S is integrally closed in $S \otimes_R K$.)
(3) If S has the property that S_Q is an integrally closed integral domain for each $Q \in \operatorname{Spec} S$, then R has the property that R_P is an integrally closed integral domain for each $P \in \operatorname{Spec} R$. In the terminology of Definition 11.1.4, this says if S is a normal ring, then R is a normal ring.

EXERCISE 6.1.5. Let R be a commutative ring and A an R-algebra which is integral over R. Show that $A = \varinjlim A_\alpha$ where A_α runs over the set of all R-subalgebras of A such that A_α is finitely generated as an R-module.

EXERCISE 6.1.6. Let S be a commutative faithful integral R-algebra. Assume R is an integral domain with quotient field K and S is an integral domain with quotient field L. By Exercise 3.1.11, L can be viewed as a field extension of K. Prove that L is algebraic over K.

EXERCISE 6.1.7. Let k be a field and $A = k[x]$ the polynomial ring over k in one variable. Let $R = k[x^2, x^3]$ be the k-subalgebra of A generated by x^2 and x^3. We know from Exercise 3.6.6 that A is a finitely generated R-module and R and A have the same quotient field, namely $K = k(x)$. Show that A is equal to the integral closure of R in K.

EXERCISE 6.1.8. This exercise is a generalization of Exercise 6.1.7. Let k be a field, x an indeterminate, and $n > 1$ an integer. Let $T = k[x]$, $S = k[x^n, x^{n+1}]$, and $R = k[x^n]$. For the tower of rings: $R \subseteq S \subseteq T$, prove the following.

(1) T is a finitely generated R-module.
(2) T and S have the same quotient field, namely $K = k(x)$.
(3) T is equal to the integral closure of S in K.
(4) T is not a separable R-algebra.
(5) S is not a separable R-algebra.
(6) T is not a separable S-algebra.

EXERCISE 6.1.9. Let k be a field and $A = k[x]$ the polynomial ring over k in one variable. Let $R = k[x^2 - 1, x^3 - x]$ be the k-subalgebra of A generated by $x^2 - 1$ and $x^3 - x$. We know from Exercise 3.6.8 that R and A have the same quotient field, namely $K = k(x)$. Show that A is equal to the integral closure of R in K. For a continuation of this example, see Section 12.4.2.

2. Some Theorems of Hilbert

In this section we prove the Hilbert Basis Theorem, Theorem 6.2.1 as well as the two classical versions of Hilbert's Nullstellensatz. Corollary 6.2.4 is commonly called the Weak Form of the Nullstellensatz while Theorem 6.2.9 is essentially the theorem that was originally proved by Hilbert. The Basis Theorem states sufficient conditions for a commutative ring to be noetherian. The two forms of the Nullstellensatz are logically equivalent and state that if k is an algebraically closed field, $A = k[x_1, \dots, x_n]$ the polynomial ring in n variables, and $f_1, \dots, f_m$ a set of polynomials in A, then the system of m polynomial equations $f_1 = 0, \dots, f_m = 0$ in n variables has a solution if and only if the ideal generated by $f_1, \dots, f_m$ in A is not the unit ideal.

2.1. The Hilbert Basis Theorem. To show that a commutative ring S is noetherian, by Theorem 6.2.1, it is sufficient to show that S is a finitely generated algebra over a noetherian ring R.

THEOREM 6.2.1. *(Hilbert Basis Theorem) Let R be a commutative noetherian ring.*

(1) The polynomial ring $R[x]$ in the variable x over R is a noetherian ring.
(2) The polynomial ring $R[x_1,\dots,x_n]$ over R in n variables is a noetherian ring.
(3) If R is a commutative noetherian ring and S is a finitely generated commutative R-algebra, then S is noetherian.

PROOF. (1): By Corollary 4.1.7, it is enough to show every ideal of $R[x]$ is finitely generated. Let J be an ideal in $R[x]$. Let I be the set of all $r \in R$ such that r is the leading coefficient for some polynomial $f \in J$. Then I is an ideal in R, hence is finitely generated, so we can write $I = Ra_1 + \cdots + Ra_m$. For each a_i there is some $f_i \in J$ such that a_i is the leading coefficient of f_i. Let $d_i = \deg f_i$ and let d be the maximum of $\{d_1,\dots,d_m\}$. If J' denotes the ideal of $R[x]$ generated by $f_1,\dots,f_m$, then $J' \subseteq J$. By Corollary 4.1.12 and Corollary 4.1.10 it is enough to prove J/J' is finitely generated. We prove that J/J' is finitely generated over R, which is a stronger statement.

Consider a typical polynomial p in J. Assume p has degree $\nu \geq d$ and leading coefficient r. Since $r \in I$, write $r = u_1a_1 + \cdots + u_ma_m$. Then $q = u_1f_1x^{\nu-d_1} + \cdots + u_mf_mx^{\nu-d_m}$ is in J', has degree ν, and leading coefficient r. The polynomial $p-q$ is in J and has degree less than ν. By iterating this argument a finite number of steps, we can show that p is congruent modulo J' to a polynomial of degree less than d. If L is the R-submodule of $R[x]$ generated by $1, x, \dots, x^{d-1}$, then we have shown that J/J' is generated over R by images from the set $J \cap L$. But $J \cap L$ is an R-submodule of L, hence is finitely generated over R, by Corollary 4.1.12.

(2): This follows from (1), by induction on n.

(3): For some n, S is the homomorphic image of the polynomial ring $R[x_1,\dots,x_n]$ in n variables over R. It follows from (2) and Corollary 4.1.13 (1) that S is noetherian. □

Hilbert's Nullstellensatz is a corollary to the following two propositions. Proposition 6.2.2 is due to Emil Artin and John Tate, [**2**].

PROPOSITION 6.2.2. *Let $A \subseteq B \subseteq C$ be a tower of commutative rings and assume A and B are subrings of C. Suppose*

(1) A is noetherian,
(2) C is finitely generated as an A-algebra,
(3) and either
  (a) C is finitely generated as a B-module, or
  (b) C is integral over B.

Then B is finitely generated as an A-algebra.

PROOF. Assume (1), (2) and (3) (b) are all satisfied. Suppose $C = A[x_1,\dots,x_m]$. In this case, we also have $C = B[x_1,\dots,x_m]$ and $x_1,\dots,x_m$ are integral over B. By Theorem 6.1.3 (1), C is finitely generated as a B-module, so (3)(a) is also satisfied. Let $C = By_1 + by_2 + \cdots + By_n$. Each x_i and each product y_iy_j is in C, so we can write

$$
\begin{aligned}
x_i &= \sum_{j=1}^{n} b_{ij} y_j \\
y_i y_j &= \sum_{k=1}^{n} b_{ijk} y_k
\end{aligned}
\tag{2.1}
$$

for certain $b_{ij} \in B$ and $b_{ijk} \in B$. Let B_0 be the A-subalgebra of B generated by all of the b_{ij} and b_{ijk}. By Theorem 6.2.1 (3), we know that B_0 is noetherian. Let $c = p(x_1, \dots, x_m)$ be an arbitrary element in $A[x_1, \dots, x_m] = C$. Using (2.1), the reader should verify that

$$c = p\Big(\sum_{j=1}^{n} b_{1j}y_j, \sum_{j=1}^{n} b_{2j}y_j, \dots\Big)$$

is in $B_0y_1 + B_0y_2 + \cdots + B_0y_n$. Therefore C is finitely generated as a B_0-module. By Corollary 4.1.12, B is finitely generated as a B_0-module. Since B_0 is finitely generated as an A-algebra, it follows that B is finitely generated as an A-algebra. □

PROPOSITION 6.2.3. *Let F/k be an extension of fields. The following are equivalent.*

(1) F is finitely generated as a k-algebra.
(2) F is finitely generated and algebraic as an extension field of k.
(3) $\dim_k(F) < \infty$.

PROOF. For a proof that (2) is equivalent to (3), see [**19**, Proposition 5.1.10], for example. For (2) implies (1), see [**19**, Theorem 5.1.4], for example. To prove that (1) implies (2) we use a proof by contradiction. By (1) we can write $F = k[x_1, \dots, x_n]$. Since F is an extension field of k, this implies $F = k(x_1, \dots, x_n)$. For contradiction's sake, assume not all of $x_1, \dots, x_n$ are algebraic over k. By Theorem 1.8.8, we can re-order and assume for some $1 \le r \le n$ that $\{x_1, \dots, x_r\}$ is a transcendence base for F over k. Then $F = k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ is algebraic over the field $K = k(x_1, \dots, x_r)$ and K is isomorphic to the field of rational functions over k in r variables. That is, K is the quotient field of the polynomial ring $k[x_1, \dots, x_r]$. Applying Proposition 6.2.2 to the tower of rings $k \subseteq K \subseteq F$, we conclude that K is finitely generated as a k-algebra. Write $K = k[y_1, \dots, y_s]$. Viewing each y_i as a rational function in $k(x_1, \dots, x_r)$, there exist polynomials f_i, g_i in $k[x_1, \dots, x_r]$ such that $y_i = f_i/g_i$. Set $g = g_1g_2\cdots g_s$. Without loss of generality assume $\deg g \ge 1$ and let h be any irreducible factor of $g+1$. Therefore, $\gcd(h, g) = 1$. Consider the element h^{-1} as an element of the field $K = k[y_1, \dots, y_s] = k[f_1/g_1, \dots, f_s/g_s]$. Then $h^{-1} = p(f_1/g_1, \dots, f_s/g_s)$ where p is a polynomial in s variables with coefficients in k. The denominators involve only the polynomials $g_1, \dots, g_s$. For some positive integer N, we get an equation of polynomials $g^N = hf$ where $f \in k[x_1, \dots, x_r]$. This is a contradiction. □

Historically, Hilbert's Nullstellensatz, Theorem 6.2.9, was proved first and used to prove Corollary 6.2.4. For this reason Corollary 6.2.4 is called the Weak Form of the Nullstellensatz. This name is a misnomer because the two are logically equivalent. The line of proof we use here is due to O. Zariski who in the article [**60**] proved a version of Proposition 6.2.3 and applied it to prove Corollary 6.2.4. The Weak Nullstellensatz will be applied below in the proof of the Nullstellensatz. In Exercise 6.2.10 the reader is asked to prove that the Weak Form of the Nullstellensatz follows from the Nullstellensatz.

COROLLARY 6.2.4. *(Hilbert's Nullstellensatz, Weak Form) If k is a field, A is a commutative finitely generated k-algebra, and $\mathfrak{m}$ is a maximal ideal in A, then $A/\mathfrak{m}$ is a finitely generated algebraic extension field of k.*

PROOF. Apply Proposition 6.2.3 to the field $F = A/\mathfrak{m}$. □

2.2. Hilbert's Nullstellensatz. Algebraic geometry is the study of systems of algebraic equations in n variables over a field k. This section is an introduction to algebraic geometry.

DEFINITION 6.2.5. Let k be any field. Let $n \geq 0$. Define *affine n-space over k* to be

$$\mathbb{A}^n_k = \{(a_1, \ldots, a_n) \mid a_i \in k\}.$$

We write simply $\mathbb{A}^n$, if k is apparent. Let

$$A = k[x_1, \ldots, x_n]$$

and $f \in A$. The *zero set* of f is the set $Z(f) = \{P \in \mathbb{A}^n \mid f(P) = 0\}$. If $T \subseteq A$, then

$$Z(T) = \{P \in \mathbb{A}^n \mid f(P) = 0 \, \forall \, f \in T\}.$$

If I is the ideal generated by T in A, then $Z(I) = Z(T)$. This is because any $g \in I$ is a linear combination of elements of T. Since A is noetherian, I is finitely generated, hence $Z(T)$ can be expressed as the zero set of a finite set of polynomials. A subset $Y \subseteq \mathbb{A}^n$ is an *algebraic set* if there exists $T \subseteq A$ such that $Y = Z(T)$.

We apply the Weak Form of Hilbert's Nullstellensatz to show that if k is algebraically closed, then a finite set of polynomials T in $A = k[x_1, \ldots, x_n]$ has a nonempty zero set if and only if the ideal generated by T is not the unit ideal. If $n = 1$, then $k[x_1]$ is a principal ideal domain, and this statement follows immediately from the definition of algebraically closed field.

THEOREM 6.2.6. *Let k be an algebraically closed field and $A = k[x_1, \ldots, x_n]$.*

(1) If M is a maximal ideal in A, then there exist elements $a_1, a_2, \ldots, a_n$ in k such that $M = (x_1 - a_1, \ldots, x_n - a_n)$.
(2) If I is a proper ideal in A, then $Z(I)$ is nonempty.

PROOF. (1): Since k is algebraically closed, Corollary 6.2.4 says the natural map $k \to A/M$ is onto. There exist $a_1, \ldots, a_n \in k$ such that $a_i + M = x_i + M$ for $i = 1, \ldots, n$. That is, $x_i - a_i \in M$ for each i. The reader should verify that the ideal $J = (x_1 - a_1, \ldots, x_n - a_n)$ is maximal. Because J is a subset of M, we see that $J = M$.

(2): Take any maximal ideal M which contains I. By Part (1), $M = (x_1 - a_1, \ldots, x_n - a_n)$ for elements $a_1, a_2, \ldots, a_n$ in k. The reader should verify that $Z(I) \supseteq Z(M)$ and that $Z(M)$ is the singleton set $\{(a_1, \ldots, a_n)\}$. $\square$

Next we show that the algebraic subsets of $\mathbb{A}^n_k$ are the closed sets for a topology.

PROPOSITION 6.2.7. *Let $\mathbb{A}^n$ be affine n-space over the field k.*

(1) The sets $\emptyset$ and $\mathbb{A}^n$ are algebraic sets.
(2) The union of two algebraic sets is an algebraic set.
(3) The intersection of any family of algebraic sets is an algebraic set.
(4) The algebraic sets can be taken as the closed sets for a topology on $\mathbb{A}^n$ which is called the Zariski topology.

PROOF. (1): Note that $\emptyset = Z(1)$ and $\mathbb{A}^n = Z(0)$.
(2): If $Y_1 = Z(T_1)$ and $Y_2 = Z(T_2)$, then

$$Y_1 \cup Y_2 = Z(T_1 T_2),$$

where $T_1 T_2 = \{f_1 f_2 \mid f_1 \in T_1, f_2 \in T_2\}$. Prove this in two steps:

Step 1: Let $P \in Y_1$. Then $f_1(P) = 0$ for all $f_1 \in T_1$. Then $(f_1 f_2)(P) = 0$. Similarly for $P \in Y_2$.

Step 2: Let $P \in Z(T_1 T_2)$ and assume $P \notin Y_1$. Then there exists $f_1 \in T_1$ such that $f_1(P) \neq 0$. But for every $f_2 \in T_2$ we have $(f_1 f_2)(P) = 0$ which implies $f_2(P) = 0$. Thus $P \in Y_2$.

(3): Let $\{Y_\alpha = Z(T_\alpha)\}$ be a family of algebraic sets. Then
$$\bigcap Y_\alpha = Z(\bigcup T_\alpha).$$
To see this, proceed in two steps:

Step 1: If $P \in \bigcap Y_\alpha$, the P is a zero of all of the T_α, hence is in $Z(\bigcup T_\alpha)$.

Step 2: If P is a zero of all of the T_α, then P is in all of the Y_α.

(4): Follows from the first three parts. □

DEFINITION 6.2.8. Let k be any field. For any $Y \subseteq \mathbb{A}^n$, we define the ideal of Y in $A = k[x_1, \dots, x_n]$ by
$$I(Y) = \{f \in A \mid f(P) = 0 \,\forall\, P \in Y\}.$$
This is an ideal, as is easily checked. The reader should verify that $I(Y) = \operatorname{Rad}(I(Y))$. Recall that any ideal that is equal to its radical is called a radical ideal. By default, $I(\emptyset) = A$.

Now we prove the second version of Hilbert's Nullstellensatz, and apply it to show that when k is algebraically closed, the operators $Z(\cdot)$ and $I(\cdot)$ induce a one-to-one correspondence between the set of closed subsets of $\mathbb{A}^n$ and the set of radical ideals in $k[x_1, \dots, x_n]$.

THEOREM 6.2.9. *(Hilbert's Nullstellensatz) Let k be an algebraically closed field and J an ideal in $A = k[x_1, \dots, x_n]$. Then* $\operatorname{Rad}(J) = I(Z(J))$.

PROOF. By Exercise 6.2.1, $\operatorname{Rad}(J) \subseteq I(Z(J))$. Let $f \in A - \operatorname{Rad}(J)$. We prove that there exists $x \in Z(J)$ such that $f(x) \neq 0$. By Lemma 3.3.7, there exists a prime ideal $P \in \operatorname{Spec} A$ such that $J \subseteq P$ and $f \notin P$. If $\bar{f}$ denotes the image of f in the integral domain $R = A/P$, then $\bar{f} \neq 0$. As a k-algebra, R is finitely generated. The localization $R_{\bar{f}}$ is generated as an R-algebra by the element $\bar{f}^{-1}$, hence $R_{\bar{f}}$ is finitely generated as a k-algebra. Let $\mathfrak{m}$ be any maximal ideal in $R_{\bar{f}}$. Since k is algebraically closed, Corollary 6.2.4 says the natural map $k \to R_{\bar{f}}/\mathfrak{m}$ is onto. Let M be the kernel of the composition of natural maps
$$A \to R \to R_{\bar{f}} \to R_{\bar{f}}/\mathfrak{m}.$$
Then M is a maximal ideal in A such that $f \notin M$ and $J \subseteq P \subseteq M$. By Theorem 6.2.6, $Z(M)$ is a singleton set $\{x\}$. This shows $x \in Z(J)$ and $f(x) \neq 0$. □

PROPOSITION 6.2.10. *Let k be an algebraically closed field and $A = k[x_1, \dots, x_n]$.*

(1) If $T_1 \subseteq T_2$ are subsets of A, then $Z(T_1) \supseteq Z(T_2)$.
(2) If $Y_1 \subseteq Y_2$ are subsets of $\mathbb{A}^n$, then $I(Y_1) \supseteq I(Y_2)$.
(3) For $Y_1, Y_2 \subseteq \mathbb{A}^n$ we have $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.
(4) For any ideal $J \subseteq A$, $I(Z(J)) = \operatorname{Rad}(J)$.
(5) For any subset $Y \subseteq \mathbb{A}^n$, $Z(I(Y)) = \bar{Y}$, the closure of Y.

PROOF. (1), (2), (3): are obvious.
(4): is a restatement of Theorem 6.2.9.
(5) The proof of Lemma 3.3.8 applies. □

Corollary 6.2.11 below is the counterpart for the Zariski topology on $\mathbb{A}^n_k$ of Corollary 3.3.9. The set of maximal ideals in the ring $A = k[x_1, \dots, x_n]$ is denoted $\operatorname{Max} A$. By Theorem 6.2.6, when k is algebraically closed, maximal ideals in $\operatorname{Max} A$ correspond to points in k^n. Since it is a subset of $\operatorname{Spec} A$, $\operatorname{Max} A$ inherits the Zariski topology. It follows from Corollary 6.2.11 that the Zariski topology on $\operatorname{Max} A$ agrees with the Zariski topology on $\mathbb{A}^n_k$.

COROLLARY 6.2.11. *Let k be an algebraically closed field. There is a one-to-one order-reversing correspondence between algebraic subsets of $\mathbb{A}^n$ and radical ideals in A given by $Y \mapsto I(Y)$ and $J \mapsto Z(J)$. Under this correspondence, an algebraic set Y is irreducible if and only if $I(Y)$ is a prime ideal.*

PROOF. The first part follows from Proposition 6.2.10. The last part can be proved as in Lemma 3.3.10. $\square$

EXAMPLE 6.2.12. Let k be an algebraically closed field and $A = k[x_1, \dots, x_n]$. The zero ideal (0) is a prime ideal of A. By Corollary 6.2.11 this implies $\mathbb{A}^n_k$ is irreducible. By Lemma 1.3.4, if U is a nonempty open subset of $\mathbb{A}^n_k$, then U is irreducible and dense.

EXAMPLE 6.2.13. Let k be a field and A a k-algebra. Assume $\dim_k(A) = n$ is finite. Using the left regular representation, we can embed A as a k-subalgebra of $\operatorname{Hom}_k(A,A)$ (see Example 1.1.13). As in [**18**, Example 1.2.3], the norm $N^A_k : A \to k$ is a homogeneous polynomial function on A of degree n and the trace $T^A_k : A \to k$ is a homogeneous linear polynomial function on A. Fix a k-basis $\alpha_1, \dots, \alpha_n$ for A. With respect to this basis, we identify A with affine n-space over k (Definition 6.2.5). That is, an element $a_1\alpha_1 + \cdots + a_n\alpha_n \in A$ corresponds to the point $(a_1, \dots, a_n) \in \mathbb{A}^n_k$. With this identification, the norm $N^A_k : A \to k$ corresponds to a homogeneous polynomial in $k[x_1, \dots, x_n]$ of degree n. Using Exercise 1.7.2 we see that an element α in A is invertible if and only if $N^A_k(\alpha) \neq 0$. The set A^* of invertible elements of A is therefore a proper open subset of $\mathbb{A}^n_k$. If k is algebraically closed, Example 6.2.12 implies A^* is a dense open subset of $\mathbb{A}^n_k$. If A is a division algebra over k, then the norm defines a homogeneous polynomial in $k[x_1, \dots, x_n]$ of degree n with no nontrivial zeros. We should advise the reader that the norm used in this example is not the norm defined specifically for an Azumaya algebra (or central simple algebra) in [**18**, Section 11.1.1].

EXAMPLE 6.2.14. Let k be a field and $n \geq 1$. Given any point $P = (a_1, \dots, x_n)$ in $\mathbb{A}^n_k$, let M be the ideal in $k[x_1, \dots, x_n]$ generated by $x_1 - a_1, \dots, x_n - a_n$. Then $Z(M) = \{P\}$, so singleton sets are closed in the Zariski topology. In the terminology of Section 1.3, this shows $\mathbb{A}^n_k$ is a T_1-space.

EXAMPLE 6.2.15. Let k be an algebraically closed field and $n \geq 1$. If M is a maximal ideal in $A = k[x_1, \dots, x_n]$, then by Theorem 6.2.6, there is a point $P = (a_1, \dots, a_n)$ in $\mathbb{A}^n_k$ such that $M = (x_1 - a_1, \dots, x_n - a_n)$ and $Z(M)$ is the singleton set $\{P\}$. Conversely, if $P = (a_1, \dots, x_n)$ is an arbitrary point in $\mathbb{A}^n_k$, then $I(P)$ is the maximal ideal in $k[x_1, \dots, x_n]$ generated by $x_1 - a_1, \dots, x_n - a_n$. Under the one-to-one correspondence of Corollary 6.2.11, maximal ideals in A correspond to closed points in $\mathbb{A}^n_k$.

COROLLARY 6.2.16. *If k is an algebraically closed field and I is an ideal in $A = k[x_1, \dots, x_n]$, then the radical of I is equal to the intersection of those maximal ideals of A that contain I. That is,*

$$\operatorname{Rad}(I) = \bigcap \{\mathfrak{m} \mid \mathfrak{m} \in \operatorname{Max} A \text{ and } I \subseteq \mathfrak{m}\}.$$

PROOF. By Lemma 3.3.7, $\operatorname{Rad}(I) = \bigcap_{\mathfrak{P} \in V(I)} \mathfrak{P}$. Hence $\operatorname{Rad}(I)$ is always a subset of $\bigcap \{\mathfrak{m} \mid \mathfrak{m} \in \operatorname{Max} A \text{ and } I \subseteq \mathfrak{m}\}$. Let $\alpha \in A$ and assume α belongs to every maximal ideal $\mathfrak{m}$ of A such that $I \subseteq \mathfrak{m}$. There is a one-to-one correspondence between points $P \in Z(I)$ and maximal ideals $\mathfrak{m}$ in A such that $I \subseteq \mathfrak{m}$. Therefore, $\alpha(P) = 0$ for every $P \in Z(I)$. By Theorem 6.2.9, $\alpha \in \operatorname{Rad}(I)$. $\square$

See Exercise 6.3.2 for a generalization of Corollary 6.2.16 to the case where the ground field k is not algebraically closed.

2.3. A Nonsingular Affine Elliptic Curve. This section is devoted to an example of an algebraic curve that is nonsingular and nonrational. Assume that the characteristic of k, the base field, is not 2. Let $A = k[x]$ be the polynomial ring in one variable over k. Then A is a unique factorization domain and x is a prime in A. Let $K = k(x)$ be the quotient field of A. Consider the polynomial $y^2 - x(x^2-1)$ in $A[y]$. By Eisenstein's Criterion, with prime $p = x$, $y^2 - x(x^2-1)$ is irreducible in $A[y]$. By Gauss' Lemma, $y^2 - x(x^2-1)$ is irreducible in $K[y]$ and $F = K[y]/(y^2 - x(x^2-1))$ is a field. The separable quadratic extension F/K is a Galois extension, $\operatorname{Aut}_K(F) = \langle \sigma \rangle$ has order 2, and σ is defined by $y \mapsto -y$.

In the following, cosets in the factor ring F are written without brackets or any extra adornment. The polynomial ring $A[y] = k[x,y]$ is a unique factorization domain. Therefore, $R = k[x,y]/(y^2 - x(x^2-1))$ is an integral domain. The diagram of ring homomorphisms

$$\begin{tikzcd}
A = k[x] \arrow[r] \arrow[d] & K = k(x) \arrow[d] \\
A[y] \arrow[r, "\alpha"] \arrow[d, "\eta"'] & K[y] \arrow[d, "\eta"] \\
R = A[y]/(y^2 - x(x^2-1)) \arrow[r, "\phi"] & F = K[y]/(y^2 - x(x^2-1))
\end{tikzcd} \tag{2.2}$$

commutes. The vertical maps are the natural maps. The map ϕ is induced by α and is one-to-one.

PROPOSITION 6.2.17. *In the above context, the following are true.*

(1) *The quotient field of R is F.*
(2) *As an A-module, R is free of rank 2. The set $\{1, y\}$ is a free basis. The image of ϕ is $\{p(x) + q(x)y \mid$ where $p(x)$ and $q(x)$ are in $A = k[x]\}$.*
(3) *The homomorphism $A \to R$ defined by sending x to its image in R is one-to-one.*
(4) *The automorphism $\sigma \in \operatorname{Aut}_K(F)$ defined by $y \mapsto -y$ restricts to an automorphism $\sigma : R \to R$.*
(5) *For any $a \in R$, define the norm of a to be $N(a) = a\sigma(a)$. Then $N(1) = 1$, $N : R \to A$, and N is multiplicative.*
(6) *The map on groups of units $k^* \to R^*$ is an isomorphism. That is, the units of R are precisely the units of k.*
(7) *x and y are irreducible elements of R.*
(8) *R is not a unique factorization domain.*
(9) *R is not a principal ideal domain.*

PROOF. (1), (2), (3), (4), and (5): These follow from Exercise 1.8.4 and Example 1.6.10 (2).

(6): The map $k \to R$ is one-to-one because k is a field. We show that $k^* \to R^*$ is onto. Let $a, b \in R$ and assume $ab = 1$. Then $N(a)N(b) = 1$ in A. But $A^* = k^*$. This proves $N(a) \in k$. By (2), a has a unique representation in the form $a = f + gy$, for polynomials f and g in $A = k[x]$. Then $N(a) = f^2 - g^2x(x^2-1) = u$ for some $u \in k^*$. Then $(f(0))^2 = u$. If $g \neq 0$, then the leading term of f^2 which is even is equal to the leading term of $g^2x(x^2-1)$, which is odd, a contradiction. Therefore, $g = 0$ and $a = f = f(0)$ is in k.

(7): If x is not irreducible, then there is a nontrivial factorization $x = ab$. By (5), we have the factorization $N(x) = x^2 = N(a)N(b)$ in $A = k[x]$. Therefore, $N(a) = x$ up to associates. By (2), a has a representation in the form $a = f + gy$, for polynomials f and g in $A = k[x]$. Then up to associates, $N(a) = f^2 - g^2x(x^2-1) = x$. Then $f^2 = g^2x(x^2-1) + x$

which is impossible because the degree of the left hand is even and that of the right hand side is odd. This proves x is not in the image of the norm map $N : R \to A$, hence x is irreducible in R.

If y is not irreducible in R, then there is a nontrivial factorization $y = ab$. By (5), we have the factorization $N(y) = x(x^2-1) = N(a)N(b)$ in $A = k[x]$. Therefore, up to associates, one of $N(a)$ or $N(b)$ is in $\{x, x+1, x-1\}$. The same proof from above shows that $x+1$ and $x-1$ are not in the image of $N : R \to A$. Therefore, y is irreducible in R.

(8): In R we have the identity $y^2 = x(x^2-1)$. By the proof of (7), $N(x) = x^2$ and $N(y) = x(x^2-1)$. Therefore, x and y are not associates of each other. So unique factorization does not exist.

(9): Consider the ideal $\mathfrak{m} = (x,y)$. Then $R/\mathfrak{m} = k[x,y]/(x,y) = k$ is a field, hence $\mathfrak{m}$ is a maximal ideal. If $\mathfrak{m} = (a)$ is principal, then $a \mid x$ and $a \mid y$. Since x and y are irreducible, by Lemma 1.5.2, this implies x and y are associates of each other, a contradiction to (8). □

2.4. An Application to Characteristic Polynomials. We apply results from Section 6.2.2 to show that the characteristic polynomial of AB is equal to the characteristic polynomial of BA when A and B are two n-by-n matrices with entries in an integral domain R.

THEOREM 6.2.18. *Let R be an integral domain. If A and B are n-by-n matrices in $M_n(R)$, then* $\operatorname{char.poly}_R(AB) = \operatorname{char.poly}_R(BA)$.

PROOF. Let k be an algebraically closed field containing R as a subring. Let $\theta : R \to k$ be the set containment map. Viewing the ring $M_n(R)$ as a subring of $M_n(k)$, it suffices to prove the theorem for matrices in $M_n(k)$. As a k-vector space, $M_n(k)$ has dimension n^2 and the set $\{e_{ij} \mid 1 \le i \le n, 1 \le j \le n\}$ of elementary matrices is a basis. We identify $M_n(k)$ with the point set $\mathbb{A}_k^{n^2}$. As in [**18**, Lemma 1.2.2], if C is a matrix in $M_n(k)$ and the characteristic polynomial of C is $\operatorname{char.poly}_k(C) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, then for each $i = 1, \dots, n$, the assignment $C \mapsto (-1)^i a_i$ defines a polynomial function $N_i : M_n(k) \to k$ which is homogeneous of degree i in n^2 variables. Fix A in $M_n(k)$ and define $f_i : M_n(k) \to k$ by $f_i(B) = N_i(AB) - N_i(BA)$. Using the definition of multiplication of matrices we see that f is a polynomial function which is homogeneous of degree i in n^2 variables. The set of zeros of f_i is a closed subset of $M_n(k)$. If B is an invertible matrix in $M_n(k)$, then $BA = B(AB)B^{-1}$. Similar matrices have the same characteristic polynomial, so in this case $\operatorname{char.poly}_k(AB) = \operatorname{char.poly}_k(BA)$. For each $1 \le i \le n$, this implies $f_i(B) = 0$ for all invertible matrices B in $M_n(k)$. By Example 6.2.13, the set of invertible matrices in $M_n(k)$ is a dense open set. Since f_i is zero on a dense set, f_i is the zero function. Since k is an infinite field, this implies f_i is the zero polynomial. Since this is true for each i, we conclude that $\operatorname{char.poly}_R(AB) = \operatorname{char.poly}_R(BA)$ for all A and for all B. □

2.5. Exercises.

EXERCISE 6.2.1. Let k be any field and I an ideal in $A = k[x_1, \dots, x_n]$. Prove:
(1) $Z(I) = Z(\operatorname{Rad}(I))$.
(2) $\operatorname{Rad}(I) \subseteq I(Z(I))$.

EXERCISE 6.2.2. Let k be a field, I an ideal in $A = k[x_1, \dots, x_n]$, and $S = A/I$. A point $P = (a_1, \dots, a_n)$ in $Z(I)$ is called a *k-rational point* on the algebraic set. Show that the k-rational points on $Z(I)$ correspond to k-algebra homomorphisms $\sigma : S \to k$.

EXERCISE 6.2.3. Let R be a commutative ring, $I = (f_1, \dots, f_m)$ an ideal in $A = R[x_1, \dots, x_n]$ generated by m polynomials, and $S = A/I$. A point $P = (a_1, \dots, a_n)$ in $\mathbb{A}_R^n$

is called an *R-rational point* of S if $f_i(P) = 0$ for $1 \le i \le m$. Show that the R-rational points of S correspond to R-algebra homomorphisms $\sigma : S \to R$.

EXERCISE 6.2.4. Let R be a commutative ring and $\phi : R[x_1,\dots,x_m] \to R[y_1,\dots,y_n]$ an R-algebra homomorphism between two polynomial rings with coefficients in R.

(1) Let $S \subseteq R$ be a finite subset which contains all of the coefficients of the polynomials $\phi(x_1),\dots,\phi(x_m)$. View R as a $\mathbb{Z}$-algebra. Let N be the $\mathbb{Z}$-subalgebra of R generated by S. Show that there is an N-algebra homomorphism ϕ_N such that the diagram

$$\begin{tikzcd} N[x_1,\dots,x_m] \arrow[r, "\phi_N"] \arrow[d] & N[y_1,\dots,y_n] \arrow[d] \\ R[x_1,\dots,x_m] \arrow[r, "\phi"] & R[y_1,\dots,y_n] \end{tikzcd}$$

commutes, where the vertical maps are induced by $N \subseteq R$. Moreover, show that the bottom row is obtained from the top by applying the functor $(\ ) \otimes_N R$.

(2) Show that $\operatorname{im}(\phi) = \operatorname{im}(\phi_N) \otimes_N R$.

(3) Show that $\ker(\phi_N)$ is a finitely generated ideal.

(4) Show that $\ker(\phi)$ is a finitely generated ideal.

EXERCISE 6.2.5. The purpose of this exercise is to prove the converse of Exercise 4.1.13 when R is commutative. Let k be a field and R a commutative artinian finitely generated k-algebra. Prove that R is finite dimensional as a k-vector space. (Hints: Use Theorem 4.5.6 to reduce to the case where R is local artinian. Consider the chain $R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots \supseteq \mathfrak{m}^k \supseteq 0$. Show that each factor $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a finitely generated vector space over k. For the first factor $R/\mathfrak{m}$, apply Corollary 6.2.4.)

EXERCISE 6.2.6. Let k be an algebraically closed field, I an ideal in $A = k[x_1,\dots,x_n]$, and $R = A/I$. Prove that the following are equivalent.

(1) R is artinian.

(2) $\dim_k(R) < \infty$.

(3) $Z(I)$ is a finite set.

Moreover, prove that $\dim_k(R)$ is an upper bound on the number of points in $Z(I)$.

EXERCISE 6.2.7. Let R be a commutative ring. Viewing R as a $\mathbb{Z}$-algebra, show that $R = \varinjlim R_\alpha$, where $\{R_\alpha\}$ is a directed system of noetherian subrings of R.

EXERCISE 6.2.8. Let R be a commutative local ring with maximal ideal $\mathfrak{m}$. Show that there is a directed system $\{R_\alpha\}$ of noetherian local subrings of R satisfying the following:

(1) The maximal ideal of R_α is $\mathfrak{m}_\alpha = \mathfrak{m} \cap R_\alpha$.

(2) $R = \varinjlim R_\alpha$.

(3) $\mathfrak{m} = \varinjlim \mathfrak{m}_\alpha$.

(4) $R/\mathfrak{m} = \varinjlim (R_\alpha/\mathfrak{m}_\alpha)$.

EXERCISE 6.2.9. In the context of Proposition 6.2.17, consider the maximal ideal $\mathfrak{m} = (x,y)$. Show that $\mathfrak{m}^2$ is principal.

EXERCISE 6.2.10. Let k be a field and $A = k[x_1,\dots,x_n]$ the polynomial ring over k in n variables. Let $\mathfrak{m}$ be a maximal ideal in A. The following is an outline of a proof that Hilbert's Nullstellensatz (Theorem 6.2.9) implies the Weak Form of the Nullstellensatz (Corollary 6.2.4).

(1) Let Ω be an algebraic closure of k. View A as a subring of $\Omega[x_1,\dots,x_n]$. Using Theorem 6.2.9, show that there exists a point $P=(a_1,\dots,a_n)$ in $\mathbb{A}^n_\Omega$ such that P is in $Z(\mathfrak{m})$, the zero set of $\mathfrak{m}$.
(2) Let $P=(a_1,\dots,a_n)$ be the point in $\mathbb{A}^n_\Omega$ from (1). Show that $F=k(a_1,\dots,a_n)$ is a finitely generated algebraic extension field of $A/\mathfrak{m}$.
(3) Use the above to prove Corollary 6.2.4.

EXERCISE 6.2.11. Let k be a field. Let A and B be finitely generated k-algebras and assume A and B are integral domains. Suppose there exist $\mathfrak{p}\in\operatorname{Spec}A$, $\mathfrak{q}\in\operatorname{Spec}B$ and a k-algebra isomorphism $\phi: A_\mathfrak{p}\to B_\mathfrak{q}$. Show that there exists $\alpha\in A-\mathfrak{p}$, $\beta\in B-\mathfrak{q}$ such that ϕ restricts to a k-algebra isomorphism $\phi: A_\alpha\to B_\beta$. (Hint: Lemma 3.1.12.)

3. Integral Extensions and Prime Ideals

In this section we prove the Going Up and Going Down Theorems, which are also known as the Cohen-Seidenberg Theorems. These are combined in Theorem 6.3.6. For an integral extension of commutative rings $A\to B$ these theorems relate the correspondence between prime ideals in A and B.

3.1. Prime Ideals. The purpose of this section is to prove some necessary results on prime ideals. The first, Lemma 6.3.2, is a result on rings that are not necessarily commutative. In Definition 1.5.1 we defined the notion of prime ideal in a commutative ring. Definition 6.3.1 below extends this definition to ideals in a general ring.

DEFINITION 6.3.1. If P is a two-sided ideal in a ring R, then we say P is *prime* in case $P\neq R$ and for any two-sided ideals I and J, if $IJ\subseteq P$, then $I\subseteq P$ or $J\subseteq P$. If R is a commutative ring, Proposition 1.5.4 shows that this definition agrees with Definition 1.5.1.

LEMMA 6.3.2. *Let R be a ring and assume $I,P_1,P_2,\dots,P_n$ are two-sided ideals. If $n\geq 3$, then assume $P_3,\dots,P_n$ are prime. If $I\subseteq P_1\cup P_2\cup\cdots\cup P_n$, then $I\subseteq P_k$ for some k.*

PROOF. By removing any P_i which is contained in another P_j, we can assume that no containment relation $P_i\subseteq P_j$ occurs unless $i=j$. The proof is by induction on n. Assume $I\subseteq P_1\cup P_2$. For contradiction's sake assume I is not contained in P_1 or P_2. Pick $x_2\in I-P_1$ and $x_1\in I-P_2$. Then $x_1\in P_1$ and $x_2\in P_2$. Since $x_1+x_2\in I\subseteq P_1\cup P_2$, there are two cases. If $x_1+x_2\in P_1$, then we get $x_2\in P_1$ which is a contradiction. Otherwise, $x_1+x_2\in P_2$, which says $x_1\in P_2$ which is also a contradiction.

Inductively assume $n>2$ and that the result holds for $n-1$. Assume P_n is prime and that no containment relation $P_i\subseteq P_n$ occurs unless $i=n$. Assume $I\subseteq P_1\cup\cdots\cup P_n$ and for contradiction's sake, assume $I\not\subseteq P_i$ for all i. Then $IP_1\cdots P_{n-1}\not\subseteq P_n$. Pick an element x in $IP_1\cdots P_{n-1}$ which is not in P_n. If $I\subseteq P_1\cup\cdots\cup P_{n-1}$, then by induction $I\subseteq P_i$ for some i. Therefore we assume $S=I-(P_1\cup\cdots\cup P_{n-1})$ is not empty. So $S\subseteq P_n$. Pick $s\in S$ and consider $s+x$ which is in I because both s and x are. Then by assumption, $s+x$ is in one of the ideals P_i. Suppose $s+x\in P_i$ and $1\leq i\leq n-1$. Because $x\in P_i$, this implies $s\in P_i$ which is a contradiction. Therefore $s+x\in P_n$. But $s\in P_n$ implies $x\in P_n$ which is again a contradiction. $\square$

LEMMA 6.3.3. *Let $P,I_1,\dots,I_n$ be ideals in the commutative ring R and assume P is prime.*

(1) If $P\supseteq\bigcap_{i=1}^n I_i$, then $P\supseteq I_i$ for some i.
(2) If $P=\bigcap_{i=1}^n I_i$, then $P=I_i$ for some i.

PROOF. (1): For contradiction's sake, assume for each i that there exists $x_i \in I_i - P$. Let $x = x_1 x_2 \cdots x_n$. So $x \notin P$ but $x \in \bigcap I_i$, a contradiction.

(2): Is left to the reader. $\square$

3.2. Going Up and Going Down Theorems. Let $\phi : A \to B$ be a homomorphism of commutative rings. In this section we study the relation between prime ideals of A and prime ideals of B. Prime ideals of A will be denoted p, p_1, p_2 and prime ideals of B will be denoted q, q_1, q_2. For notational convenience, instead of $\phi^{-1}(q)$, we will write $q \cap A$. In this case, $p = q \cap A$ is a prime ideal of A, and we say *q lies over p*. By pB we denote the ideal of B generated by $\phi(p)$. As in Exercise 3.3.8, a minimal element of $V(pB)$ is called a minimal over-ideal of pB. The going up and going down terminology refers to set containment and the existence of ideals in $\operatorname{Spec} B$ lying over a chain of ideals $p_1 \subsetneq p_2$ in $\operatorname{Spec} A$. We say *going down holds for ϕ*, if for all such p_1, p_2, whenever there exists q_2 lying over p_2, then there also exists q_1 lying over p_1 such that $q_1 \subsetneq q_2$. Proposition 6.3.4 provides an equivalent condition to going down. We say *going up holds for ϕ*, if for all such p_1, p_2, whenever there exists q_1 lying over p_1, then there also exists q_2 lying over p_2 such that $q_1 \subsetneq q_2$.

PROPOSITION 6.3.4. *Let $\phi : A \to B$ be a homomorphism of commutative rings. The following are equivalent.*

(1) For any p_1, p_2 in $\operatorname{Spec} A$ such that $p_1 \subsetneq p_2$, and for any $q_2 \in \operatorname{Spec} B$ lying over p_2, there exists $q_1 \in \operatorname{Spec} B$ lying over p_1 such that $q_1 \subsetneq q_2$.

(2) For any p in $\operatorname{Spec} A$, if q is a minimal prime over-ideal in $\operatorname{Spec} B$ for pB, then $q \cap A = p$.

PROOF. (1) implies (2): Let $p \in \operatorname{Spec} A$ and assume $q \in \operatorname{Spec} B$ is minimal such that $q \supseteq pB$. Then $q \cap A \supseteq p$. Assume $q \cap A \neq p$. According to (1) there exists $q_1 \in \operatorname{Spec} B$ such that $q_1 \cap A = p$ and $q_1 \subsetneq q$. In this case $pB \subseteq q_1 \subsetneq q$ which is a contradiction to the minimal property of q.

(2) implies (1): Assume $p_1 \subsetneq p_2$ are in $\operatorname{Spec} A$ and $q_2 \in \operatorname{Spec} B$ such that $q_2 \cap A = p_2$. By Exercise 3.3.8, pick any minimal prime over-ideal q_1 for $p_1 B$ such that $p_1 B \subseteq q_1 \subseteq q_2$. By (2), we have $q_1 \cap A = p_1$. $\square$

Now we show that going down always holds if B is a flat A-algebra.

THEOREM 6.3.5. *If $\phi : A \to B$ is a homomorphism of commutative rings such that B is a flat A-algebra, then going down holds for ϕ.*

PROOF. Let $p_1 \subsetneq p_2$ in $\operatorname{Spec} A$ and $q_2 \in \operatorname{Spec} B$ such that $q_2 \cap A = p_2$. Then $\phi_2 : A_{p_2} \to B_{q_2}$ is a local homomorphism of local rings. By Proposition 3.7.2, B_{q_2} is a flat A_{p_2}-algebra. By Exercise 3.5.12, B_{q_2} is a faithfully flat A_{p_2}-algebra. By Lemma 3.5.5, $\phi_2^\sharp : \operatorname{Spec} B_{q_2} \to \operatorname{Spec} A_{p_2}$ is onto. Let $Q_1 \in \operatorname{Spec} B_{q_2}$ be a prime ideal lying over $p_1 A_{p_2}$ and set $q_1 = Q_1 \cap B$. Then $q_1 \subseteq q_2$. The commutative diagram

$$\begin{tikzcd} \operatorname{Spec} B_{q_2} \arrow[r, "\phi_2^\sharp"] \arrow[d] & \operatorname{Spec} A_{p_2} \arrow[d] \\ \operatorname{Spec} B \arrow[r, "\phi^\sharp"] & \operatorname{Spec} A \end{tikzcd}$$

shows that q_1 is a prime ideal of B lying over p_1. $\square$

The following useful form of the Going Up and Going Down Theorem as well as its proof are from [**41**, (5.E), Theorem 5].

THEOREM 6.3.6. *Assume B is a commutative faithful integral A-algebra.*

(1) *The natural map $\theta^\sharp : \operatorname{Spec} B \to \operatorname{Spec} A$ is onto.*
(2) *If $p \in \operatorname{Spec} A$ and $q_1, q_2 \in \operatorname{Spec} B$ are two primes in B lying over p, then q_1 is not a subset of q_2.*
(3) *(Going Up Holds) For any p_1, p_2 in $\operatorname{Spec} A$ such that $p_1 \subsetneq p_2$, and for any $q_1 \in \operatorname{Spec} B$ lying over p_1, there exists $q_2 \in \operatorname{Spec} B$ lying over p_2 such that $q_1 \subsetneq q_2$.*
(4) *If $q \in \operatorname{Spec} B$ and $p = q \cap A$, then q is a maximal ideal of B if and only if p is a maximal ideal of A.*

For (5) and (6) assume A and B are integral domains, that K is the quotient field of A and that A is integrally closed in K.

(5) *(Going Down Holds) For any p_1, p_2 in $\operatorname{Spec} A$ such that $p_1 \subsetneq p_2$, and for any $q_2 \in \operatorname{Spec} B$ lying over p_2, there exists $q_1 \in \operatorname{Spec} B$ lying over p_1 such that $q_1 \subsetneq q_2$.*
(6) *If L is a normal extension field of K, and B is equal to the integral closure of A in L, then any two prime ideals of B lying over the same prime $p \in \operatorname{Spec} A$ are conjugate to each other by some automorphism $\sigma \in \operatorname{Aut}_K(L)$.*

PROOF. (4): We have B/q is a faithful integral A/p-algebra (Exercise 6.1.2). If follows from Lemma 6.1.4 that A/p is a field if and only if B/q is a field. Or in other words, q is a maximal ideal if and only if p is a maximal ideal.

(1) and (2): Let $p \in \operatorname{Spec} A$. Tensoring the integral extension $A \to B$ with $(\ ) \otimes_A A_p$ we get the integral extension $A_p \to B \otimes_A A_p$. The prime ideals of B lying over p correspond to the prime ideals of B_p lying over pA_p. By (4), these are the maximal ideals of B_p. The ring B_p contains at least one maximal ideal, by Zorn's Lemma. This proves (1). Because there is no inclusion relation between two maximal ideals, this proves (2).

(3): Suppose p_1, p_2 are in $\operatorname{Spec} A$ and $p_1 \subsetneq p_2$. Assume q_1 is in $\operatorname{Spec} B$ such that $p_1 \cap A = p_1$. Then $A/p_1 \to B/q_1$ is an integral extension of rings. By (1) there exists a prime ideal q_2/q_1 in $\operatorname{Spec}(B/q_1)$ lying over p_2/p_1. Then $q_2 \in \operatorname{Spec} B$ lies over p_2 and $q_1 \subsetneq q_2$.

(6): Let $G = \operatorname{Aut}_K(L)$ be the group of K-automorphisms of L. If $\sigma \in G$, then σ restricts to an A-automorphism of B. In particular, if $q \in \operatorname{Spec} B$, then $\sigma(q)$ is also in $\operatorname{Spec} B$. Let $q, q' \in \operatorname{Spec} B$ and assume $q \cap A = q' \cap A$. We show that $q' = \sigma(q)$ for some $\sigma \in G$.

First we prove this under the assumption that $(L : K)$ is finite. Then $G = \{\sigma_1, \dots, \sigma_n\}$ is finite as well. Let $\sigma_i(q) = q_i$, for $1 \le i \le n$. For contradiction's sake, assume $q' \neq q_i$ for any i. By (2), q' is not contained in any q_i. By Lemma 6.3.2, there exists $x \in q'$ such that x is not in any q_i. Suppose ℓ is the characteristic of K. Set

$$y = \begin{cases} \prod_{i=1}^n \sigma_i(x) & \text{if } \ell = 0 \\ \left(\prod_{i=1}^n \sigma_i(x)\right)^{\ell^\nu} & \text{if } \ell > 0 \end{cases}$$

where ν is chosen to be a sufficiently large positive integer such that y is separable over K. It follows that $y \in K$. Since $\sigma_i(x) \notin q$ for each i and q is a prime ideal, it follows that $y \notin q$. Notice that $y \in B \cap K$, so y is integral over A. Since A is integrally closed in K we see that $y \in A$. Since $x \in q'$, it follows that $y \in q' \cap A = q \cap A$. This is a contradiction.

Now assume L is infinite over K. Let $F = L^G$ be the subfield fixed by G. Then L is Galois over F and F is purely inseparable over K.

If $F \neq K$, let ℓ be the characteristic of K and let C be the integral closure of A in F. Let $p \in \operatorname{Spec} A$ and let S be the set of all x in C such that $x^{\ell^\nu} \in p$ for some $\nu \ge 0$. Let $q \in \operatorname{Spec} C$

such that $p = q \cap A$. Then clearly $S \subseteq q$. Conversely, if $x \in q$, then $x \in F$, so x is algebraic and purely inseparable over K. So $x^{\ell^\nu} \in K$ for some $\nu \geq 0$. Since x is integral over A, there is a monic polynomial $f(t) \in A[t]$ such that $f(x) = 0$. Then $0 = (f(x))^{\ell^\nu} = f(x^{\ell^\nu})$ so x^{ℓ^ν} is integral over A. Because A is integrally closed in K, $x^{\ell^\nu} \in A \cap q = p$. This shows that S is the unique prime ideal of C lying over p. Replace K with F, A with C and p with S. It is enough to prove (6) under the assumption that L is Galois over K.

Assume L over K is a Galois extension and that B is the integral closure of A in L. Let $q, q' \in \operatorname{Spec} B$ and assume $q \cap A = q' \cap A = p$. Let $\mathscr{S}$ be the set of all finite Galois extensions T of K contained in L. If $T \in \mathscr{S}$, let

$$F_0(T) = \{\sigma \in \operatorname{Aut}_K(T) \mid \sigma(q \cap T) = q' \cap T\}.$$

By the finite version of (6) we know that $F_0(T)$ is a nonempty closed subset of G. Let $F(T)$ be the preimage of $F_0(T)$ under the continuous mapping $G \to \operatorname{Aut}_K(T)$. Then $F(T)$ is a nonempty closed subset of G. If $T \subseteq T'$ are two such intermediate fields in $\mathscr{S}$, then $F(T) \supseteq F(T')$. For any finite collection $\{T_1, \dots, T_n\}$ of objects in $\mathscr{S}$, there is another object T in $\mathscr{S}$ such that $T_i \subseteq T$ for all i. Therefore, $\cap_{i=1}^n F(T_i) \supseteq F(T) \neq \emptyset$. Because G is compact, this means

$$F = \bigcap_{T \in \mathscr{S}} F(T) \neq \emptyset.$$

Let $\sigma \in F$. For every $x \in q$, there is some intermediate field T in $\mathscr{S}$ such that $x \in q \cap T$. Hence $\sigma(x) \in q' \cap T$. Therefore $\sigma(q) = q'$.

(5): Let L_1 be the quotient field of B and K the quotient field of A. Let L be a normal extension of K containing L_1. Let C be the integral closure of A in L. Then C is also the integral closure of B in L. We are given $p_1, p_2 \in \operatorname{Spec} A$ such that $p_1 \subsetneq p_2$ and $q_2 \in \operatorname{Spec} B$ such that $p_2 = q_2 \cap A$. Let Q_1 be a prime ideal in $\operatorname{Spec} C$ lying over p_1. By Part (3) applied to $A \subseteq C$, there is $Q_2 \in \operatorname{Spec} C$ lying over p_2 such that $Q_1 \subsetneq Q_2$. Let Q be in $\operatorname{Spec} C$ lying over q_2. Since $p_2 = Q \cap A = Q_2 \cap A$, by Part (6) there exists $\sigma \in \operatorname{Aut}_K(L)$ such that $\sigma(Q_2) = Q$. Put $q_1 = \sigma(Q_1) \cap B$. Then $q_1 \subsetneq q_2$ and $q_1 \cap A = \sigma(Q_1) \cap A = Q_1 \cap A = p_1$. □

COROLLARY 6.3.7. *Let R be a local ring and S a commutative R-algebra which is faithful and finitely generated as an R-module. Then S is semilocal.*

PROOF. Let $\mathfrak{m}$ be the maximal ideal of R. By Theorem 6.3.6 (4), the maximal ideals of S correspond to the maximal ideals of $S/\mathfrak{m}S$. Because $S/\mathfrak{m}S$ is finite dimensional over $R/\mathfrak{m}$, it is artinian (Exercise 4.1.13). By Proposition 4.5.3, $S/\mathfrak{m}S$ is semilocal. □

3.3. Exercises.

EXERCISE 6.3.1. Let S be a commutative faithful integral R-algebra. Let $J(R)$ be the Jacobson radical of R, and $J(S)$ the Jacobson radical of S. Prove that $J(R) = J(S) \cap R$.

EXERCISE 6.3.2. Prove the following generalization of Corollary 6.2.16. Let k be a field and R a finitely generated k-algebra. Prove:

(1) The Jacobson radical of R, $J(R)$, is equal to the nil radical of R, $\operatorname{Rad}_R(0)$. (Hints: If $\bar{k}$ is an algebraic closure of k, then $\bar{R} = R \otimes_R \bar{k}$ is a faithfully flat integral R-algebra. Exercise 6.3.1.)
(2) If $\alpha \in R$ and α is not a nilpotent element of R, then the basic open set $U(\alpha)$ contains a closed point of $\operatorname{Spec} R$. If U is a nonempty open subset of $\operatorname{Spec} R$, then U contains a closed point of $\operatorname{Spec} R$.

CHAPTER 7

The Topological Completion of Rings and Modules

We define filtrations and completions for modules over a general ring, but for most of this chapter, the ground ring is assumed to be commutative. A nonincreasing chain of submodules $\{M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots\}$ in an R-module M is called a filtration of M. Associated to a filtration is a topology on M. The completion of M with respect to the topology defined by a filtration is denoted M^*. The subject of this chapter is the functor that maps M to M^*. We study many of the functorial properties of completion of both rings and modules. If I is an ideal of R, then the I-adic topology on M is defined by the filtration $\{M \supseteq IM \supseteq I^2M \supseteq I^3M \supseteq \cdots\}$. The completion of an R-module with respect to the topology defined by a filtration is equal to an inverse limit. Therefore, the topics in this chapter are extensions of those we studied in Section 2.7.

In Section 7.2 we study graded rings. There is a fundamental connection between graded rings and the filtration of a ring R by ideals. The I-adic completion of a commutative ring R is denoted $\hat{R}$. We show $\hat{R}$ is a flat R-algebra, if R is noetherian. The roles played by graded rings are central to the proofs.

Modules which are separated and complete with respect to a topology play an important role in commutative algebra. If I is contained in the Jacobson radical of R and M is finitely generated, we prove that the I-adic completion of M is separated and complete. This important result is a corollary to the Krull Intersection Theorem, which itself is a corollary to the Artin-Rees Theorem. In Corollary 7.3.12, another highlight of this chapter, we prove that the I-adic completion of a commutative noetherian ring is noetherian.

Section 7.4 contains some important properties of a ring R that is separated and complete with respect to an I-adic topology. Most of the results in this section are motivated by the question of which properties of R/I lift to the same properties for R. For example, in Hensel's Lemma, we ask whether the factorization of a polynomial over R/I implies the existence of a corresponding factorization over R.

1. I-adic Topology and Completion

This section contains the basic definitions for the completion of an R-module with respect to a filtration. We study the first properties of the functor which maps an R-module M to its completion M^* with respect to a filtration. The topological completion is shown to be equal to an inverse limit. For most of the results of this section, the ground ring R is a general ring.

1.1. Completion of a Linear Topological Module. Let R be a ring and M an R-module. A *filtration* of M is a nonincreasing chain of submodules

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq M_3 \cdots.$$

Using the set of submodules $\{M_n\}_{n\geq 0}$ in a filtration, we define a topology on M. Given any $x \in M$, a base for the neighborhoods of x is the set $\{x + M_n \mid n \geq 0\}$. The *linear topology* on M defined by the filtration $\{M_n\}_{n\geq 0}$ is the smallest topology on M containing all of the open sets $\{x+M_n \mid x\in M, n\geq 0\}$. If L is a submodule of M and $\eta : M \to M/L$ is the natural map, then the chain $\{\eta(M_n)\}_{n\geq 0} = \{(M_n+L)/L\}_{n\geq 0}$ is a filtration of M/L that induces a linear topology on M/L. The chain of submodules $\{M_n\cap L\}_{n\geq 0}$ is a filtration of L which induces a linear topology on L. As in Section 1.3, we say that M is *separated* (that is, *Hausdorff*) if for any two distinct points $x,y\in M$, there are neighborhoods $x\in U$ and $y\in V$ such that $U\cap V=\emptyset$. If I is a two-sided ideal in R, the chain of ideals $R\supseteq I^1\supseteq I^2\supseteq I^3\supseteq\dots$ is a filtration of R which defines the *I-adic topology on R*. This agrees with the terminology of Definition 2.7.20. The chain of submodules $M\supseteq I^1M\supseteq I^2M\supseteq I^3M\supseteq\dots$ is a filtration of M which defines the *I-adic topology on M*.

LEMMA 7.1.1. *Let R be a ring, M an R-module with a filtration $\{M_n\}_{n\geq 0}$, and L a submodule. With respect to the linear topology defined by this filtration, the following are true.*

(1) *Each set M_n is open and closed.*
(2) *Addition on M is continuous.*
(3) *The natural maps $0\to L \xrightarrow{\subseteq} M \xrightarrow{\eta} M/L \to 0$ are continuous.*
(4) *For each n, M/M_n has the discrete topology, which is to say "points are open".*

PROOF. (1): By definition, each left coset $(x+M_n)$ is open. The decomposition of M into left cosets gives $M-M_n=\bigcup_{x\notin M_n}(x+M_n)$, which is open.

(2): Follows from the formula for addition of left cosets $(x+y)+M_n=(x+M_n)+(y+M_n)$.

(3): Is left to the reader.

(4): M/M_n has the finite filtration $M/M_n\supseteq M_1/M_n\supseteq\cdots\supseteq M_{n-1}/M_n\supseteq M_n/M_n=0$ which terminates with (0). $\square$

LEMMA 7.1.2. *Let $\{M_n\}_{n\geq 0}$ be a filtration of the R-module M. Let $N=\bigcap_{n\geq 0}M_n$. Then*

(1) *N is the closure of $\{0\}$.*
(2) *M is separated if and only if $N=0$.*
(3) *If L is a submodule of M, then M/L is separated if and only if L is closed.*

PROOF. (1): An element x is in the closure of $\{0\}$ if and only if every neighborhood of x contains 0. Since $\{x+M_n\}_{n\geq 0}$ is a base for the neighborhoods of x, it follows that x is in the closure of $\{0\}$ if and only if $x\in N$.

(2): If $x\in N$ and $x\neq 0$, then every neighborhood of x contains 0 so M is not separated. If $x,y\in M$ and $x-y\notin N$, then for some $n\geq 0$, $x-y\notin M_n$. Then $(x+M_n)\cap(y+M_n)=\emptyset$. This says that M/N is separated, so if $N=0$, then M is separated.

(3): Is left to the reader. $\square$

DEFINITION 7.1.3. Let $\{M_n\}_{n\geq 0}$ be a filtration of the R-module M. A sequence (x_ν) of elements of M is a *Cauchy sequence* if for every open submodule U there exists $n_0\geq 0$ such that $x_\mu - x_\nu\in U$ for all $\mu\geq n_0$ and all $\nu\geq n_0$. Since U is a submodule, this is equivalent to $x_{\nu+1}-x_\nu\in U$ for all $\nu\geq n_0$. A point x is a *limit* of a sequence (x_ν) if for every open submodule U there exists $n_0\geq 0$ such that $x-x_\nu\in U$ for all $\nu\geq n_0$. We say M is *complete* if every Cauchy sequence has a limit. We say that two Cauchy sequences (x_ν) and (y_ν) are *equivalent* and write $(x_\nu)\sim(y_\nu)$ if 0 is a limit of $(x_\nu-y_\nu)$.

LEMMA 7.1.4. *In the setting of Definition 7.1.3, let C denote the set of all Cauchy sequences in M.*

(1) *The relation $\sim$ is an equivalence relation on C.*
(2) *If $(x_\nu) \in C$ and $(y_\nu) \in C$, then $(x_\nu + y_\nu) \in C$.*
(3) *If $(x_\nu) \sim (x'_\nu) \in C$ and $(y_\nu) \sim y'_\nu) \in C$, then $(x_\nu + y_\nu) \sim (x'_\nu + y'_\nu) \in C$.*
(4) *If $(x_\nu) \in C$ and $r \in R$, then $(rx_\nu) \in C$.*
(5) *If $(x_\nu) \sim (x'_\nu) \in C$ and $r \in R$, then $(rx_\nu) \sim (rx'_\nu) \in C$.*

PROOF. Is left to the reader. □

DEFINITION 7.1.5. Let $\{M_n\}_{n\geq 0}$ be a filtration of the R-module M. Let M^* denote the set of all equivalence classes of Cauchy sequences in M. We call M^* the *topological completion* of M. Then Lemma 7.1.4 says that M^* is an R-module. For any $x \in M$, the constant sequence (x) is a Cauchy sequence, so $x \mapsto (x)$ defines an R-module homomorphism $\eta : M \to M^*$. The reader should verify that the kernel of η is the subgroup N of Lemma 7.1.2. Therefore η is one-to-one if and only if M is separated. A Cauchy sequence is in the image of η if it has a limit in M, hence M is complete if the natural map $\eta : M \to M^*$ is onto. For M to be separated and complete it is necessary and sufficient that η be an isomorphism, which is true if and only if every Cauchy sequence has a unique limit in M.

LEMMA 7.1.6. *In the setting of Definition 7.1.3, assume L is a submodule of M. If M is complete, then M/L is complete.*

PROOF. Let $(x_\nu + L)$ be a Cauchy sequence in M/L. For each ν there is a positive integer $i(\nu)$ such that $x_{\nu+1} - x_\nu \in M_{i(\nu)} + L$ for all $\nu \geq i(\nu)$. For each ν pick $y_\nu \in M_{i(\nu)}$ and $z_\nu \in L$ such that $x_{\nu+1} - x_\nu = y_\nu + z_\nu$. Define a sequence $s = (x_1, x_1 + y_1, x_1 + y_1 + y_2, x_1 + y_1 + y_2 + y_3, \dots)$ in M. Since 0 is a limit for (y_ν), it follows that s is a Cauchy sequence in M. Since M is complete, s has a limit, say s_0. Notice that $s_{\nu+1} - x_{\nu+1} \in L$. Therefore, $s_0 + L$ is a limit for $(x_\nu + L)$ in M/L. □

1.2. Functorial Properties of Completion.

PROPOSITION 7.1.7. *Let $\{M_n\}_{n\geq 0}$ be a filtration of the R-module M and M^* the topological completion. Then M^* is isomorphic to $\varprojlim M/M_n$ as R-modules.*

PROOF. For any n the natural map $\eta_n : M \to M/M_n$ is continuous and maps a Cauchy sequence (x_ν) in M to a Cauchy sequence $(\eta_n(x_\nu))$ in M/M_n. As M/M_n has the discrete topology, $(\eta_n(x_\nu))$ is eventually constant, hence has a limit. Two equivalent Cauchy sequences will have the same limit in M/M_n, so there is a well defined continuous R-module homomorphism $f_n : M^* \to M/M_n$ defined by $(x_\nu) \mapsto \varinjlim(\eta_n(x_\nu))$. According to Definition 2.7.12, there is a unique R-module homomorphism $\beta : M^* \to \varprojlim M/M_n$. A Cauchy sequence is in the kernel of β if and only if it is equivalent to 0. Therefore, β is one-to-one. By Proposition 2.7.13, we can view the inverse limit as a submodule of the direct product. If the inverse limit is given the topology it inherits from the direct product of the discrete spaces $\prod M/M_n$, then β is continuous. An element of the inverse limit can be viewed as $(x_n) \in \prod M/M_n$ such that $x_n = \phi_{n+1}(x_{n+1})$ for all n, where $\phi_{n+1} : M/M_{n+1} \to M/M_n$ is the natural map. In this case, $x_{n+1} - x_n \in M_n$ so (x_n) is the image under η of a Cauchy sequence in M. This shows β is onto, and therefore β is an isomorphism. □

Suppose that $\{A_n\}$ is a filtration for the R-module A, and that $\{B_n\}$ is a filtration for B. A *morphism* from $\{A_n\}$ to $\{B_n\}$ is an R-module homomorphism $\alpha : A \to B$ such that for each $n \geq 0$, $\alpha(A_n) \subseteq B_n$. In this case α induces a commutative square

$$\begin{tikzcd} A/A_{n+1} \arrow[r, "\alpha"] \arrow[d, "\phi_{n+1}"'] & B/B_{n+1} \arrow[d, "\psi_{n+1}"] \\ A/A_n \arrow[r, "\alpha"] & B/B_n \end{tikzcd}$$

for each $n \geq 0$. Hence there is a morphism of inverse systems $\alpha : \{A/A_n\} \to \{B/B_n\}$. As in Section 2.7, α induces a homomorphism $\varprojlim A/A_n \to \varprojlim B/B_n$.

PROPOSITION 7.1.8. *If*

$$\{A_n\} \xrightarrow{\alpha} \{B_n\} \xrightarrow{\beta} \{C_n\}$$

is a sequence of morphisms of R-modules equipped with filtrations, such that for every $n \geq 0$ the sequence

$$0 \to A_n \xrightarrow{\alpha} B_n \xrightarrow{\beta} C_n \to 0$$

is an exact sequence of R-modules. Then

$$0 \to \varprojlim A/A_n \xrightarrow{\overleftarrow{\alpha}} \varprojlim B/B_n \xrightarrow{\overleftarrow{\beta}} \varprojlim C/C_n \to 0$$

is an exact sequence of R-modules.

PROOF. It follows from Theorem 2.5.2 that the sequence

$$0 \to A/A_n \xrightarrow{\alpha} B/B_n \xrightarrow{\beta} C/C_n \to 0$$

is an exact sequence of R-modules for each $n \geq 0$. Apply Proposition 2.7.19 to the exact sequence of morphisms of inverse systems $\{A/A_n\} \xrightarrow{\alpha} \{A/B_n\} \xrightarrow{\beta} \{C/C_n\}$. □

COROLLARY 7.1.9. *Let $\{B_n\}$ be a filtration for the R-module B. Suppose*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is an exact sequence of R-modules. Give A the filtration $\{A_n\} = \{\alpha^{-1}(B_n)\}$ and C the filtration $\{C_n\} = \{\beta(B_n)\}$. Then the sequence of completions

$$0 \to A^* \xrightarrow{\alpha^*} B^* \xrightarrow{\beta^*} C^* \to 0$$

is an exact sequence of R-modules.

PROOF. By construction,

$$0 \to A/A_n \xrightarrow{\alpha} B/B_n \xrightarrow{\beta} C/C_n \to 0$$

is an exact sequence of R-modules. Now apply Proposition 7.1.8 and Proposition 7.1.7. □

COROLLARY 7.1.10. *Let $\{M_n\}$ be a filtration for the R-module M and M^* the topological completion.*

(1) For each $n \geq 0$ we have $M^*/M_n^* \cong M/M_n$.
(2) With respect to the filtration $\{M_n^*\}$, the R-module M^* is complete and separated. That is, $M^* \cong (M^*)^*$.

PROOF. (1): Apply Corollary 7.1.9 to the sequence $0 \to M_n \to M \to M/M_n \to 0$. Since M/M_n has the discrete topology, $M/M_n \cong (M/M_n)^*$.

(2): Take inverse limits in Part (1). □

PROPOSITION 7.1.11. *Let R be a ring and I a two-sided ideal in R such that R is separated and complete with respect to the I-adic topology. Then*

(1) *$1+x$ is a unit of R for every $x \in I$, and*
(2) *I is contained in $\mathrm{J}(R)$, the Jacobson radical of R.*

PROOF. By Nakayama's Lemma (Theorem 4.2.3), it is enough to prove that $1-x$ is invertible for every $x \in I$. Since the I-adic topology on R is separated, $\cap I^n = 0$. The sequence $s = (1, 1+x, 1+x+x^2, 1+x+x^2+x^3, \dots)$ is a Cauchy sequence in R. Since R is complete, s converges in R. Now $(1-x)s = s(1-x) = 1-(x,x^2,x^3,\dots)$ is equal to 1 since the Cauchy sequence $(x,x^2,x^3,\dots)$ converges to 0. $\square$

COROLLARY 7.1.12. *Let R be a commutative ring and $\mathfrak{m}$ a maximal ideal in R. If $\hat{R} = \varprojlim R/\mathfrak{m}^i$ is the $\mathfrak{m}$-adic completion, then $\hat{R}$ is a local ring with maximal ideal $\hat{\mathfrak{m}} = \varprojlim \mathfrak{m}/\mathfrak{m}^i$.*

PROOF. By Corollary 7.1.10 (1), $\hat{R}/\hat{\mathfrak{m}} \cong R/\mathfrak{m}$, so $\hat{\mathfrak{m}}$ is a maximal ideal of $\hat{R}$. By Corollary 7.1.10 (2), $\hat{R}$ is separated and complete with respect to the topology associated to the filtration $(\mathfrak{m}^i)\widehat{\ }$. By Lemma 2.7.18, we can view $\hat{\mathfrak{m}}$ as the set of all sequences $(x_1,x_2,\dots) \in \prod_{i=1}^{\infty} R/\mathfrak{m}^i$ such that $x_1 \in \mathfrak{m}$ and $x_i - x_{i+1} \in \mathfrak{m}^i$ for all $i \geq 1$. From this we see that $\hat{\mathfrak{m}}^i \subseteq (\mathfrak{m}^i)\widehat{\ }$. The proof of Proposition 7.1.11 shows that $\hat{\mathfrak{m}}$ is contained in the Jacobson radical of $\hat{R}$. Hence, $\hat{R}$ has a unique maximal ideal and is a local ring. $\square$

1.3. Exercises.

EXERCISE 7.1.1. Let R be a commutative ring, I an ideal in R, and

$$A \xrightarrow{\alpha} B \to 0$$

an exact sequence of R-modules. Prove that the I-adic filtration $\{I^n B\}_{n\geq 0}$ of B is equal to the filtration $\{\alpha(I^n A)\}_{n\geq 0}$ of B inherited from A by the surjection α.

EXERCISE 7.1.2. Let R be a commutative ring and I an ideal in R. Prove:

(1) The I-adic completion of $M = R \oplus R$ is isomorphic to $\hat{R} \oplus \hat{R}$. (Hint: Corollary 7.1.9.)
(2) If M is a finitely generated free R-module, then the I-adic completion of M is a finitely generated free $\hat{R}$-module.

EXERCISE 7.1.3. Let R be a commutative ring and I a nilpotent ideal in R ($I^N = (0)$, for some $N \geq 1$).

(1) Show that $\varprojlim R/I^i = R$.
(2) If R is a commutative local artinian ring with maximal ideal $\mathfrak{m}$, show that R is separated and complete with respect to the $\mathfrak{m}$-adic topology.

EXERCISE 7.1.4. Let R be a commutative ring and I an ideal in R. Let J be another ideal of R such that $I \subseteq J$. Prove:

(1) In the I-adic topology on R, J is both open and closed.
(2) If $\hat{J} = \varprojlim J/I^n$ and $\hat{R} = \varprojlim R/I^n$, then $\hat{R}/\hat{J} = R/J$.
(3) J is a prime ideal if and only if $\hat{J}$ is a prime ideal.

EXERCISE 7.1.5. Let R be a commutative ring. Let I and J be ideals of R. Prove:

(1) The I-adic topology on R is equal to the J-adic topology on R if and only if there exists $m > 0$ such that $I^m \subseteq J$ and $J^m \subseteq I$.

(2) If the I-adic topology on R is equal to the J-adic topology on R, then there is an isomorphism of rings $\varprojlim R/I^k \to \varprojlim R/J^k$. (Hint: Exercise 2.7.20.)

For a continuation of this exercise, see Exercise 9.1.7.

2. Graded Rings and Graded Modules

In this section all rings are commutative.

2.1. Definitions and First Principles. A *graded ring* is a commutative ring R which under addition is the internal direct sum $R = \bigoplus_{n=0}^{\infty} R_n$ of a set of additive subgroups $\{R_n\}_{n\geq 0}$ satisfying the property that $R_iR_j \subseteq R_{i+j}$ for all $i,j \geq 0$. The reader should verify (Exercise 7.2.1) that R_0 is a subring of R and each R_n is an R_0-module. An element of R_n is said to be *homogeneous of degree n*. The set $R_+ = \bigoplus_{n=1}^{\infty} R_n$ is an ideal of R (Exercise 7.2.2), and is called the *exceptional ideal* of R.

EXAMPLE 7.2.1. Let R be any commutative ring and $S = R[x_1,\dots,x_m]$ the polynomial ring over R in m variables $x_1,\dots,x_m$. A *monomial* over R is any polynomial that looks like $rx_1^{e_1}\cdots x_m^{e_m}$, where $r \in R$ and each exponent e_i is a nonnegative integer. The *degree* of a monomial is $-\infty$ if $r = 0$, otherwise it is the sum of the exponents $e_1 + \cdots + e_m$. A polynomial in S is said to be *homogeneous* if it is a sum of monomials all of the same degree. Let $S_0 = R$ be the set of all polynomials in S of degree less than or equal to 0. For all $n \geq 1$, let S_n be the set of all homogeneous polynomials in S of degree n. The reader should verify that S is a graded ring.

Let R be a graded ring. A *graded R-module* is an R-module M which under addition is the internal direct sum $M = \bigoplus_{n\in\mathbb{Z}} M_n$ of a set of additive subgroups $\{M_n\}_{n\in\mathbb{Z}}$ and such that $R_iM_j \subseteq M_{i+j}$ for all pairs i,j. The reader should verify that each M_n is an R_0-module (Exercise 7.2.3). Any $x \in M_n$ is said to be *homogeneous* of degree n. Every $y \in M$ can be written uniquely as a finite sum $y = \sum_{n=-d}^{d} y_n$ where $y_n \in M_n$. We call the elements $y_{-d},\dots,y_0,\dots,y_d$ the homogeneous components of y. The set of *homogeneous elements* of M is

$$M^h = \bigcup_{d\in\mathbb{Z}} M_d.$$

Let M and N be graded R-modules and $\theta : M \to N$ an R-module homomorphism. We say θ is a *homomorphism of graded R-modules* if for every $n \in \mathbb{Z}$ we have $\theta(M_n) \subseteq N_n$.

PROPOSITION 7.2.2. *Let R be a graded ring. The following are equivalent.*

(1) R is a noetherian ring.

(2) R_0 is a noetherian ring and R is a finitely generated R_0-algebra.

PROOF. (2) implies (1): This follows straight from Theorem 6.2.1 (3).

(1) implies (2): By Corollary 4.1.13 (1), $R_0 = R/R_+$ is noetherian. By Corollary 4.1.7, the ideal R_+ is finitely generated. Write $R_+ = Rx_1 + \cdots + Rx_m$. Assume without loss of generality that each x_i is homogeneous of degree $d_i > 0$. Let S be the R_0-subalgebra of R generated by $x_1,\dots,x_m$. Inductively assume $n > 0$ and that S contains $R_0 + R_1 + \cdots + R_{n-1}$. We show that S contains R_n, which will finish the proof. Let $y \in R_n$. Write $y = r_1x_1 + \cdots + r_mx_m$. Each r_i can be written as a sum of its homogeneous components. Because y is homogeneous and each x_i is homogeneous, after rearranging and re-labeling, we can assume each r_i is either zero or homogeneous of degree e_i where $e_i + d_i = n$. Because $d_i > 0$, we have $0 \leq e_i < n$, which says each r_i is in $R_0 + R_1 + \cdots + R_{n-1}$. By the inductive hypothesis, each r_i is in S which says $y \in S$. $\square$

2.2. The Grading Associated to a Filtration.

EXAMPLE 7.2.3. Let R be a commutative ring. Suppose we have a filtration $J = \{J_n\}_{n\geq 0}$ of R by ideals

$$R = J_0 \supseteq J_1 \supseteq J_2 \supseteq \dots$$

such that for all $m,n \geq 0$ we have $J_m J_n \subseteq J_{m+n}$. Multiplication in R defines an R-module homomorphism

$$\mu_0 : J_m \otimes_R J_n \to \frac{J_{m+n}}{J_{m+n+1}}$$

where $\mu_0(x\otimes y) = xy \pmod{J_{m+n+1}}$. The kernel of μ_0 contains the image of $J_{m+1} \otimes_R J_n$, so μ_0 factors through

$$\mu_1 : \frac{J_m}{J_{m+1}} \otimes_R J_n \to \frac{J_{m+n}}{J_{m+n+1}}.$$

The kernel of μ_1 contains the image of $\frac{J_m}{J_{m+1}} \otimes_R J_{n+1}$, so μ_1 factors through

$$\mu_{mn} : \frac{J_m}{J_{m+1}} \otimes_R \frac{J_n}{J_{n+1}} \to \frac{J_{m+n}}{J_{m+n+1}}.$$

The graded ring associated to this filtration is

$$\operatorname{gr}_J(R) = \bigoplus_{n=0}^{\infty} \frac{J_n}{J_{n+1}} = \frac{R}{J_1} \oplus \frac{J_1}{J_2} \oplus \cdots \oplus \frac{J_n}{J_{n+1}} \oplus \dots$$

where multiplication of two homogeneous elements x_m, x_n is defined to be $\mu_{mn}(x_m \otimes x_n)$. The reader should verify that $\operatorname{gr}_J(R)$ is a graded ring. When I is an ideal of R, the I-adic filtration

$$R = I^0 \supseteq I^1 \supseteq I^2 \supseteq \dots$$

has the associated graded ring $\operatorname{gr}_I(R) = \bigoplus_{n\geq 0} I^n/I^{n+1}$. The reader should verify that $\operatorname{gr}_I(R)$ is an R/I-algebra which is generated by the set of homogeneous elements of degree one, $\operatorname{gr}_I(R)_1 = I/I^2$.

EXAMPLE 7.2.4. Let R be an integral domain. Let g be an element of R such that g is nonzero and g is not invertible. Then there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & Rg \arrow[r] \arrow[d] & R \arrow[r] \arrow[d] & R/Rg \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Rg^{i+1} \arrow[r] & Rg^i \arrow[r] & Rg^i/Rg^{i+1} \arrow[r] & 0
\end{tikzcd}$$

of R-modules where the vertical maps are "multiply by g^i". If we set $I = Rg$, then I^i/I^{i+1} is a free R/I-module of rank 1 and is generated by the coset $g^i + I^{i+1}$. The R/I-algebra homomorphism $\delta : (R/I)[x] \to \operatorname{gr}_I(R) = \bigoplus_{i\geq 0} I^i/I^{i+1}$ defined by $x \mapsto g + I/I^2$ is an isomorphism of graded rings.

EXAMPLE 7.2.5. Let R be a commutative ring and I an ideal of R. Let M be an R module and $F = \{M_n\}_{n\geq 0}$ an I-filtration of M. Set $\operatorname{gr}_F(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$. Using the method of Example 7.2.3, the reader should verify that $\operatorname{gr}_F(M)$ is a graded $\operatorname{gr}_I(R)$-module. We call this the *associated graded module* for the I-filtration F of M. The graded $\operatorname{gr}_I(R)$-module associated to the I-adic filtration $\{I^n M\}_{n\geq 0}$ is denoted $\operatorname{gr}_I(M)$.

DEFINITION 7.2.6. Let R be a commutative ring and $J = \{J_n\}_{n\geq 0}$ a filtration of R by ideals. Let M be an R-module which also has a filtration $\{M_n\}_{n\geq 0}$. We say that M is a *filtered* R-module, or that the filtrations of R and M are *compatible*, if $J_i M_j \subseteq M_{i+j}$, for all $i \geq 0$ and $j \geq 0$. If the filtration of R is defined by an ideal I, then M is a filtered R-module if $IM_n \subseteq M_{n+1}$ for all $n \geq 0$. In this case, we also say the filtration $\{M_n\}_{n\geq 0}$ is an *I-filtration*. If $IM_n = M_{n+1}$ for all sufficiently large n, then we say the filtration is a *stable I-filtration*.

EXAMPLE 7.2.7. Let R be a commutative ring and $J = \{J_n\}_{n\geq 0}$ a filtration of R by ideals. Let M be an R-module. The filtration of M *inherited* from R is defined by $M_n = J_n M$. The filtration $\{M_n\}_{n\geq 0}$ makes M into a *filtered* R-module.

EXAMPLE 7.2.8. Let R be a commutative ring, and I an ideal in R. The I-adic filtration of R and the I-adic filtration $\{I^n M\}$ of M are compatible. Moreover, $\{I^n M\}$ is a stable I-filtration of M.

According to Proposition 7.1.7, the completion depends only on the topology, not necessarily the filtration. In other words, different filtrations may give rise to the same topology, and therefore the same completions.

PROPOSITION 7.2.9. *Let R be a noetherian commutative ring and I an ideal of R. The following are true.*

(1) The associated graded ring $\operatorname{gr}_I(R) = \bigoplus_{n\geq 0} I^n/I^{n+1}$ is noetherian.
(2) Let M be a finitely generated R module and $F = \{M_n\}_{n\geq 0}$ a stable I-filtration of M. Then $\operatorname{gr}_F(M) = \bigoplus_{n\geq 0} M_n/M_{n+1}$ is a finitely generated graded $\operatorname{gr}_I(R)$-module.

PROOF. (1): Since R is noetherian, by Corollary 4.1.13, R/I is noetherian. By Corollary 4.1.7, I is finitely generated. Therefore $\operatorname{gr}_I(R)$ is a finitely generated R/I-algebra and by Proposition 7.2.2, $\operatorname{gr}_I(R)$ is noetherian.

(2): Since M is a finitely generated R-module and R is noetherian, Corollary 4.1.12 implies each M_n is finitely generated over R. Each M_n/M_{n+1} is finitely generated over R and annihilated by I, so M_n/M_{n+1} is finitely generated over R/I. For any $d > 0$, $M_0/M_1 \oplus \cdots \oplus M_d/M_{d+1}$ is finitely generated over R/I.

For some $d > 0$ we have $IM_{d+r} = M_{d+r+1}$, for all $r \geq 0$. By induction, $I^r M_d = M_{d+r}$, for all $r \geq 1$. It follows that

$$\left(I^r/I^{r+1}\right)(M_d/M_{d+1}) = M_{d+r}/M_{d+r+1}$$

which shows that $\operatorname{gr}_F(M)$ is generated as a graded $\operatorname{gr}_I(R)$-module by the set $M_0/M_1 \oplus \cdots \oplus M_d/M_{d+1}$. A finite set of generators for $M_0/M_1 \oplus \cdots \oplus M_d/M_{d+1}$ over R/I will also generate $\operatorname{gr}_F(M)$ as a graded $\operatorname{gr}_I(R)$-module. □

2.3. The Artin-Rees Theorem.

LEMMA 7.2.10. *Let R be a commutative ring and I an ideal of R. If $\{M_n\}$ and $\{M'_n\}$ are stable I-filtrations of the R-module M, then there exists an integer n_0 such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \geq 0$. All stable I-filtrations of M give rise to the same topology on M, namely the I-adic topology.*

PROOF. It is enough to show this for $\{M'_n\} = \{I^n M\}$. For some n_0 we have $IM_n = M_{n+1}$ for all $n \geq n_0$. Then $IM_{n_0} = M_{n_0+1}$, $I^2 M_{n_0} = IM_{n_0+1} = M_{n_0+2}$, and iterating n times, $I^n M_{n_0} = IM_{n_0+n-1} = M_{n_0+n}$. Therefore $I^n M \supseteq I^n M_{n_0} = M_{n+n_0}$. For the reverse direction, start with $IM = IM_0 \subseteq M_1$. We get $I^2 M \subseteq M_2$, and iterating n times we get $I^n M \subseteq M_n$. Therefore $I^{n+n_0} \subseteq I^n M \subseteq M_n$ for all $n \geq 0$. □

EXAMPLE 7.2.11. Let R be a commutative ring and I an ideal of R. Then $S = R \oplus I \oplus I^2 \oplus I^3 \oplus \dots$ is a graded ring. If R is noetherian, then I is finitely generated so S is a finitely generated R-algebra and is noetherian by Proposition 7.2.2. Let M be an R module and $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$ an I-filtration of M (Definition 7.2.6). For each $i \geq 0$ we have $IM_i \subseteq M_{i+1}$, hence $I^j M_i \subseteq M_{i+j}$. Therefore $T = M_0 \oplus M_1 \oplus M_2 \oplus M_3 \oplus \dots$ is a graded S-module.

LEMMA 7.2.12. *Let R be a commutative ring and I an ideal of R. Let M be an R module and*

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$$

an I-filtration of M such that for each i, M_i is a finitely generated R-module. The following are equivalent.

(1) *The I-filtration $\{M_n\}_{n\geq 0}$ is stable. That is, there exists $d > 0$ such that $IM_n = M_{n+1}$ for all $n \geq d$.*
(2) *If $S = R \oplus I \oplus I^2 \oplus I^3 \oplus \cdots$ and $T = M_0 \oplus M_1 \oplus M_2 \oplus M_3 \oplus \cdots$, then T is a finitely generated S-module.*

PROOF. (2) implies (1): Assume T is finitely generated over S. Suppose U is a finite subset of T which generates T over S. By making U larger (but still finite), we may assume U consists of a finite set of homogeneous elements $U = \{x_1, \dots, x_m\}$ where x_i has degree d_i. Let d be the maximum of $\{d_1, \dots, d_m\}$. Assume $n \geq d$ and $y \in M_n$. Write $y = r_1 x_1 + \cdots + r_m x_m$. Each r_i can be written as a sum of its homogeneous components. Because y is homogeneous and each x_i is homogeneous, after rearranging and re-labeling, we may assume each r_i is either zero or homogeneous of degree e_i where $e_i + d_i = n$. For each i, $r_i \in I^{n-d_i}$. This shows that

$$M_n = \sum_{i=1}^{m} I^{n-d_i} M_{d_i}$$

for all $n \geq d$. It follows that

$$M_{n+1} = \sum_{i=1}^{m} I^{n-d_i+1} M_{d_i} = I\left(\sum_{i=1}^{m} I^{n-d_i} M_{d_i}\right) = IM_n.$$

(1) implies (2): If $M_{n+1} = IM_n$ for all $n \geq d$, then T is generated over S by the set

$$C = M_0 \oplus M_1 \oplus M_2 \oplus \cdots \oplus M_d.$$

A finite set of generators for C over R will also generate T over S. □

THEOREM 7.2.13. *(Artin-Rees) Let R be a noetherian commutative ring, I an ideal in R, M a finitely generated R-module, $\{M_n\}_{n\geq 0}$ a stable I-filtration of M, and N a submodule of M. Then*

(1) *$\{N \cap M_n\}_{n\geq 0}$ is a stable I-filtration of N.*
(2) *There exists an integer $d > 0$ such that*

$$I^n M \cap N = I^{n-d}(I^d M \cap N)$$

for all $n > d$.

PROOF. (1): Let $S = \bigoplus_{n\geq 0} I^n$. Since R is noetherian, by Corollary 4.1.7, I is finitely generated. But S is generated as an R-algebra by I, so Proposition 7.2.2 implies S is noetherian. By Corollary 4.1.12, each M_n is finitely generated as an R-module. By Lemma 7.2.12, $T = \bigoplus_{n\geq 0} M_n$ is finitely generated as an S-module. For each $n \geq 0$ we have $I(N \cap M_n) \subseteq IN \cap IM_n \subseteq N \cap M_{n+1}$. Therefore $\{N \cap M_n\}_{n\geq 0}$ is an I-filtration of N and

$U = \bigoplus_{n\geq 0} N \cap M_n$ is an S-submodule of T. By Corollary 4.1.12, U is finitely generated over S. We are done by Lemma 7.2.12.

Part (2) follows from Part (1) because the filtration $\{I^n M\}_{n\geq 0}$ is a stable filtration of M. □

COROLLARY 7.2.14. *Let R be a noetherian commutative ring, I an ideal in R, M a finitely generated R-module, and N a submodule of M. Then there exists an integer n_0 such that $I^{n+n_0}N \subseteq (I^n M) \cap N$ and $(I^{n+n_0}M) \cap N \subseteq I^n N$ for all $n \geq 0$. The I-adic topology of N coincides with the topology induced on N by the I-adic topology of M.*

PROOF. The filtration $\{I^n N\}_{n\geq 0}$ is a stable filtration of N and by Theorem 7.2.13, $\{(I^n M) \cap N_{n\geq 0}\}$ is a stable I-filtration of N. The rest comes from Lemma 7.2.10. □

COROLLARY 7.2.15. *Let R be a noetherian commutative ring, I an ideal in R, and*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

an exact sequence of finitely generated R-modules. The sequence

$$0 \to \hat{A} \to \hat{B} \to \hat{C} \to 0$$

of I-adic completions is an exact sequence of $\hat{R}$-modules.

PROOF. First give B the I-adic filtration $\{I^n B\}_{n\geq 0}$. Give C the filtration $\{\beta(I^n B)\}_{n\geq 0}$, which is the same as the I-adic filtration on C, by Exercise 7.1.1. Give A the filtration $\{\alpha^{-1}(I^n B)\}_{n\geq 0}$. By Corollary 7.1.9, the sequence of completions

$$0 \to A^* \xrightarrow{\alpha^*} B^* \xrightarrow{\beta^*} C^* \to 0$$

is an exact sequence of R-modules. Because we started with I-filtrations, the homomorphisms are $\hat{R}$-linear. We already know that $B^* = \hat{B}$ and $C^* = \hat{C}$. By Corollary 7.2.14, $A^* = \hat{A}$, so we are done. □

2.4. Exercises.

EXERCISE 7.2.1. Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a graded ring. Show that R_0 is a subring of R and each R_n is an R_0-module.

EXERCISE 7.2.2. Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a graded ring. Show that the set $R_+ = \bigoplus_{n=1}^{\infty} R_n$ is an ideal of R.

EXERCISE 7.2.3. Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a graded ring and $M = \bigoplus_{n=0}^{\infty} M_n$ a graded R-module. Show that each M_n is an R_0-module.

3. The Completion of a Noetherian Ring

This section contains some important theorems on I-adic completions of commutative noetherian rings. If R is a commutative noetherian ring and I is an ideal in R, then in Corollary 7.3.4 we show that $\hat{R}$ is a flat R-algebra. In Corollary 7.3.12, we show that $\hat{R}$ is noetherian. The proof is an application of the Krull Intersection Theorem, which itself is a corollary to the Artin-Rees Theorem.

3.1. The Completion of a Noetherian Ring is Flat. Let R be a commutative ring, I an ideal in R, and M an R-module. Let $\hat{R}$ be the I-adic completion of R and $\hat{M}$ the I-adic completion of M. Then $\hat{R}$ is an R-algebra and $\hat{M}$ is a module over both $\hat{R}$ and R. The natural maps $R \to \hat{R}$, $M \to \hat{M}$ and the multiplication map induce the $\hat{R}$-module homomorphisms

$$\hat{R} \otimes_R M \to \hat{R} \otimes_R \hat{M} \to \hat{R} \otimes_{\hat{R}} \hat{M} \xrightarrow{\cong} \hat{M}.$$

Taking the composition gives the natural $\hat{R}$-module homomorphism $\hat{R} \otimes_R M \to \hat{M}$.

PROPOSITION 7.3.1. *Let R be a commutative ring, I an ideal in R, and M a finitely generated R-module. Let $\hat{R}$ be the I-adic completion of R and $\hat{M}$ the I-adic completion of M.*

(1) $\hat{R} \otimes_R M \to \hat{M}$ is onto.
(2) If M is finitely presented, then $\hat{R} \otimes_R M \cong \hat{M}$.
(3) If R is noetherian, then $\hat{R} \otimes_R M \cong \hat{M}$.

PROOF. (1): By hypothesis, M is finitely generated. By Lemma 1.6.11, M is the homomorphic image of a finitely generated free R-module F. There is an exact sequence

$$0 \to K \to F \to M \to 0$$

where K is the kernel. Apply the tensor functor $\hat{R} \otimes_R (\cdot)$ and the I-adic completion functor to this sequence to get the commutative diagram

$$\begin{tikzcd} & \hat{R} \otimes_R K \arrow[r] \arrow[d, "\alpha"] & \hat{R} \otimes_R F \arrow[r] \arrow[d, "\beta"] & \hat{R} \otimes_R M \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & \hat{K} \arrow[r] & \hat{F} \arrow[r] & \hat{M} \arrow[r] & 0 \end{tikzcd}$$

The top row is exact because tensoring is right exact. By Corollary 7.2.15, the bottom row is exact. By Exercise 7.1.2, $\hat{R} \otimes_R F \cong \hat{F}$, so β is an isomorphism. It follows from Theorem 2.5.2 that γ is onto. This proves (1).

(2): If M is finitely presented, then K is finitely generated and applying (1) to K we see that α is onto. It follows from Theorem 2.5.2 that γ is an isomorphism.

(3): Follows from (2) and Corollary 4.1.12. □

COROLLARY 7.3.2. *Let R be a commutative noetherian ring, I an ideal in R, and $\hat{R}$ the I-adic completion of R. The following are true.*

(1) $\hat{R} \otimes_R I \cong \hat{I} = \hat{R}I$.
(2) $\widehat{I^n} = (\hat{I})^n$.
(3) $\hat{R}$ is separated and complete for the $\hat{I}$-adic topology. $\hat{I}$ is contained in the Jacobson radical of $\hat{R}$.
(4) $I^n/I^{n+1} \cong \hat{I}^n/\hat{I}^{n+1}$ and the associated graded rings $\operatorname{gr}_I(R)$ and $\operatorname{gr}_{\hat{I}}(\hat{R})$ are isomorphic as graded rings.

PROOF. (1): Since R is noetherian, I is finitely generated. The diagram

$$\begin{tikzcd} 0 \arrow[r] & \hat{R} \otimes_R I \arrow[r, "a"] \arrow[d, "\alpha"] & \hat{R} \otimes_R R \arrow[d, "\beta"] \\ 0 \arrow[r] & \hat{I} \arrow[r, "b"] & \hat{R} \end{tikzcd}$$

commutes and by Proposition 7.3.1, α and β are isomorphisms. The image of $\beta \circ a$ is $\hat{R}I$.

(2): The diagram

$$\begin{tikzcd}
0 \arrow[r] & \hat{R} \otimes_R I^n \arrow[r, "a"] \arrow[d, "\alpha"'] & \hat{R} \otimes_R R \arrow[d, "\beta"'] \\
0 \arrow[r] & \widehat{I^n} \arrow[r, "b"] & \hat{R}
\end{tikzcd}$$

commutes and by Proposition 7.3.1, α and β are isomorphisms. The image of $\beta \circ a$ is $\hat{R}I^n = (\hat{R}I)^n$, which by Part (1) is $(\hat{I})^n$.

(3): The first claim follows from Corollary 7.1.10 and Part (2). The second statement follows from Proposition 7.1.11.

(4): By Corollary 7.1.10, for each $n \geq 0$, $R/I^n \cong \hat{R}/\widehat{I^n}$. Now use the exact sequence $0 \to I^n/I^{n+1} \to R/I^{n+1} \to R/I^n \to 0$ and Part (2). $\square$

COROLLARY 7.3.3. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and $\hat{R}$ the $\mathfrak{m}$-adic completion of R. Then $\hat{R}$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$.*

PROOF. This follows from Corollary 7.1.12. $\square$

COROLLARY 7.3.4. *Let R be a commutative noetherian ring and I an ideal in R. Then the I-adic completion $\hat{R}$ is a flat R-module.*

PROOF. Let $0 \to A \to B$ be an exact sequence of finitely generated R-modules. By Corollary 7.2.15, the sequence of completions $0 \to \hat{A} \to \hat{B}$ is exact. By Proposition 7.3.1, the sequence $0 \to \hat{R} \otimes_R A \to \hat{R} \otimes_R B$ is exact. It follows from Proposition 3.7.3 that $\hat{R}$ is flat as an R-module. $\square$

3.2. The Krull Intersection Theorem. When R is a commutative ring with ideal I, and M is an R-module, the Krull Intersection Theorem, in conjunction with Nakayama's Lemma, provide useful criteria for the I-adic topology on M to be separated.

THEOREM 7.3.5. *(Krull Intersection Theorem) Let R be a commutative noetherian ring, I an ideal in R, and M a finitely generated R-module. If $N = \bigcap_{n \geq 0} I^n M$, then $IN = N$.*

PROOF. By Theorem 7.2.13, there exists a positive integer d such that for all $n > d$, $I^n M \cap N = I^{n-d}(I^d M \cap N)$. Fix $n > d$. Then $I^{n-d}(I^d M \cap N) \subseteq IN$ and $N \subseteq I^n M$. Putting all of this together,

$$N \subseteq I^n M \cap N \subseteq I^{n-d}(I^d M \cap N) \subseteq IN \subseteq N,$$

so we are done. $\square$

COROLLARY 7.3.6. *The following are true for any commutative noetherian ring R with ideal I.*

(1) If I is contained in the Jacobson radical of R and M is a finitely generated R-module, then $\bigcap_{n \geq 0} I^n M = 0$. The I-adic topology of M is separated.

(2) If I is contained in the Jacobson radical of R, then $\bigcap_{n \geq 0} I^n = 0$. The I-adic topology of R is separated.

(3) If R is a noetherian integral domain and I is a proper ideal of R, then $\bigcap_{n \geq 0} I^n = 0$. The I-adic topology of R is separated.

PROOF. (1): By Theorem 7.3.5, if $N = \bigcap_{n \geq 0} I^n M$, then $IN = N$. By Nakayama's Lemma, Theorem 4.2.3, $N = 0$.

(2): Follows from (1) with $M = R$.

(3): By Theorem 7.3.5, if $N = \bigcap_{n \geq 0} I^n$, then $IN = N$. By Nakayama's Lemma, Lemma 2.2.1, $I + \operatorname{annih}_R(N) = R$. Since $I \neq R$ and $N \subseteq R$ and R is a domain we conclude that $\operatorname{annih}_R(N) = R$. That is, $N = 0$. $\square$

THEOREM 7.3.7. *Let R be a commutative noetherian ring and I an ideal in R. The following are equivalent.*

(1) *Every ideal J in R is closed in the I-adic topology.*
(2) *I is contained in $\mathrm{J}(R)$, the Jacobson radical of R.*
(3) *The I-adic completion of R, $\hat{R}$, is a faithfully flat R-algebra.*
(4) *If N is a finitely generated R-module, then the I-adic topology on N is separated.*
(5) *If N is a finitely generated R-module, then every submodule of N is closed in the I-adic topology on N.*

If R and I satisfy any of the equivalent conditions in Theorem 7.3.7, then we say R, I is a *Zariski pair*.

PROOF. (1) implies (2): Assume I is not contained in $\mathrm{J}(R)$. Let $\mathfrak{m}$ be a maximal ideal of R such that I is not a subset of $\mathfrak{m}$. Since $\mathfrak{m}$ is prime, $I^n \not\subseteq \mathfrak{m}$ for all $n \geq 1$, by Proposition 1.5.4. Then $I^n + \mathfrak{m} = R$ for all $n \geq 1$. By Lemma 7.1.2, $\mathfrak{m}$ is not closed.

(2) implies (3): By Corollary 7.3.4, $\hat{R}$ is flat. Let $\mathfrak{m}$ be a maximal ideal in R. By Exercise 7.1.4, $\hat{\mathfrak{m}} = \varprojlim \mathfrak{m}/I^i$ is a maximal ideal in $\hat{R}$. Since $\mathfrak{m}\hat{R} \subseteq \hat{\mathfrak{m}}$, it follows from Lemma 3.5.1 (4) that $\hat{R}$ is a faithfully flat R-algebra.

(3) implies (2): Let $\mathfrak{m}$ be a maximal ideal of R. By Lemma 3.5.5, there is a maximal ideal M in $\hat{R}$ such that $M \cap R = \mathfrak{m}$. By Corollary 7.3.2 (3), $I\hat{R} \subseteq M$. It follows that $I \subseteq I\hat{R} \cap R \subseteq M \cap R = \mathfrak{m}$. Therefore, $I \subseteq \mathrm{J}(R)$.

(2) implies (4): This is Corollary 7.3.6.

(4) implies (5): Apply Lemma 7.1.2.

(5) implies (1): Is trivial. □

3.3. Exercises.

EXERCISE 7.3.1. Let R be a commutative ring and $S = R[x_1, \dots, x_m]$ the polynomial ring over R in m variables $x_1, \dots, x_m$. Prove:

(1) If S_n is the set of homogeneous polynomials in S of degree n, then $S = S_0 \oplus S_1 \oplus S_2 \oplus \cdots$ is a graded ring and $S_0 = R$.
(2) As an R-algebra, S is generated by S_1.
(3) Let $I = S_+ = S_1 \oplus S_2 \oplus \cdots$ be the exceptional ideal of S. Then $I^n = S_n \oplus S_{n+1} \oplus S_{n+2} \oplus \cdots$

EXERCISE 7.3.2. Let k be a field and $A = k[x_1, \dots, x_m]$ the polynomial ring in m variables over k. As in Exercise 7.3.1, $A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$ is a graded k-algebra and $A_0 = k$. Also, if $I = A_+ = A_1 \oplus A_2 \oplus \cdots$ is the exceptional ideal of A, then $I^n = A_n \oplus A_{n+1} \oplus A_{n+2} \oplus \cdots$. Let $R = A_0 \oplus A_n \oplus A_{n+1} \oplus A_{n+2} \oplus \cdots$. Prove:

(1) R is a graded k-subalgebra of A.
(2) I^n is an ideal in A, and an ideal in R.
(3) Prove that I^n is equal to $R : A = \{\alpha \in A \mid \alpha A \subseteq R\}$, the conductor ideal from A to R (see Exercise 1.1.8).

EXERCISE 7.3.3. Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a graded ring.

(1) Show that $J_n = \bigoplus_{i=n}^{\infty} R_i$ is an ideal in R and $J = \{J_n\}_{n \geq 0}$ is a filtration of R by ideals.
(2) Give R the filtration $J = \{J_n\}_{n \geq 0}$ defined in (1). Show that the natural map from R to the associated graded ring $\mathrm{gr}_J(R)$ is an isomorphism.

(3) If $R^* = \varprojlim R/J_n$ is the completion of R and $P = \{\sum_{i=0}^{\infty} x_i \mid x_i \in R_i\}$, show that there is an R-module isomorphism $R^* \cong P$. (Hint: Use Proposition 7.1.7. An element of the inverse limit can be viewed as a sequence (s_n) such that $s_{n+1} - s_n$ is in R_n.)

EXERCISE 7.3.4. Let R be a commutative ring and $S = R[x_1, \dots, x_m]$ the polynomial ring over R in m variables $x_1, \dots, x_m$. Show that if $I = Sx_1 + \cdots + Sx_m$, then the I-adic completion of S is isomorphic to the power series ring $R[[x_1, \dots, x_m]]$

EXERCISE 7.3.5. Let R be a commutative ring and I an ideal in R. Show that if M is a finitely generated projective R-module, then the I-adic completion of M is a finitely generated projective $\hat{R}$-module.

EXERCISE 7.3.6. Let R be a noetherian ring, I an ideal in R, and $\{a_1, \dots, a_n\}$ a set of generators of I. Show that the I-adic completion of R is isomorphic to $R[[x_1, \dots, x_n]]/(x_1 - a_1, \dots, x_n - a_n)$.

3.4. The Completion of a Noetherian Ring is Noetherian. Let R be any ring. Let A and B be two R-modules, let $\{A_n\}$ be a filtration for A, and let $\{B_n\}$ be a filtration for B. As in Section 7.1.2, a morphism from $\{A_n\}$ to $\{B_n\}$ is an R-module homomorphism $\alpha : A \to B$ such that for each $n \ge 0$, $\alpha(A_n) \subseteq B_n$. For each $n \ge 0$ the diagram of R-modules

$$\begin{tikzcd}
0 \arrow[r] & A_n/A_{n+1} \arrow[r] \arrow[d, "\gamma_n"] & A/A_{n+1} \arrow[r, "\phi_{n+1}"] \arrow[d, "\beta_{n+1}"] & A/A_n \arrow[r] \arrow[d, "\beta_n"] & 0 \\
0 \arrow[r] & B_n/B_{n+1} \arrow[r] & B/B_{n+1} \arrow[r, "\psi_{n+1}"] & B/B_n \arrow[r] & 0
\end{tikzcd}$$

commutes and the rows are exact. The three vertical arrows are induced by α. By the universal mapping property of the inverse limit, α induces a homomorphism $\varprojlim A/A_n \to \varprojlim B/B_n$. By the isomorphism of Proposition 7.1.7, α induces a homomorphism on the completions, $\alpha^* : A^* \to B^*$. The maps $\{\gamma_n\}_{n\ge 0}$ define a graded homomorphism

$$\mathrm{gr}(\alpha) : \mathrm{gr}(A) \to \mathrm{gr}(B)$$

of graded R-modules. (Here the grading of R is trivial. Every element is homogeneous of degree zero.)

LEMMA 7.3.8. *In the above context, let $\alpha : \{A_n\} \to \{B_n\}$ be a morphism of R-modules equipped with filtrations. Let $\alpha^* : A^* \to B^*$ be the homomorphism of completions and $\mathrm{gr}(\alpha) : \mathrm{gr}(A) \to \mathrm{gr}(B)$ the graded homomorphism of graded R-modules. Then*

(1) if $\mathrm{gr}(\alpha)$ is one-to-one, then α^* is one-to-one, and
(2) if $\mathrm{gr}(\alpha)$ is onto, then α^* is onto.

PROOF. The Snake Lemma (Theorem 2.5.2) applied to the previous diagram gives an exact sequence

$$0 \to \ker\gamma_n \to \ker\beta_{n+1} \xrightarrow{\theta_{n+1}} \ker\beta_n \xrightarrow{\partial} \operatorname{coker}\gamma_n \to \operatorname{coker}\beta_{n+1} \xrightarrow{\rho_{n+1}} \operatorname{coker}\beta_n \to 0.$$

(1): Assume $\ker\gamma_n = 0$ for all $n \ge 0$. Since $\beta_0 = 0$, an inductive argument shows that $\ker\beta_n = 0$ for all $n \ge 0$. By Proposition 7.1.8, the homomorphism on the inverse limits is one-to-one.

(2): Assume $\operatorname{coker}\gamma_n = 0$ for all $n \ge 0$. It is immediate that $\theta_{n+1} : \ker\beta_{n+1} \to \ker\beta_n$ is onto for all $n \ge 0$. Since $\beta_0 = 0$, an inductive argument shows that $\operatorname{coker}\beta_n = 0$ for all

$n \geq 0$. Applying Proposition 2.7.19 to the sequence of morphisms of inverse systems of R-modules
$$\{\ker \beta_n, \theta_{n+1}\} \to \{A/A_n, \phi_{n+1}\} \to \{B/B_n, \psi_{n+1}\}$$
it follows that $\varprojlim A/A_n \to \varprojlim B/B_n$ is onto. Hence $\alpha^* : A^* \to B^*$ is onto. □

DEFINITION 7.3.9. Suppose $R = \bigoplus_{i\geq 0} R_i$ is a commutative graded ring and $M = \bigoplus_{i\in\mathbb{Z}} M_i$ is a graded R-module. Given any $\ell \in \mathbb{Z}$, define the *twisted* module $M(-\ell)$ to be equal to M as a $\mathbb{Z}$-module, but with the grading shifted by ℓ. That is, $M(-\ell) = \bigoplus_{d\in\mathbb{Z}} M(-\ell)_d$, where $M(-\ell)_d = M_{d-\ell}$. The reader should verify that $M(-\ell)$ is a graded R-module.

DEFINITION 7.3.10. Let R be a commutative ring that has a filtration by ideals, $J = \{J_n\}_{n\geq 0}$. Given any $\ell \geq 0$, define a filtration shifted by ℓ by:
$$J(-\ell)_n = \begin{cases} R & \text{if } n < \ell \\ J_{n-\ell} & \text{if } n \geq \ell. \end{cases}$$
Denote this new filtration by $J(-\ell)$. The reader should verify that $\operatorname{gr}_{J(-\ell)}(R)$ and the twisted module $\operatorname{gr}_J(R)(-\ell)$ defined in Definition 7.3.9 are isomorphic as graded $\operatorname{gr}_J(R)$-modules.

PROPOSITION 7.3.11. *Let R be a commutative ring with a filtration $J = \{J_n\}_{n\geq 0}$ by ideals under which R is complete. Let M be a filtered R-module with filtration $\{M_n\}_{n\geq 0}$ under which M is separated.*

(1) If the graded $\operatorname{gr}_J(R)$-module $\operatorname{gr}(M)$ is finitely generated, then the R-module M is finitely generated.
(2) If every graded $\operatorname{gr}_J(R)$-submodule of $\operatorname{gr}(M)$ is finitely generated, then the R-module M satisfies the ACC on submodules (in other words, M is noetherian).

PROOF. (1): Pick a finite generating set $u_1, \dots, u_m$ for $\operatorname{gr}(M)$ as a graded $\operatorname{gr}_J(R)$-module. After splitting each u_i into its homogeneous components we assume each u_i is homogeneous of degree d_i. For each i pick $v_i \in M_{d_i}$ such that u_i is the image of v_i under the map $M_{d_i} \to M_{d_i}/M_{1+d_i}$. By $R(-d_i)$ we denote the R-module R with the twisted filtration $J(-d_i)$. The R-module homomorphism $\phi_i : R \to M$ defined by $1 \mapsto v_i$ defines a morphism of filtrations $\{R(-d_i)_n\} \to \{M_n\}$. Let $F = R(-d_1) \oplus \cdots \oplus R(-d_m)$ be the free R-module with the filtration $\{F_n = \bigoplus_{i=1}^m R(-d_i)_n\}$. Let $\phi : F \to M$ be the sum $\phi_1 + \cdots + \phi_m$ where each ϕ_i is applied to component i of the direct sum. So ϕ is a morphism of filtered R-modules. There is a homomorphism $\operatorname{gr}(\phi) : \operatorname{gr}(F) \to \operatorname{gr}(M)$ of graded $\operatorname{gr}_J(R)$-modules. By construction, the image of $\operatorname{gr}(\phi)$ contains a generating set so it is onto. By Lemma 7.3.8, the map on completions $\hat{\phi} : \hat{F} \to \hat{M}$ is onto. The square
$$\begin{tikzcd} F \arrow[r, "\phi"] \arrow[d, "\alpha"'] & M \arrow[d, "\beta"] \\ \hat{F} \arrow[r, "\hat{\phi}"] & \hat{M} \end{tikzcd}$$
commutes and $\hat{\phi}$ is onto. Because M is separated, β is one-to-one. Because R is complete, so is each $R(-d_i)$. Therefore, α is onto. The reader should verify that ϕ is onto. This shows that M is generated as an R-module by $v_1, \dots, v_m$.

(2): By Lemma 4.1.6 it is enough to show that every submodule L of M is finitely generated. Give L the filtration $L_n = M_n \cap L$. Then this makes L into a filtered R-module and $\bigcap_{n\geq 0} L_n = 0$. Since $L_{n+1} = L_n \cap M_{n+1}$, the induced map $L_n/L_{n+1} \to M_n/M_{n+1}$ is one-to-one. The graded homomorphism $\operatorname{gr}(L) \to \operatorname{gr}(M)$ of graded $\operatorname{gr}_J(R)$-modules is also one-to-one. By hypothesis, $\operatorname{gr}(L)$ is finitely generated. By Part (1), L is finitely generated. $\square$

COROLLARY 7.3.12. *Let R be a commutative noetherian ring.*

(1) If I is an ideal of R, then the I-adic completion of R is noetherian.
(2) If $S = R[[x_1,\dots,x_m]]$ is the power series ring over R in m variables, then S is noetherian.

PROOF. (1): By Corollary 7.3.2 and Proposition 7.2.9, the associated graded rings $\operatorname{gr}_I(R)$ and $\operatorname{gr}_{\hat{I}}(\hat{R})$ are isomorphic to each other and are noetherian. So every ideal of $\operatorname{gr}_{\hat{I}}(\hat{R})$ is finitely generated. By Proposition 7.3.11, every ideal of $\hat{R}$ is finitely generated and by Corollary 4.1.7, $\hat{R}$ is noetherian.

(2): By The Hilbert Basis Theorem (Theorem 6.2.1) $A = R[x_1,\dots,x_m]$ is noetherian. By Exercise 7.3.4, S is the completion of A for the I-adic topology, where $I = Ax_1 + \cdots + Ax_m$. $\square$

COROLLARY 7.3.13. *Let R be a commutative ring with a filtration by ideals $\{J_n\}_{n\geq 0}$. Let M be a filtered R-module with filtration $\{M_n\}_{n\geq 0}$. Assume that R is complete and that M is separated. Let F be a finitely generated submodule of M. If $M_k = M_{k+1} + J_kF$ for all $k \geq 0$, then $F = M$.*

PROOF. Let $\{x_1,\dots,x_m\}$ be a generating set for the R-module F, which we view as a subset of $M = M_0$. Let ξ_i be the image of x_i in M/M_1. Let F_1 be the kernel of $F \to M/M_1$. For all $k \geq 0$, $J_kF \subseteq M_k$. By hypothesis, the natural map $\eta_k : J_kF \to M_k/M_{k+1}$ is onto. Since $J_kF_1 + J_{k+1}F \subseteq M_{k+1}$, $(J_k/J_{k+1})(F/F_1) \to M_k/M_{k+1}$ is onto. Therefore, the graded $\operatorname{gr}_J(R)$-module $\operatorname{gr}(M)$ is generated by the finite set $\{\xi_1,\dots,\xi_m\}$. By Proposition 7.3.11, M is generated by $\{x_1,\dots,x_m\}$. $\square$

COROLLARY 7.3.14. *Let R, I be a Zariski pair (Theorem 7.3.7). Let $\mathfrak{a}$ be an ideal in R. If $\mathfrak{a}\hat{R}$ is a principal ideal, then $\mathfrak{a}$ is a principal ideal.*

PROOF. Assume $\mathfrak{a}\hat{R} = \alpha\hat{R}$, for some $\alpha \in \hat{R}$. By Corollary 7.3.12, $\hat{R}$ is noetherian. By Corollary 7.2.14 there exists $n_0 \geq 1$ such that $\alpha\hat{R} \cap \hat{I}^{n_0} \subseteq \hat{I}\alpha\hat{R}$. Write $\alpha = \sum_{i=1}^m a_i\beta_i$, for some $a_i \in \mathfrak{a}$ and $\beta_i \in \hat{R}$. By Corollary 7.1.10 there exist elements b_i in R such that $b_i - \beta_i \in \hat{I}^{n_0}$ for each i. Set $a = \sum_i a_ib_i$. Then $a \in \mathfrak{a} \subseteq \alpha\hat{R}$. Also, $a - \alpha = \sum_i a_i(b_i - \beta_i) \in \hat{I}^{n_0}$ is in $\hat{I}^{n_0} \cap \alpha\hat{R} \subseteq \hat{I}\alpha\hat{R}$. Therefore, $\alpha\hat{R} \subseteq a\hat{R} + \hat{I}\alpha\hat{R}$. By Corollary 7.3.2, $\hat{I} \subseteq \mathrm{J}(\hat{R})$. By Nakayama's Lemma (Corollary 2.2.5), $\alpha\hat{R} = a\hat{R}$. Using Lemma 3.5.4, we get $\mathfrak{a} = \mathfrak{a}\hat{R} \cap R = \alpha\hat{R} \cap R = a\hat{R} \cap R = aR$. $\square$

3.5. Exercises.

EXERCISE 7.3.7. Let $R = \bigoplus_{i\geq 0} R_0$ be a commutative graded ring and $M = \bigoplus_{i\geq 0} M_0$ a graded R-module. Prove that $M(-\ell)$ is a graded R-module, for any $\ell \geq 0$.

EXERCISE 7.3.8. Let R be a commutative ring with ideal I. Given any $\ell \geq 0$ prove that the twisted filtration $\{R(-\ell)_n\}_{n\geq 0}$ is a stable I-filtration of the R-module $R(-\ell)$.

EXERCISE 7.3.9. In Exercise 7.3.8, show that the graded $\operatorname{gr}_I(R)$-module associated to the twisted filtration $\{R(-\ell)_n\}_{n\geq 0}$ is the twisted module $\operatorname{gr}_I(R)(-\ell)$. In other words, show that the graded $\operatorname{gr}_I(R)$-modules $\operatorname{gr}(R(-\ell))$ and $\operatorname{gr}_I(R)(-\ell)$ are isomorphic.

EXERCISE 7.3.10. Let R be a commutative ring and I an ideal in R.

(1) Prove that if R/I is noetherian, and I/I^2 is a finitely generated R/I-module, then the associated graded ring $\mathrm{gr}_I(R) = \bigoplus_{n\geq 0} I^n/I^{n+1}$ is noetherian.
(2) Assume moreover that R is separated and complete for the I-adic topology. Prove that R is noetherian.

4. Lifting of Idempotents and Hensel's Lemma

As in Section 3.3.1, if R is a ring, then $\mathrm{idemp}(R) = \{x \in R \mid x^2 - x = 0\}$ denotes the set of idempotents of R. The homomorphic image of an idempotent is an idempotent, so given a homomorphism of rings $A \to B$, there is a function $\mathrm{idemp}(A) \to \mathrm{idemp}(B)$. If this function is onto, then we say idempotents of B lift to idempotents of A. In this section we prove that when R is a ring and I is an ideal of R such that $I \subseteq \mathrm{J}(R)$ and R is separated and complete with respect to the I-adic topology, then idempotents of R/I lift to idempotents in R. This is proved in the main result, Corollary 7.4.1, which is a corollary to Nakayama's Lemma (Theorem 4.2.3). We then proceed to give two important applications of Corollary 7.4.1. In Proposition 7.4.3 we show that the change of base functor from the category of finitely generated projective R-modules to the category of finitely generated projective R/I-modules is essentially surjective. We end this section with a second application of the main result to prove Corollary 7.4.4 which is a general form of Hensel's Lemma. In the classical Hensel's Lemma, R is usually assumed to be a complete local ring with maximal ideal $\mathfrak{m}$ and residue field k. Then if $f \in R[x]$ is a monic polynomial such that f has a factorization $\bar{f} = \bar{g}_0\bar{h}_0$ in $k[x]$, where g_0 and h_0 are monic and $\gcd(\bar{g}_0, \bar{h}_0) = 1$ in $k[x]$, then the factorization lifts to a factorization over R. That is, there exist monic polynomials g, h in $R[x]$ such that $f = gh$, $\bar{g} = \bar{g}_0$, $\bar{h} = \bar{h}_0$, and g and h generate the unit ideal in $R[x]$.

COROLLARY 7.4.1. *Let R be a ring and I a two-sided ideal of R such that $I \subseteq \mathrm{J}(R)$. If R is separated and complete with respect to the I-adic topology (that is, $R \to \varprojlim R/I^n$ is an isomorphism), then* $\mathrm{idemp}(R) \to \mathrm{idemp}(R/I)$ *is onto.*

PROOF. Let $\bar{x} \in R/I$ be an idempotent. For $n \geq 1$, I/I^n is nilpotent. By Corollary 4.2.8 (2), $\mathrm{idemp}(R/I^n) \to \mathrm{idemp}(R/I)$ is onto for $n > 1$. Set $e_1 = x$. By induction, there is a sequence $(\bar{e}_i)$ in $\prod_i R/I^i$ such that $e_n^2 - e_n \in I^n$ and $e_{n+1} - e_n \in I^n$. So $(\bar{e}_i)$ is an idempotent in $R = \varprojlim R/I^n$ which maps to $\bar{x}$ in R/I. □

COROLLARY 7.4.2. *Let R be a commutative ring and I an ideal in R such that R is separated and complete with respect to the I-adic topology (that is, $R \to \varprojlim R/I^n$ is an isomorphism). Let A be an R-algebra which is integral over R.*

(1) If A is an R-module of finite presentation, then A is separated and complete in the IA-adic topology, $IA \subseteq \mathrm{J}(A)$, and $\mathrm{idemp}(A) \to \mathrm{idemp}(A \otimes_R (R/I))$ *is onto. That is, an idempotent $\bar{e}$ in A/IA lifts to an idempotent e in A.*
(2) If A is commutative, then $\mathrm{idemp}(A) \to \mathrm{idemp}(A \otimes_R (R/I))$ *is onto.*

PROOF. (1): Assume that A is an R-module of finite presentation. We are given that $R \to \varprojlim R/I^n$ is an isomorphism. By Proposition 7.3.1, $A \to \varprojlim A/(I^nA)$ is an isomorphism, so A is separated and complete in the IA-adic topology. By Proposition 7.1.11, IA is contained in the Jacobson radical of A. The conclusion follows from Corollary 7.4.1 (3).

(2): First we reduce to the case where A is generated as an R-algebra by a single element. Let $a \in A$ be a preimage of $\bar{e}$. Let C be the R-subalgebra of A generated by a. Then A is a faithful C-algebra which is integral over C. By Theorem 6.3.6, $\operatorname{Spec} A \to \operatorname{Spec} C$ is onto. The reader should verify that $\operatorname{Spec} \bar{A} \to \operatorname{Spec} \bar{C}$ is onto as well, where $\bar{C} = C/IC$.

Write $\bar{a}$ for the image of a in $\bar{C}$. Under the natural map $\bar{C} \to \bar{A}$, we have $\bar{a} \mapsto \bar{e}$. The reader should verify that $\operatorname{Spec} \bar{C} = V(\bar{a}) \cup V(1-\bar{a})$, so by Corollary 3.3.14 there is a unique idempotent $\bar{f}$ in $\bar{C}$ such that $V(\bar{a}) = V(\bar{f})$. From this it follows that $\bar{f} \mapsto \bar{e}$. If there exists an idempotent f in C that lifts $\bar{f}$, then using $C \to A$, we get a lifting of $\bar{e}$.

Now assume A is generated as an R-algebra by a single element a. Then a is integral over R. Let $p \in R[x]$ be a monic polynomial such that $p(a) = 0$. Let $C = R[x]/(p)$. Then C is a finitely generated free R-module. Let J be the kernel of the natural projection $C \to A$. Let $\{J_\alpha\}$ be the directed system of all finitely generated ideals in C such that $J_\alpha \subseteq J$. Then $C_\alpha = C/J_\alpha$ is an R-module of finite presentation, for each α, and $A = \varinjlim C_\alpha$. Therefore, $\bar{A} = A/IA = \varinjlim C_\alpha/IC_\alpha = \varinjlim \bar{C}_\alpha$. By Exercise 2.7.19, an idempotent $\bar{e}$ in $\bar{A}$ comes from an idempotent $\bar{e}_\alpha$ in $\bar{C}_\alpha$, for some α. By (1) we can lift $\bar{e}_\alpha$ to an idempotent $e_\alpha \in C_\alpha$. Using $C_\alpha \to A$, we get a lifting of $\bar{e}$ to an idempotent in A. $\square$

As an application of Corollary 7.4.1, we give sufficient conditions on a ring R and an ideal I in R such that every finitely generated projective R/I-module lifts to a finitely generated projective R-module. If $\mathfrak{C}$ is the category of finitely generated projective R-modules and $\mathfrak{D}$ is the category of finitely generated projective R/I-modules, then Proposition 7.4.3 shows that the functor $(\ ) \otimes_R (R/I) : \mathfrak{C} \to \mathfrak{D}$ is essentially surjective.

PROPOSITION 7.4.3. *Let R be a ring and I a two-sided ideal of R such that $I \subseteq \mathrm{J}(R)$ and R is separated and complete with respect to the I-adic topology (that is, $R \to \varprojlim R/I^n$ is an isomorphism).*

(1) If Q is a finitely generated projective R/I-module, then there is a finitely generated projective R-module P such that $Q \cong P \otimes_R (R/I)$.
(2) If $g : Q_1 \to Q_2$ is a homomorphism of finitely generated projective R/I-modules, then g lifts to a homomorphism $f : P_1 \to P_2$ of finitely generated projective R-modules.
(3) If Q is an R/I-progenerator module, then there is an R-progenerator module P such that $Q \cong P \otimes_R (R/I)$.

PROOF. (1): For some $m > 0$, there is an isomorphism $(R/I)^m \cong Q \oplus Q_0$. Let $\bar{e}$ be the idempotent matrix in $M_m(R/I)$ such that $Q \cong \operatorname{im}(\bar{e})$ and $Q_0 \cong \ker(\bar{e})$. Since $\varprojlim M_n(R/I^n) = M_n(\varprojlim R/I^n) = M_n(R)$, by Corollary 7.4.1, we can lift $\bar{e}$ to an idempotent $e \in M_n(R)$. If we set $P = \operatorname{im}(e)$, then $Q \cong P \otimes_R (R/I)$.

(2): Using (1), there are projective R-modules P_i such that $Q_i \cong P_i \otimes_R (R/I)$. Combined with g, there is a diagram

$$\begin{tikzcd} P_1 \arrow[r] \arrow[d, dashed, "\exists f"'] & Q_1 \arrow[r] \arrow[d, "g"] & 0 \\ P_2 \arrow[r] & Q_2 \arrow[r] & 0 \end{tikzcd}$$

where the rows are exact. Since P_1 is a projective R-module, there exists a map f which makes the diagram commutative (Proposition 2.1.1).

(3): Is left to the reader. $\square$

As an application of Corollary 7.4.2, we prove the following form of Hensel's Lemma.

COROLLARY 7.4.4. *(Hensel's Lemma) Let R be a commutative ring and I an ideal of R such that R is separated and complete with respect to the I-adic topology (that is, $R \to \varprojlim R/I^n$ is an isomorphism). If there exist polynomials $f, g_0, h_0 \in R[x]$ such that*

(1) f, g_0 and h_0 are monic,

(2) $f - g_0 h_0 \in IR[x]$*, and*
(3) $R[x] = g_0 R[x] + h_0 R[x] + IR[x]$*,*

then there exist polynomials $g, h \in R[x]$ *such that*

(4) g *and* h *are monic,*
(5) $R[x] = gR[x] + hR[x]$*,*
(6) $g - g_0 \in IR[x]$*,*
(7) $h - h_0 \in IR[x]$*, and*
(8) $f = gh \in R[x]$*.*

PROOF. Write $\bar{R}$ for R/I and let $\bar{f}, \bar{g}_0, \bar{h}_0$ denote the images of the polynomials in $\bar{R}[x]$. By (2) we have $\bar{f} = \bar{g}_0 \bar{h}_0$ and by (3), $(\bar{g}_0, \bar{h}_0)$ is the unit ideal of $\bar{R}[x]$. If we set $S = R[x]/(f)$, then S is a finitely generated free R-module and the rank of S is equal to $\deg f = \deg g_0 + \deg h_0$, by Example 1.6.10 (2). Write $\bar{S}$ for $S/IS = S \otimes_R \bar{R}$. By the Chinese Remainder Theorem, Theorem 1.1.7,

$$\bar{S} = \frac{\bar{R}[x]}{(\bar{f})} = \frac{\bar{R}[x]}{(\bar{g}_0 \bar{h}_0)} = \frac{\bar{R}[x]}{(\bar{g}_0)} \oplus \frac{\bar{R}[x]}{(\bar{h}_0)}.$$

By Lemma 3.2.4, corresponding to the direct summands of $\bar{S}$ are orthogonal idempotents $\bar{e}_1, \bar{e}_2$ and $1 = \bar{e}_1 + \bar{e}_2$. By Corollaries 7.4.2 and 7.4.1, the map $\operatorname{idemp} S \to \operatorname{idemp} \bar{S}$ is a one-to-one correspondence. The idempotents $\bar{e}_1, \bar{e}_2$ lift to idempotents e_1, e_2 of S such that $e_1 e_2 = 0$ and $e_1 + e_2 = 1$. The decomposition of $\bar{S}$ lifts to a decomposition $S = R[x]/(f) = Se_1 \oplus Se_2$. Let $\theta_1 : R[x] \to Se_1$ be the composite map $R[x] \to R[x]/(f) \cong S \to Se_1$. Denote by n_0 the degree of g_0. In $R[x]$ consider the R-submodule $T = R \cdot 1 + Rx + \cdots + Rx^{n_0 - 1}$. Consider the composite map

$$R[x] \xrightarrow{\theta_1} Se_1 \to \frac{Se_1}{ISe_1} \cong \frac{\bar{R}[x]}{(\bar{g}_0)}.$$

If $\bar{x}$ denotes the coset $x + (\bar{g}_0)$ in $\bar{R}[x]/(\bar{g}_0)$, then the image of T in $\bar{R}[x]/(\bar{g}_0)$ is the $\bar{R}$-submodule $\bar{R} \cdot 1 + \bar{R}\bar{x} + \cdots + \bar{R}\bar{x}^{n_0 - 1}$, which is equal to $\bar{R}[x]/(\bar{g}_0)$. Therefore, Se_1 is generated as an R-module by $\theta_1(T)$ and ISe_1. Nakayama's Lemma (Corollary 2.2.5 (2)) says that $\theta_1(T) = Se_1$. If we write $y_1 = \theta_1(x) = xe_1$, then $y_1^{n_0} \in \theta_1(T)$. Hence there is a monic polynomial $g \in R[x]$ of degree n_0 such that $\theta_1(g) = g(y_1) = 0$. There is a map $\tilde{\theta}_1$ such that

$$\begin{tikzcd}
R[x] \arrow[rr, "\theta_1"] \arrow[dr] & & Se_1 \\
& \frac{R[x]}{(g)} \arrow[ur, "\tilde{\theta}_1"'] &
\end{tikzcd}$$

is a commutative diagram. Tensoring $\tilde{\theta}_1$ with $(\ ) \otimes_R \bar{R}$, the diagram

$$\begin{tikzcd}
\frac{R[x]}{(g)} \arrow[r, "\tilde{\theta}_1"] \arrow[d] & Se_1 \arrow[d] & \\
\frac{\bar{R}[x]}{(\bar{g})} \arrow[r, "\tilde{\theta}_1 \otimes 1"] & \frac{Se_1}{ISe_1} \arrow[r, "\cong"] & \frac{\bar{R}[x]}{(\bar{g}_0)}
\end{tikzcd}$$

commutes. Therefore, in the ring $\bar{R}[x]$, $\bar{g}$ is in the ideal $(\bar{g}_0)$. That is, $\bar{g}_0$ divides $\bar{g}$. Since both polynomials are monic of degree n_0, the Division Algorithm implies that $\bar{g}_0 = \bar{g}$. This shows $\tilde{\theta}_1 \otimes 1$ is an isomorphism of $\bar{R}$-modules. Since Se_1 is a direct summand of S,

Se_1 is R-projective. By Example 1.6.10 (2), $R[x]/(g)$ is a free R-module of rank n_0. By Exercise 4.2.7, it follows that $\tilde{\theta}_1$ is an isomorphism. Likewise there is a monic polynomial $h \in R[x]$ such that the degree of h is equal to the degree of h_0, $\bar{h} = \bar{h}_0$, $h(xe_2) = 0$, and $R[x]/(h) \cong Se_2$. So the image of h under $\theta_2 : R[x] \to Se_2$ is 0. Since gh is in the kernel of the map $R[x] \to R[x]/(f) = S = Se_1 \oplus Se_2$, it follows that f divides gh. Since gh and f are both monic of the same degree, it follows that $f = gh$. In the commutative diagram

$$\begin{tikzcd} \frac{R[x]}{(f)} \arrow[r] \arrow[d] & \frac{R[x]}{(g)} \bigoplus \frac{R[x]}{(h)} \arrow[d] \\ S \arrow[r] & Se_1 \bigoplus Se_2 \end{tikzcd}$$

all of the maps are isomorphisms. By Theorem 1.1.7, the ideal (g,h) is equal to $R[x]$. $\square$

When R is a complete local ring with maximal ideal $\mathfrak{m}$, Lemma 7.4.5, which is due to Azumaya [**9**], shows that simple roots have unique liftings modulo $\mathfrak{m}$.

LEMMA 7.4.5. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field k such that R is separated and complete with respect to the $\mathfrak{m}$-adic topology. Let $f \in R[x]$ be a monic polynomial and $a \in R$. If $\bar{a} \in k$ is a simple root of $\bar{f}$, then there exists a unique $b \in R$ such that $f(b) = 0$ and $b - a \in \mathfrak{m}$.*

PROOF. Assume $\bar{a}$ is a simple root of $\bar{f}$. Then there exists a monic polynomial $g_0 \in R[x]$ such that $\bar{f} = (x - \bar{a})\bar{g}_0$ in $k[x]$ and $\bar{g}_0(\bar{a}) \neq 0$. Therefore, $x - \bar{a}$ and $\bar{g}_0$ generate the unit ideal in $k[x]$. By Corollary 7.4.4, there are $b \in R$, $g \in R[x]$ such that $f = (x - b)g$, $b - a \in \mathfrak{m}$ and $\bar{g} = \bar{g}_0$. This shows $f(b) = 0$. Now suppose $c - a \in \mathfrak{m}$ and $f(c) = 0$. Then $(c - b)g(c) = 0$. But $g(c) \notin \mathfrak{m}$ because $\bar{c} = \bar{a}$ is not a root of $\bar{g}$. Since R is a local ring, this implies $g(c)$ is an invertible element of R. Hence $c - b = 0$ and b is unique. $\square$

CHAPTER 8

Homological Algebra

This chapter presents a self-contained introduction to homological algebra. The only references are to results already proven in the earlier chapters. In Sections 8.1 and 8.2 the goal is to derive the fundamental properties of the left derived and right derived groups of a covariant or contravariant additive functor from a category of modules to the category of abelian groups. Section 8.3 is an introduction to the Tor and Ext groups. These groups arise when the theory developed in the first two sections is applied to the bifunctors defined by tensor product and Hom.

In Section 8.4 the notions of projective dimension and injective dimension are introduced for a module M. For a commutative ring R, the cohomological dimension is defined and some of the first properties are proven. Section 8.5 is an introduction to group cohomology. If G is a group, and A is a G-module, the cohomology groups of G with coefficients in A are defined using the theory from Section 8.3. Section 8.6 contains an introduction to the theory of faithfully flat descent. The starting point for this theory is the Amitsur complex associated to a faithfully flat extension of commutative rings, S/R. Hochschild cohomology is defined in Section 8.7. The Amitsur complex is the basis for the Amitsur cohomology of Section 8.8. We show that Amitsur cohomology can be used to parametrize the twisted forms of a module.

Throughout this chapter, R denotes an arbitrary ring. Unless otherwise specified, a module will be a left R-module, a homomorphism will be a homomorphism of R-modules, and a functor will be an additive functor from the category of R-modules to the category of abelian groups. (See Example 8.1.2 for the definition of additive functor.)

The author acknowledges that the material in this section is based on various sources, including [**51**], [**41**], [**23**], [**36**], [**14**], [**30**], and [**47**].

1. Homology Group Functors

1.1. Chain Complexes. A *chain complex* in ${}_R\mathfrak{M}$ is a sequence of R-modules $\{A_i \mid i \in \mathbb{Z}\}$ and homomorphisms $d_i : A_i \to A_{i-1}$ such that $d_{i-1}d_i = 0$ for all $i \in \mathbb{Z}$. The maps d_i are called the *boundary maps*. The notation $A_\bullet$ denotes a chain complex. If it is important to reference the boundary maps, we will write $(A_\bullet, d_\bullet)$. If the modules A_i are specified for some range $n_0 \le i \le n_1$, then it is understood that $A_i = 0$ for $i < n_0$ or $i > n_1$. Let $A_\bullet$ and $B_\bullet$ be chain complexes. A *morphism of chain complexes* is a sequence of homomorphisms $f = \{f_i : A_i \to B_i \mid i \in \mathbb{Z}\}$ such that for each i the diagram

$$\begin{tikzcd}
A_{i+1} \arrow[r, "d_{i+1}"] \arrow[d, "f_{i+1}"] & A_i \arrow[r, "d_i"] \arrow[d, "f_i"] & A_{i-1} \arrow[d, "f_{i-1}"] \\
B_{i+1} \arrow[r, "d_{i+1}"] & B_i \arrow[r, "d_i"] & B_{i-1}
\end{tikzcd}$$

commutes. In this case we write $f : A_\bullet \to B_\bullet$. The reader should verify that the collection of all chain complexes over R together with morphisms is a category. In some of the exercises listed below the reader is asked to verify many of the important features of this category.

Suppose $A_\bullet$ is a chain complex and $n \in \mathbb{Z}$. Elements of A_n are called *n-chains*. The module A_n contains the two submodules

$$\begin{aligned} \mathrm{B}_n(A_\bullet) &= \operatorname{im} d_{n+1}, \quad \text{and} \\ \mathrm{Z}_n(A_\bullet) &= \ker d_n. \end{aligned}$$

Elements of $\mathrm{B}_n(A_\bullet)$ are called *n-boundaries* and elements of $\mathrm{Z}_n(A_\bullet)$ are called *n-cycles*. The condition $d_i d_{i+1} = 0$ translates into $\mathrm{B}_n(A_\bullet) \subseteq \mathrm{Z}_n(A_\bullet)$. The *nth homology module* of $A_\bullet$ is defined to be the quotient

$$\mathrm{H}_n(A_\bullet) = \mathrm{Z}_n(A_\bullet)/\mathrm{B}_n(A_\bullet) = \ker d_n / \operatorname{im} d_{n+1}.$$

EXAMPLE 8.1.1.
(1) A short exact sequence $0 \to A \to B \to C \to 0$ is a chain complex. It is understood that the sequence is extended with 0 terms.
(2) If M is an R-module, then a projective resolution

$$\cdots \to P_1 \to P_0 \to M \to 0$$

of M is a chain complex (see Exercise 2.2.5). It is understood that the sequence is extended with 0 terms.
(3) If $A_\bullet$ is a chain complex, the reader should verify that the following are equivalent
  (a) $\mathrm{H}_n(A_\bullet) = 0$ for all $n \in \mathbb{Z}$.
  (b) $A_\bullet$ is an exact sequence.

EXAMPLE 8.1.2. A covariant functor $\mathfrak{F} : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$ is said to be *additive* in case for every pair of R-modules A, B, the map $\mathfrak{F}(\cdot) : \operatorname{Hom}_R(A,B) \to \operatorname{Hom}_\mathbb{Z}(\mathfrak{F}(A), \mathfrak{F}(B))$ is a $\mathbb{Z}$-module homomorphism. In particular, under a covariant additive functor, the zero homomorphism is mapped to the zero homomorphism. It follows that if $A_\bullet$ is a chain complex, then $\mathfrak{F}(A_\bullet)$ is a chain complex. It is for this reason that additive functors play an important role in homological algebra. A contravariant functor $\mathfrak{F} : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$ is said to be *additive* in case for every pair of R-modules A, B, the map $\mathfrak{F}(\cdot) : \operatorname{Hom}_R(A,B) \to \operatorname{Hom}_\mathbb{Z}(\mathfrak{F}(B), \mathfrak{F}(A))$ is a $\mathbb{Z}$-module homomorphism.

LEMMA 8.1.3. *Let n be an arbitrary integer.*
(1) If $f : A_\bullet \to B_\bullet$ is a morphism of chain complexes, then the assignment

$$z_n + \mathrm{B}_n(A_\bullet) \mapsto f_n(z_n) + \mathrm{B}_n(B_\bullet)$$

defines an R-module homomorphism

$$\mathrm{H}_n(f) : \mathrm{H}_n(A_\bullet) \to \mathrm{H}_n(B_\bullet).$$

(2) The assignment $A_\bullet \mapsto \mathrm{H}_n(A_\bullet)$ defines a functor from the category of chain complexes to the category of R-modules.

PROOF. (1): Given $z_n \in \mathrm{Z}_n(A_\bullet)$, we have $d_n f_n(z_n) = f_{n-1} d_n(z_n) = f_{n-1}(0) = 0$. This says that the composite map

$$f_n : \mathrm{Z}_n(A_\bullet) \to \mathrm{Z}_n(B_\bullet) \to \mathrm{H}_n(B_\bullet)$$

is well defined. Given $a_{n+1} \in A_{n+1}$, $f_n d_{n+1}(a_{n+1}) = d_{n+1} f_{n+1}(a_{n+1})$. This implies that $f_n(\mathrm{B}_n(A_\bullet)) \subseteq \mathrm{B}_n(B_\bullet)$, so $\mathrm{H}_n(f) : \mathrm{H}_n(A_\bullet) \to \mathrm{H}_n(B_\bullet)$ is well defined.

(2): is left to the reader. $\square$

1.2. Exercises.

EXERCISE 8.1.1. For the category of chain complexes, the reader should give appropriate definitions for the following terminology.

(1) The *kernel* of a morphism.
(2) The *cokernel* of a morphism.
(3) The *image* of a morphism.
(4) A *subchain complex* of a chain complex and the *quotient* of a chain complex modulo a subchain complex.
(5) *monomorphism*, *epimorphism*, and *isomorphism*.
(6) *short exact sequence*.

EXERCISE 8.1.2. Let $A_\bullet$ be a chain complex. For each $n \in \mathbb{Z}$ there are short exact sequences of R-modules.

(1) $0 \to \mathrm{B}_n(A_\bullet) \to \mathrm{Z}_n(A_\bullet) \to \mathrm{H}_n(A_\bullet) \to 0$
(2) $0 \to \mathrm{Z}_n(A_\bullet) \to A_n \to \mathrm{B}_{n-1}(A_\bullet) \to 0$
(3) $0 \to \mathrm{H}_n(A_\bullet) \to A_n/\mathrm{B}_n(A_\bullet) \to \mathrm{B}_{n-1}(A_\bullet) \to 0$

EXERCISE 8.1.3. Let $A_\bullet$ be a chain complex. For each $n \in \mathbb{Z}$ there is an exact sequence of R-modules.

$$0 \to \mathrm{H}_n(A_\bullet) \to A_n/\mathrm{B}_n(A_\bullet) \xrightarrow{d_n} \mathrm{Z}_{n-1}(A_\bullet) \to \mathrm{H}_{n-1}(A_\bullet) \to 0$$

EXERCISE 8.1.4. Let $\mathfrak{F}$ be an exact covariant additive functor from ${}_R\mathfrak{M}$ to ${}_\mathbb{Z}\mathfrak{M}$. If $A_\bullet$ is a chain complex, then $\mathfrak{F}(\mathrm{H}_n(A_\bullet)) \cong \mathrm{H}_n(\mathfrak{F}(A_\bullet))$. (Hint: Start with the exact sequences

$$0 \to \mathrm{B}_n(A_\bullet) \to \mathrm{Z}_n(A_\bullet) \to \mathrm{H}_n(A_\bullet) \to 0$$
$$0 \to \mathrm{Z}_n(A_\bullet) \to A_n \to \mathrm{B}_{n-1}(A_\bullet) \to 0$$

and apply $\mathfrak{F}$.)

EXERCISE 8.1.5. Let J be an index set and $\{(A^j)_\bullet \mid j \in J\}$ a collection of chain complexes.

(1) Show that

$$\cdots \xrightarrow{\oplus d_{n+1}} \bigoplus_{j \in J} (A^j)_n \xrightarrow{\oplus d_n} \bigoplus_{j \in J} (A^j)_{n-1} \xrightarrow{\oplus d_{n-1}} \cdots$$

is a chain complex, which is called the *direct sum chain complex*.

(2) Show that homology commutes with a direct sum. That is

$$\mathrm{H}_n\left(\bigoplus_{j \in J} (A^j)_\bullet\right) \cong \bigoplus_{j \in J} \mathrm{H}_n\big((A^j)_\bullet\big).$$

(Hint: Start with the exact sequences

$$0 \to \mathrm{B}_n((A^j)_\bullet) \to \mathrm{Z}_n((A^j)_\bullet) \to \mathrm{H}_n((A^j)_\bullet) \to 0$$
$$0 \to \mathrm{Z}_n((A^j)_\bullet) \to (A^j)_n \to \mathrm{B}_{n-1}((A^j)_\bullet) \to 0$$

and take direct sums.)

EXERCISE 8.1.6. Let $\{(A^j)_\bullet, \phi^i_j\}$ be a directed system of chain complexes for a directed index set I.

(1) Show that

$$\cdots \xrightarrow{\vec{d}_{n+1}} \varinjlim (A^j)_n \xrightarrow{\vec{d}_n} \varinjlim (A^j)_{n-1} \xrightarrow{\vec{d}_{n-1}} \cdots$$

is a chain complex, which is called the *direct limit chain complex*.

(2) Show that homology commutes with a direct limit. That is

$$\mathrm{H}_n\left(\varinjlim (A^j)_\bullet\right) \cong \varinjlim \mathrm{H}_n\big((A^j)_\bullet\big).$$

(Hint: Start with the exact sequences

$$0 \to \mathrm{B}_n((A^j)_\bullet) \to \mathrm{Z}_n((A^j)_\bullet) \to \mathrm{H}_n((A^j)_\bullet) \to 0$$
$$0 \to \mathrm{Z}_n((A^j)_\bullet) \to (A^j)_n \to \mathrm{B}_{n-1}((A^j)_\bullet) \to 0$$

and take direct limits.)

1.3. The Long Exact Sequence of Homology.

THEOREM 8.1.4. *Let*

$$0 \to A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \to 0$$

be an exact sequence of chain complexes. Then there is a long exact sequence of homology modules

$$\cdots \to \mathrm{H}_n(A_\bullet) \xrightarrow{\mathrm{H}(f)} \mathrm{H}_n(B_\bullet) \xrightarrow{\mathrm{H}(g)} \mathrm{H}_n(C_\bullet) \xrightarrow{\partial} \mathrm{H}_{n-1}(A_\bullet) \xrightarrow{\mathrm{H}(f)} \mathrm{H}_{n-1}(B_\bullet) \xrightarrow{\mathrm{H}(g)} \cdots$$

PROOF. The idea for the proof is to reduce the problem into two applications of the Snake Lemma (Theorem 2.5.2).

Step 1: For each $n \in \mathbb{Z}$ the sequences

$$0 \to \mathrm{Z}_n(A_\bullet) \xrightarrow{f_n} \mathrm{Z}_n(B_\bullet) \xrightarrow{g_n} \mathrm{Z}_n(C_\bullet)$$

$$A_n/\mathrm{B}_n(A_\bullet) \xrightarrow{f_n} B_n/\mathrm{B}_n(B_\bullet) \xrightarrow{g_n} C_n/\mathrm{B}_n(C_\bullet) \to 0$$

are exact. To see this, start with the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_n \arrow[r, "f_n"] \arrow[d, "d_n"] & B_n \arrow[r, "g_n"] \arrow[d, "d_n"] & C_n \arrow[r] \arrow[d, "d_n"] & 0 \\
0 \arrow[r] & A_{n-1} \arrow[r] & B_{n-1} \arrow[r] & C_{n-1} \arrow[r] & 0
\end{tikzcd}$$

and apply the Snake Lemma. For the first sequence, use the fact that $\mathrm{Z}_n(X_\bullet)$ is the the kernel of d_n for $X = A, B, C$. For the second sequence, use the fact that $\mathrm{B}_{n-1}(X_\bullet)$ is the image of d_n for $X = A, B, C$ and increment n by one.

Step 2: For each $n \in \mathbb{Z}$ there is an exact sequence

$$\mathrm{H}_n(A_\bullet) \xrightarrow{\mathrm{H}(f)} \mathrm{H}_n(B_\bullet) \xrightarrow{\mathrm{H}(g)} \mathrm{H}_n(C_\bullet) \xrightarrow{\partial} \mathrm{H}_{n-1}(A_\bullet) \xrightarrow{\mathrm{H}(f)} \mathrm{H}_{n-1}(B_\bullet) \xrightarrow{\mathrm{H}(g)} \mathrm{H}_{n-1}(C_\bullet)$$

of R-modules. To see this, start with the commutative diagram

$$\begin{tikzcd}
 & A_n/\mathrm{B}_n(A_\bullet) \arrow[r, "f_n"] \arrow[d, "d_n"] & B_n/\mathrm{B}_n(B_\bullet) \arrow[r, "g_n"] \arrow[d, "d_n"] & C_n/\mathrm{B}_n(C_\bullet) \arrow[r] \arrow[d, "d_n"] & 0 \\
0 \arrow[r] & \mathrm{Z}_{n-1}(A_\bullet) \arrow[r, "f_{n-1}"] & \mathrm{Z}_{n-1}(B_\bullet) \arrow[r, "g_{n-1}"] & \mathrm{Z}_{n-1}(C_\bullet) &
\end{tikzcd}$$

the rows of which are exact by Step 1. The exact sequence of Exercise 8.1.3 says that the kernel of d_n is $\mathrm{H}_n()$ and the cokernel is $\mathrm{H}_{n-1}()$. Apply the Snake Lemma. $\square$

THEOREM 8.1.5. *In the context of Theorem 8.1.4, the connecting homomorphism* $\partial : \mathrm{H}_n(C_\bullet) \to \mathrm{H}_{n-1}(A_\bullet)$ *is natural. More specifically, if*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_\bullet & \xrightarrow{f} & B_\bullet & \xrightarrow{g} & C_\bullet & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\chi} & & \downarrow{\scriptstyle\rho} & & \downarrow{\scriptstyle\sigma} & & \\ 0 & \longrightarrow & A'_\bullet & \xrightarrow{f'} & B'_\bullet & \xrightarrow{g'} & C'_\bullet & \longrightarrow & 0 \end{array}$$

is a commutative diagram of chain complexes with exact rows, then there is a commutative diagram

$$\begin{array}{ccccccc} \mathrm{H}_n(A_\bullet) & \xrightarrow{\mathrm{H}(f)} & \mathrm{H}_n(B_\bullet) & \xrightarrow{\mathrm{H}(g)} & \mathrm{H}_n(C_\bullet) & \xrightarrow{\partial} & \mathrm{H}_{n-1}(A_\bullet) \\ \downarrow{\scriptstyle \mathrm{H}(\chi)} & & \downarrow{\scriptstyle \mathrm{H}(\rho)} & & \downarrow{\scriptstyle \mathrm{H}(\sigma)} & & \downarrow{\scriptstyle \mathrm{H}(\chi)} \\ \mathrm{H}_n(A'_\bullet) & \xrightarrow{\mathrm{H}(f')} & \mathrm{H}_n(B'_\bullet) & \xrightarrow{\mathrm{H}(g')} & \mathrm{H}_n(C'_\bullet) & \xrightarrow{\partial'} & \mathrm{H}_{n-1}(A'_\bullet) \end{array}$$

with exact rows for each $n \in \mathbb{Z}$.

PROOF. Most of this follows straight from Lemma 8.1.3 and Theorem 8.1.4. It is only necessary to check that the third square is commutative. For this, use the definition of ∂ given in the proof of Theorem 2.5.2. The gist of the proof is $\mathrm{H}(\chi)\partial = \chi_{n-1} f_{n-1}^{-1} d_n g_n^{-1} = {f'_{n-1}}^{-1} d'_n {g'_n}^{-1} \sigma_n = \partial' \mathrm{H}(\sigma)$. The details are left to the reader. □

1.4. Homotopy Equivalence. Let $A_\bullet$ and $B_\bullet$ be chain complexes. By $\mathrm{Hom}(A_\bullet, B_\bullet)$ we denote the set of all morphisms $f : A_\bullet \to B_\bullet$. For each $i \in \mathbb{Z}$, $f_i : A_i \to B_i$ is an R-module homomorphism. The sum of two morphisms $f, g \in \mathrm{Hom}(A_\bullet, B_\bullet)$ is defined to be the sequence $f + g = \{f_i + g_i \mid i \in \mathbb{Z}\}$. This binary operation turns $\mathrm{Hom}(A_\bullet, B_\bullet)$ into a $\mathbb{Z}$-module. Two morphisms f, g are said to be *homotopic* if there exists a sequence of R-module homomorphisms $\{k_i : A_i \to B_{i+1} \mid i \in \mathbb{Z}\}$ such that $f_n - g_n = d_{n+1} k_n + k_{n-1} d_n$ for each $n \in \mathbb{Z}$. If f and g are homotopic, then we write $f \sim g$ and the sequence $\{k_i\}$ is called a *homotopy operator*. The reader should verify that homotopy equivalence is an equivalence relation on $\mathrm{Hom}(A_\bullet, B_\bullet)$.

THEOREM 8.1.6. *Let* $A_\bullet$ *and* $B_\bullet$ *be chain complexes. For each* $n \in \mathbb{Z}$*, the functor* $\mathrm{H}_n()$ *is constant on homotopy equivalence classes. In other words, if f and g are homotopic in* $\mathrm{Hom}(A_\bullet, B_\bullet)$*, then* $H(f)$ *is equal to* $H(g)$ *in* $\mathrm{Hom}_R(\mathrm{H}_n(A_\bullet), \mathrm{H}_n(B_\bullet))$.

PROOF. We are given a homotopy operator $\{k_i : A_i \to B_{i+1} \mid i \in \mathbb{Z}\}$ such that for any $z \in \mathrm{Z}_n(A_\bullet)$

$$(f_n - g_n)(z) = d_{n+1} k_n(z) + k_{n-1} d_n(z)$$

for each $n \in \mathbb{Z}$. But $d_n(z) = 0$, which implies $f_n(z) - g_n(z) = d_{n+1} k_n(z) \in \mathrm{B}_n(B_\bullet)$. □

THEOREM 8.1.7. *Let* $X_\bullet$ *and* $Y_\bullet$ *be chain complexes such that each* X_i *is a projective* R*-module and* $X_i = Y_i = 0$ *for all* $i < 0$*. Suppose* M *and* N *are* R*-modules and that there exist* R*-module homomorphisms* ε *and* π *such that*

$$\cdots \to X_2 \to X_1 \to X_0 \xrightarrow{\varepsilon} M \to 0$$

is a chain complex and

$$\cdots \to Y_2 \to Y_1 \to Y_0 \xrightarrow{\pi} N \to 0$$

is a long exact sequence.

(1) *Given any* $f \in \mathrm{Hom}_R(M, N)$*, there exists a morphism* $f : X_\bullet \to Y_\bullet$ *which commutes with* f *on the augmented chain complexes. That is,* $f\varepsilon = \pi f_0$.

(2) The morphism f is unique up to homotopy equivalence.

PROOF. (1): The morphism f is constructed recursively. To construct f_0, consider the diagram

$$\begin{tikzcd} X_0 \arrow[d, dashed, "\exists f_0"'] \arrow[dr, "f\varepsilon"] & & \\ Y_0 \arrow[r, "\pi"] & N \arrow[r] & 0 \end{tikzcd}$$

with bottom row exact. Since X_0 is projective, there exists $f_0 : X_0 \to Y_0$ such that $\pi f_0 = f\varepsilon$.

To construct f_1, start with the commutative diagram

$$\begin{tikzcd} X_1 \arrow[r, "d_1"] \arrow[d, dashed, "\exists f_1"'] & X_0 \arrow[r, "\varepsilon"] \arrow[d, "f_0"] & M \arrow[d, "f"] \\ Y_1 \arrow[r, "d_1"] & Y_0 \arrow[r, "\pi"] & N \end{tikzcd}$$

The top row is a chain complex, the bottom row is exact. Because $\pi f_0 d_1 = f\varepsilon d_1 = 0$, it follows that $\operatorname{im}(f_0 d_1) \subseteq \ker(\pi) = \operatorname{im}(d_1)$. Consider the diagram

$$\begin{tikzcd} X_1 \arrow[d, dashed, "\exists f_1"'] \arrow[dr, "f_0 d_1"] & & \\ Y_1 \arrow[r, "d_1"] & \operatorname{im} d_1 \arrow[r] & 0 \end{tikzcd}$$

in which the bottom row is exact. Since X_1 is projective, there exists $f_1 : X_1 \to Y_1$ such that $d_1 f_1 = f_0 d_1$.

Recursively construct f_{n+1} using f_n and f_{n-1}. Start with the commutative diagram

$$\begin{tikzcd} X_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, dashed, "\exists f_{n+1}"'] & X_n \arrow[r, "d_n"] \arrow[d, "f_n"] & X_{n-1} \arrow[d, "f_{n-1}"] \\ Y_{n+1} \arrow[r, "d_{n+1}"] & Y_n \arrow[r, "d_n"] & Y_{n-1} \end{tikzcd}$$

The top row is a chain complex, the bottom row is exact. Since $d_n f_n d_{n+1} = f_{n-1} d_n d_{n+1} = 0$, it follows that $\operatorname{im}(f_n d_{n+1}) \subseteq \ker(d_n) = \operatorname{im}(d_{n+1})$. Consider the diagram

$$\begin{tikzcd} X_{n+1} \arrow[d, dashed, "\exists f_{n+1}"'] \arrow[dr, "f_n d_{n+1}"] & & \\ Y_{n+1} \arrow[r, "d_{n+1}"] & \operatorname{im} d_{n+1} \arrow[r] & 0 \end{tikzcd}$$

in which the bottom row is exact. Since X_{n+1} is projective, there exists $f_{n+1} : X_{n+1} \to Y_{n+1}$ such that $d_{n+1} f_{n+1} = f_n d_{n+1}$. This proves Part (1).

(2): Assume that $g : X_\bullet \to Y_\bullet$ is another morphism such that $g\varepsilon = g_0\pi$. We construct a homotopy operator $\{k_i : X_i \to Y_{i+1}\}$ recursively. Start by setting $k_i = 0$ for all $i < 0$.

To construct k_0, start with the commutative diagram

$$\begin{tikzcd} & X_0 \arrow[r, "\varepsilon"] \arrow[d, "f_0 - g_0"] & M \arrow[d, "f"] \\ Y_1 \arrow[r, "d_1"] & Y_0 \arrow[r, "\pi"] & N \end{tikzcd}$$

in which the bottom row is exact. Because $\pi f_0 = \pi g_0 = f\varepsilon$, it follows that $\operatorname{im}(f_0 - g_0) \subseteq \ker(\pi) = \operatorname{im}(d_1)$. Consider the diagram

$$\begin{tikzcd} & X_0 \arrow[dl, dashed, "\exists k_0"'] \arrow[d, "f_0-g_0"] & \\ Y_1 \arrow[r, "d_1"] & \operatorname{im} d_1 \arrow[r] & 0 \end{tikzcd}$$

in which the bottom row is exact. Since X_0 is projective, there exists $k_0 : X_0 \to Y_1$ such that $d_1 k_0 = f_0 - g_0$.

Recursively construct k_n using k_{n-1} and k_{n-2}. Start with the commutative diagram

$$\begin{tikzcd} & X_n \arrow[r, "d_n"] \arrow[d, "f_n-g_n"'] & X_{n-1} \arrow[r, "d_{n-1}"] \arrow[dl, "k_{n-1}"'] \arrow[d, "f_{n-1}-g_{n-1}"] & X_{n-2} \arrow[dl, "k_{n-2}"'] \\ Y_{n+1} \arrow[r, "d_{n+1}"'] & Y_n \arrow[r, "d_n"'] & Y_{n-1} & \end{tikzcd}$$

The top row is a chain complex, the bottom row is exact. Since

$$d_n(f_n - g_n) = (f_{n-1} - g_{n-1})d_n = (d_n k_{n-1} + k_{n-2} d_{n-1})d_n = d_n k_{n-1} d_n$$

it follows that $\operatorname{im}(f_n - g_n - k_{n-1}d_n) \subseteq \ker(d_n) = \operatorname{im}(d_{n+1})$. Consider the diagram

$$\begin{tikzcd} & X_n \arrow[dl, dashed, "\exists k_n"'] \arrow[d, "f_n-g_n-k_{n-1}d_n"] & \\ Y_{n+1} \arrow[r, "d_{n+1}"] & \operatorname{im} d_{n+1} \arrow[r] & 0 \end{tikzcd}$$

in which the bottom row is exact. Since X_n is projective, there exists $k_n : X_n \to Y_{n+1}$ such that $d_{n+1}k_n = f_n - g_n - k_{n-1}d_n$. This proves Part (2). $\square$

1.5. Exercises.

EXERCISE 8.1.7. Suppose f and g are homotopic morphisms from $A_\bullet$ to $B_\bullet$ and $\mathfrak{F}$ is an covariant additive functor on R-modules. Prove that $\mathfrak{F}(f)$ and $\mathfrak{F}(g)$ are homotopic morphisms from $\mathfrak{F}(A_\bullet)$ to $\mathfrak{F}(B_\bullet)$.

EXERCISE 8.1.8. Let $A_\bullet$ be a chain complex. A *contracting homotopy* is a homotopy operator $\{k_i : A_i \to A_{i+1} \mid i \in \mathbb{Z}\}$ such that $d_{n+1}k_n + k_{n-1}d_n$ is equal to the identity function on A_n for each $n \in \mathbb{Z}$. Show that if a contracting homotopy exists, then $\mathrm{H}_n(A_\bullet) = 0$ for all n.

EXERCISE 8.1.9. (Tensor defines an additive functor) Let M be a right R-module. Show that $M \otimes_R (\cdot)$ is an additive functor ${}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$.

EXERCISE 8.1.10. (Hom defines an additive functor) Let M be an R-module. Prove that $\operatorname{Hom}_R(M, \cdot)$ is a covariant additive functor and $\operatorname{Hom}_R(\cdot, M)$ is a contravariant additive functor.

EXERCISE 8.1.11. Assume we are given a commutative diagram

$$\begin{tikzcd}
\arrow[r] & A_n \arrow[r, "f_n"] \arrow[d, "\alpha_n"] & B_n \arrow[r, "g_n"] \arrow[d, "\beta_n"] & C_n \arrow[r, "h_n"] \arrow[d, "\cong"', "\gamma_n"] & A_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\alpha_{n-1}"] & B_{n-1} \arrow[r, "g_{n-1}"] \arrow[d, "\beta_{n-1}"] & C_{n-1} \arrow[r] \arrow[d, "\cong"', "\gamma_{n-1}"] & {} \\
\arrow[r] & X_n \arrow[r, "r_n"] & Y_n \arrow[r, "s_n"] & Z_n \arrow[r, "t_n"] & X_{n-1} \arrow[r, "r_{n-1}"] & Y_{n-1} \arrow[r, "s_{n-1}"] & Z_{n-1} \arrow[r] & {}
\end{tikzcd}$$

where the rows are chain complexes. If the rows are exact sequences and γ_n is an isomorphism for every n, then there is an exact sequence

$$\cdots \to A_n \xrightarrow{\delta_n} X_n \oplus B_n \xrightarrow{\varepsilon_n} Y_n \xrightarrow{\partial_n} A_{n-1} \xrightarrow{\delta_{n-1}} X_{n-1} \oplus B_{n-1} \xrightarrow{\varepsilon_{n-1}} Y_{n-1} \xrightarrow{\partial_{n-1}} \cdots$$

where the maps are defined as follows: $\delta_n = (\alpha_n, f_n)$, $\varepsilon_n = r_n - \beta_n$, and $\partial_n = h_n \gamma_n^{-1} s_n$. The maps γ_n are called *excision isomorphisms* and the resulting long exact sequence is called a *Mayer-Vietoris sequence*. (Hint: This can be proved directly by showing exactness at each term.)

1.6. Left Derived Functors. Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be a covariant additive functor. To $\mathfrak{F}$ we associate a sequence of functors $\mathrm{L}_n \mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$, one for each $n \geq 0$, called the *left derived functors* of $\mathfrak{F}$. For any left R-module M, if $P_\bullet \to M \to 0$ is a projective resolution of M, define $\mathrm{L}_n \mathfrak{F}(M)$ to be the nth homology group of the complex $\mathfrak{F}(P_\bullet)$. In Theorem 8.1.8, we show that this definition does not depend on the choice of $P_\bullet$. Given any R-module homomorphism $\phi : M \to N$, let $P_\bullet \to M$ be a projective resolution of M and $Q_\bullet \to N$ a projective resolution of N. According to Theorem 8.1.7 there is an induced morphism of chain complexes $\phi : P_\bullet \to Q_\bullet$ which is unique up to homotopy equivalence. Applying the functor, we get a morphism of chain complexes $\mathfrak{F}(\phi) : \mathfrak{F}(P_\bullet) \to \mathfrak{F}(Q_\bullet)$. According to Exercise 8.1.7, this morphism depends only on the homotopy class of $\phi : P_\bullet \to Q_\bullet$. This morphism induces a $\mathbb{Z}$-module homomorphism $\mathrm{L}_n \mathfrak{F}(\phi) : \mathrm{L}_n \mathfrak{F}(M) \to \mathrm{L}_n \mathfrak{F}(N)$ for each n. In Theorem 8.1.8, we show that this definition does not depend on the choice of $P_\bullet$ and $Q_\bullet$.

THEOREM 8.1.8. *Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be an additive covariant functor. For each $n \geq 0$ there is an additive covariant functor $\mathrm{L}_n \mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$.*

PROOF. First we show that the definition of left derived functors does not depend on the choice of projective resolution. Let M be an R-module and suppose we are given two projective resolutions $P_\bullet \to M$ and $Q_\bullet \to M$. Starting with the identity map $1 : M \to M$, apply Theorem 8.1.7 (1) from both directions to get morphisms $f : P_\bullet \to Q_\bullet$ and $g : Q_\bullet \to P_\bullet$. Theorem 8.1.7 (2) (from both directions) says $fg \sim 1$ and $gf \sim 1$. By Exercise 8.1.7, $\mathfrak{F}(fg) \sim 1$ and $\mathfrak{F}(gf) \sim 1$. In conclusion, there is an isomorphism

$$\psi(P_\bullet, Q_\bullet) : \mathrm{H}_n(\mathfrak{F}(P_\bullet)) \cong \mathrm{H}_n(\mathfrak{F}(Q_\bullet))$$

which is uniquely determined by the module M and the two resolutions $P_\bullet$ and $Q_\bullet$. The inverse function is $\psi(Q_\bullet, P_\bullet)$.

Secondly, suppose $\phi : M \to N$ is any R-module homomorphism. We show that

$$\mathrm{L}_n \mathfrak{F}(\phi) : \mathrm{L}_n \mathfrak{F}(M) \to \mathrm{L}_n \mathfrak{F}(N)$$

is well defined. Start with a projective resolution $P_\bullet \to M$ of M and a projective resolution $R_\bullet \to N$ of N. In the paragraph preceding this theorem it was shown that ϕ, $P_\bullet$ and $R_\bullet$ uniquely determine a homomorphism

$$\phi(P_\bullet, R_\bullet) : \mathrm{H}_n(\mathfrak{F}(P_\bullet)) \to \mathrm{H}_n(\mathfrak{F}(R_\bullet)).$$

Suppose $Q_\bullet \to M$ is another projective resolution of M, and $S_\bullet \to N$ is another projective resolution of N, and

$$\phi(Q_\bullet, S_\bullet) : \mathrm{H}_n(\mathfrak{F}(Q_\bullet)) \to \mathrm{H}_n(\mathfrak{F}(S_\bullet))$$

is the associated homomorphism. By the first paragraph of this proof, there are isomorphisms $\psi(P_\bullet, Q_\bullet) : \mathrm{H}_n(\mathfrak{F}(P_\bullet)) \cong \mathrm{H}_n(\mathfrak{F}(Q_\bullet))$ and $\psi(R_\bullet, S_\bullet) : \mathrm{H}_n(\mathfrak{F}(R_\bullet)) \cong \mathrm{H}_n(\mathfrak{F}(S_\bullet))$. To show that $\mathrm{L}_n\,\mathfrak{F}(\phi)$ is well defined, it suffices to show that the square

$$\begin{tikzcd}
\mathrm{H}_n(\mathfrak{F}(P_\bullet)) \arrow[r, "\psi(P_\bullet,Q_\bullet)"] \arrow[d, "\phi(P_\bullet,R_\bullet)"'] & \mathrm{H}_n(\mathfrak{F}(Q_\bullet)) \arrow[d, "\phi(Q_\bullet,S_\bullet)"] \\
\mathrm{H}_n(\mathfrak{F}(R_\bullet)) \arrow[r, "\psi(R_\bullet,S_\bullet)"] & \mathrm{H}_n(\mathfrak{F}(S_\bullet))
\end{tikzcd}$$

commutes. The $\mathbb{Z}$-module homomorphisms in this square are uniquely determined by morphisms in the category of chain complexes which make up a square

$$\begin{tikzcd}
P_\bullet \arrow[r, "\alpha"] \arrow[d, "\gamma"'] & Q_\bullet \arrow[d, "\delta"] \\
R_\bullet \arrow[r, "\beta"] & S_\bullet
\end{tikzcd}$$

which is not necessarily commutative. Nevertheless, up to homotopy equivalence, this square is commutative. That is, by Theorem 8.1.7, $\delta\alpha \sim \beta\gamma$.

The rest of the details are left to the reader. $\square$

THEOREM 8.1.9. *Let*

$$\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$$

be a projective resolution of the R-module M. Define $K_0 = \ker \varepsilon$, and for each $n > 0$, define $K_n = \ker d_n$. If $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is an additive covariant functor, then

$$\mathrm{L}_{n+1}\,\mathfrak{F}(M) = \mathrm{L}_{n-i}\,\mathfrak{F}(K_i)$$

for $i = 0, \ldots, n-1$.

PROOF. Notice that for each $\ell \geq 1$

$$\cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \to \cdots \xrightarrow{d_{\ell+1}} P_\ell \xrightarrow{d_\ell} K_{\ell-1} \to 0 \tag{1.1}$$

is a projective resolution for $K_{\ell-1}$. Define a chain complex $P(-\ell)_\bullet$ by truncating $P_\bullet$ and shifting the indices. That is, $P(-\ell)_i = P_{\ell+i}$ and $d(-\ell)_i = d_{\ell+i}$, for each $i \geq 0$. Using this notation, (1.1) becomes

$$\cdots \to P(-\ell)_{n-\ell+1} \xrightarrow{d(-\ell)_{n-\ell+1}} P(-\ell)_{n-\ell} \to \cdots \xrightarrow{d(-\ell)_1} P(-\ell)_0 \xrightarrow{d(-\ell)_0} K_{\ell-1} \to 0 \tag{1.2}$$

By Theorem 8.1.8 we may compute the $(n-\ell+1)$th left derived of $K_{\ell-1}$ using the projective resolution (1.2). For $\ell \geq 1$ the sequences (1.1) and (1.2) agree, hence applying $\mathfrak{F}$ and taking homology yields

$$\mathrm{L}_{n-\ell+1}\,\mathfrak{F}(K_{\ell-1}) = \mathrm{L}_{n+1}\,\mathfrak{F}(M)$$

as required. $\square$

1.7. The Long Exact Sequence.

LEMMA 8.1.10. *Suppose*

$$0 \to A \xrightarrow{\sigma} B \xrightarrow{\tau} C \to 0$$

is a short exact sequence of R-modules, $P_\bullet \to A$ is a projective resolution of A, and $R_\bullet \to C$ is a projective resolution of C. Then there exists a projective resolution $Q_\bullet \to B$ for B and morphisms σ and τ such that

$$0 \to P_\bullet \xrightarrow{\sigma} Q_\bullet \xrightarrow{\tau} R_\bullet \to 0$$

is a short exact sequence of chain complexes. Moreover, for each $n \geq 0$ the short exact sequence

$$0 \to P_n \xrightarrow{\sigma_n} Q_n \xrightarrow{\tau_n} R_n \to 0$$

is split exact.

PROOF. Start with the diagram

$$\begin{array}{ccccccccc} & & P_0 & & & & R_0 & & \\ & & \downarrow{\scriptstyle\alpha} & & & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow{\sigma} & B & \xrightarrow{\tau} & C & \longrightarrow & 0 \\ & & \downarrow & & & & \downarrow & & \\ & & 0 & & & & 0 & & \end{array}$$

where the horizontal row is exact, and P_0 and R_0 are projectives. Because R_0 is projective, there exists $\beta_2 : R_0 \to B$ such that $\tau\beta_2 = \gamma$. Let $\beta_1 = \sigma\alpha$. Let $\beta : P_0 \oplus R_0 \to B$ be defined by $(x,y) \mapsto \beta_1(x) + \beta_2(y)$. Let $Q_0 = P_0 \oplus R_0$ and let σ_0 and τ_0 be the injection and projection maps. The diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_0 & \xrightarrow{\sigma_0} & Q_0 & \xrightarrow{\tau_0} & R_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow{\sigma} & B & \xrightarrow{\tau} & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

commutes and the rows and columns are exact. The Snake Lemma (Theorem 2.5.2) says that

$$0 \to \ker\alpha \xrightarrow{\sigma} \ker\beta \xrightarrow{\tau} \ker\gamma \to 0$$

is a short exact sequence. The proof follows by induction. $\square$

THEOREM 8.1.11. *Suppose*

$$0 \to A \xrightarrow{\sigma} B \xrightarrow{\tau} C \to 0$$

is a short exact sequence of R-modules and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is an additive covariant functor.

(1) There exists a long exact sequence of left derived groups

$$\cdots \xrightarrow{\tau} \mathrm{L}_{n+1}\mathfrak{F}(C) \xrightarrow{\partial} \mathrm{L}_n\mathfrak{F}(A) \xrightarrow{\sigma} \mathrm{L}_n\mathfrak{F}(B) \xrightarrow{\tau} \mathrm{L}_n\mathfrak{F}(C) \xrightarrow{\partial} \mathrm{L}_{n-1}\mathfrak{F}(A) \to \cdots$$
$$\cdots \xrightarrow{\partial} \mathrm{L}_1\mathfrak{F}(A) \xrightarrow{\sigma} \mathrm{L}_1\mathfrak{F}(B) \xrightarrow{\tau} \mathrm{L}_1\mathfrak{F}(C) \xrightarrow{\partial} \mathrm{L}_0\mathfrak{F}(A) \xrightarrow{\sigma} \mathrm{L}_0\mathfrak{F}(B) \xrightarrow{\tau} \mathrm{L}_0\mathfrak{F}(C) \to 0.$$

(2) The functor $\mathrm{L}_0\,\mathfrak{F}$ is right exact.

PROOF. (1): Start with projective resolutions $P_\bullet \to A$ for A and $R_\bullet \to C$ for C. Use Lemma 8.1.10 to construct a projective resolution $Q_\bullet \to B$ for B and morphisms σ and τ such that

$$0 \to P_\bullet \xrightarrow{\sigma} Q_\bullet \xrightarrow{\tau} R_\bullet \to 0$$

is a short exact sequence of chain complexes. Applying the functor,

$$0 \to \mathfrak{F}(P_\bullet) \xrightarrow{\sigma} \mathfrak{F}(Q_\bullet) \xrightarrow{\tau} \mathfrak{F}(R_\bullet) \to 0 \tag{1.3}$$

is a short exact sequence of chain complexes because for each n

$$0 \to P_n \xrightarrow{\sigma_n} Q_n \xrightarrow{\tau_n} R_n \to 0$$

is split exact. The result follows from Theorem 8.1.4 applied to (1.3).

(2): Because the chain complex $A_\bullet$ is zero in degrees $i < 0$, the sequence

$$\mathrm{L}_0\,\mathfrak{F}(A) \to \mathrm{L}_0\,\mathfrak{F}(B) \to \mathrm{L}_0\,\mathfrak{F}(C) \to 0$$

is exact. □

LEMMA 8.1.12. *(The Cube Lemma) Let*

$$\begin{tikzcd}
K \arrow[rrrrr, dashed, "a"] \arrow[dr] \arrow[ddddd, dashed, "b"'] & & & & & L \arrow[dl] \arrow[ddddd, dashed, "d"] \\
& A \arrow[rrr] \arrow[dr, "\alpha"] \arrow[ddd] & & & B \arrow[dl, "\beta"'] \arrow[ddd] & \\
& & E \arrow[r] \arrow[d] & F \arrow[d] & & \\
& & G \arrow[r] & H & & \\
& C \arrow[rrr] \arrow[ur, "\gamma"] & & & D \arrow[ul, "\delta"'] & \\
M \arrow[rrrrr, dashed, "c"] \arrow[ur] & & & & & N \arrow[ul]
\end{tikzcd}$$

be a diagram of R-module homomorphisms. The subdiagram made up of the 8 *inner vertices and* 12 *edges is called a* cube. *Let K, L, M, N be the kernels of $\alpha, \beta, \gamma, \delta$ respectively. If the cube is commutative, then there exist unique homomorphisms a, b, c, d such that the overall diagram commutes.*

PROOF. There is a unique $a : K \to L$ such that the diagram

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, dashed, "a"'] & A \arrow[r, "\alpha"] \arrow[d] & E \arrow[d] \\
0 \arrow[r] & L \arrow[r] & B \arrow[r, "\beta"] & F
\end{tikzcd}$$

commutes. Likewise for $b : K \to M$, $c : M \to N$, and $d : L \to N$. To finish the proof, we show that the square

$$\begin{tikzcd} K \arrow[r, "a"] \arrow[d, "b"'] & L \arrow[d, "d"] \\ M \arrow[r, "c"] & N \end{tikzcd}$$

commutes. Look at the composite homomorphism

$$K \xrightarrow{a} L \xrightarrow{d} N \to D$$

which factors into

$$K \to A \to B \to D$$

which factors into

$$K \to A \to C \to D$$

which factors into

$$K \xrightarrow{b} M \to C \to D$$

which factors into

$$K \xrightarrow{b} M \xrightarrow{c} N \to D.$$

Since $N \to D$ is one-to-one, this proves $da = cb$. □

LEMMA 8.1.13. *Suppose*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "a"] & B \arrow[r, "\tau"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "\sigma'"] & B' \arrow[r, "\tau'"] & C' \arrow[r] & 0 \end{tikzcd}$$

is a commutative diagram of R-modules, with exact rows. Suppose we are given projective resolutions for the four corners $P_\bullet \to A$, $R_\bullet \to C$, $P'_\bullet \to A'$, and $R'_\bullet \to C'$. Then there exist projective resolutions $Q_\bullet \to B$ and $Q'_\bullet \to B'$ and morphisms such that the diagram of chain complexes

$$\begin{tikzcd} 0 \arrow[r] & P_\bullet \arrow[r, "\sigma"] \arrow[d, "a"] & Q_\bullet \arrow[r, "\tau"] \arrow[d, "b"] & R_\bullet \arrow[r] \arrow[d, "c"] & 0 \\ 0 \arrow[r] & P'_\bullet \arrow[r, "\sigma'"] & Q'_\bullet \arrow[r, "\tau'"] & R'_\bullet \arrow[r] & 0 \end{tikzcd}$$

is commutative with exact rows.

PROOF. The morphisms $a : P_\bullet \to P'_\bullet$ and $c : R_\bullet \to R'_\bullet$ exist by Theorem 8.1.7. The projective resolutions $Q_\bullet \to B$, $Q'_\bullet \to B'$ and the remaining morphisms are constructed iteratively. The reader should verify the inductive step, which is similar to the basis step given below.

Start with the commutative diagram

$$\begin{tikzcd}
& P_0 \arrow[dl, "a_0"'] \arrow[dd, "d"] & & & & R_0 \arrow[dl, "c_0"'] \arrow[dd, "f"] \\
P'_0 \arrow[dd, "d'"'] & & & & R'_0 \arrow[dd, "f'"] & \\
& A \arrow[rr, "\sigma"] \arrow[dl, "a"'] & & B \arrow[rr, "\tau"] \arrow[dl, "b"'] & & C \arrow[dl, "c"'] \\
A' \arrow[rr, "\sigma'"] & & B' \arrow[rr, "\tau'"] & & C' &
\end{tikzcd}$$

The maps $d, d', f, f', \tau, \tau'$ are onto and σ, σ' are one-to-one. The R-modules P_0, R_0, P'_0, R'_0 are projective. Because R_0 is projective, there exists $e_2 : R_0 \to B$ such that $\tau e_2 = f$. Let $e_1 = \sigma d$. Because R'_0 is projective, there exists $e'_2 : R'_0 \to B'$ such that $\tau' e'_2 = f'$. Let $e_1 = \sigma' d'$. Consider the diagram

$$\begin{tikzcd}
& & & R_0 \arrow[dll, "e_2"'] \arrow[dl, "f"] \arrow[ddd, "c_0"] \\
& B \arrow[r, "\tau"'] \arrow[d, "b"] & C \arrow[d, "c"] & \\
P'_0 \arrow[r, "\sigma' d'"] & B' \arrow[r, "\tau'"] & C' & \\
& & & R'_0 \arrow[ull, "e'_2"] \arrow[ul, "f'"']
\end{tikzcd}$$

which is not necessarily commutative. The row $P'_0 \to B' \to C'$ is exact. By construction of e_2 and e'_2, it follows that $\tau'(be_2 - e'_2 c_0) = 0$. Since R_0 is projective, there exists $e_3 : R_0 \to P'_0$ such that $\sigma' d' e_3 = be_2 - e'_2 c_0$. Set $Q_0 = P_0 \oplus R_0$ and define $e : Q_0 \to B$ by $(x, y) \mapsto e_1(x) + e_2(y)$. Set $Q'_0 = P'_0 \oplus R'_0$ and define $e' : Q'_0 \to B'$ by $(x, y) \mapsto e'_1(x) + e'_2(y)$. Let σ_0, σ'_0 be the injection maps and let τ_0, τ'_0 be the projection maps. The diagram

$$\begin{tikzcd}
0 \arrow[r] & P_0 \arrow[r, "\sigma_0"] \arrow[d, "d"] & Q_0 \arrow[r, "\tau_0"] \arrow[d, "e"] & R_0 \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & A \arrow[r, "\sigma"] & B \arrow[r, "\tau"] & C \arrow[r] & 0
\end{tikzcd}$$

commutes, the top row is split exact and e is onto. The diagram

$$\begin{tikzcd}
0 \arrow[r] & P'_0 \arrow[r, "\sigma'_0"] \arrow[d, "d'"] & Q'_0 \arrow[r, "\tau'_0"] \arrow[d, "e'"] & R'_0 \arrow[r] \arrow[d, "f'"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\sigma'"] & B' \arrow[r, "\tau'"] & C' \arrow[r] & 0
\end{tikzcd}$$

commutes, the top row is split exact, and e' is onto. Define $b_0 : Q_0 \to Q_0'$ by the assignment $(x,y) \mapsto (a_0(x) + e_3(y), c_0(y))$. The reader should verify that the diagram

$$\begin{tikzcd}
Q_0 \arrow[r, "b_0"] \arrow[d, "e"'] & Q_0' \arrow[d, "e'"] \\
B \arrow[r, "b"] & B'
\end{tikzcd}$$

commutes. Let K, L, M be the kernels of d, e, f respectively. Let K', L', M' be the kernels of d', e', f' respectively. According to Lemma 8.1.12 there are unique homomorphisms connecting the kernels to the rest of the diagram. The overall diagram

$$\begin{tikzcd}
& K \arrow[rr] \arrow[dl] \arrow[dd] & & L \arrow[rr] \arrow[dl] \arrow[dd] & & M \arrow[dl] \arrow[dd] \\
K' \arrow[rr] \arrow[dd] & & L' \arrow[rr] \arrow[dd] & & M' \arrow[dd] & \\
& P_0 \arrow[rr] \arrow[dl] \arrow[dd] & & Q_0 \arrow[rr] \arrow[dl] \arrow[dd] & & R_0 \arrow[dl] \arrow[dd] \\
P_0' \arrow[rr] \arrow[dd] & & Q_0' \arrow[rr] \arrow[dd] & & R_0' \arrow[dd] & \\
& A \arrow[rr] \arrow[dl] & & B \arrow[rr] \arrow[dl] & & C \arrow[dl] \\
A' \arrow[rr] & & B' \arrow[rr] & & C' &
\end{tikzcd}$$

commutes, which completes the basis step. The reader should verify the inductive step and complete the proof. $\square$

THEOREM 8.1.14. *In the long exact sequence of Theorem 8.1.11, the connecting homomorphisms ∂ are natural. That is, given a commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "a"] & B \arrow[r, "\tau"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\sigma'"] & B' \arrow[r, "\tau'"] & C' \arrow[r] & 0
\end{tikzcd}$$

of R-modules, with exact rows, the diagram

$$\begin{tikzcd}
\mathrm{L}_n \mathfrak{F}(C) \arrow[r, "\partial"] \arrow[d, "c"'] & \mathrm{L}_{n-1} \mathfrak{F}(A) \arrow[d, "a"] \\
\mathrm{L}_n \mathfrak{F}(C') \arrow[r, "\partial"] & \mathrm{L}_{n-1} \mathfrak{F}(A')
\end{tikzcd}$$

commutes for all $n \geq 1$.

PROOF. Use Lemma 8.1.13 to get the two short exact sequences of projective resolutions. The split exact rows remain exact after applying $\mathfrak{F}$. Use Theorem 8.1.5. $\square$

1.8. Exercises.

EXERCISE 8.1.12. If $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is an exact additive functor, then for any left R-module A, $\mathrm{L}_i \mathfrak{F}(A) = 0$ for all $i \geq 1$.

EXERCISE 8.1.13. Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be a right exact additive functor.

(1) For any left R-module A, $\mathrm{L}_0 \mathfrak{F}(A) = \mathfrak{F}(A)$.
(2) For any short exact sequence of R-modules $0 \to A \to B \to C \to 0$, there is a long exact sequence of left derived groups

$$\cdots \xrightarrow{\partial} \mathrm{L}_1 \mathfrak{F}(A) \to \mathrm{L}_1 \mathfrak{F}(B) \to \mathrm{L}_1 \mathfrak{F}(C) \xrightarrow{\partial} \mathfrak{F}(A) \to \mathfrak{F}(B) \to \mathfrak{F}(C) \to 0$$

EXERCISE 8.1.14. If P is a projective R-module, and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is a covariant additive functor, then $\mathrm{L}_i \mathfrak{F}(P) = 0$ for all $i \geq 1$.

1.9. Left Derived Groups of an Acyclic Resolution. Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be a right exact covariant additive functor. We say that the left R-module C is $\mathfrak{F}$-acyclic in case $\mathrm{L}_n \mathfrak{F}(C) = 0$ for all $n \geq 1$. The next result says that the left derived groups $\mathrm{L}_n \mathfrak{F}(M)$ may be computed using a resolution of M by $\mathfrak{F}$-acyclic modules.

THEOREM 8.1.15. *Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be a right exact covariant additive functor. Let M be a left R-module and $C_\bullet \to M \to 0$ a resolution of M by $\mathfrak{F}$-acyclic modules. Then*

$$\mathrm{L}_n \mathfrak{F}(M) \cong \mathrm{H}_n(\mathfrak{F}(C_\bullet))$$

for all $n \geq 0$.

PROOF. If we take C_{-1} to be M and take K_j to be $\ker\{d_j : C_j \to C_{j-1}\}$, then there is a short exact sequence

$$0 \to K_j \to C_j \to K_{j-1} \to 0 \tag{1.4}$$

for each $j \geq 0$.

Step 1: Prove that there is an exact sequence

$$0 \to \mathrm{H}_{j+1}(\mathfrak{F}(C_\bullet)) \to \mathfrak{F}K_j \to \mathfrak{F}C_j \to \mathfrak{F}K_{j-1} \to 0$$

for each $j \geq 0$. Since $\mathfrak{F}$ is right exact, (1.4) gives rise to the exact sequence

$$0 \to X_j \to \mathfrak{F}K_j \to \mathfrak{F}C_j \to \mathfrak{F}K_{j-1} \to 0 \tag{1.5}$$

where we take X_j to be the group that makes the sequence exact. The goal is to prove $X_j \cong \mathrm{H}_{j+1}(\mathfrak{F}(C_\bullet))$. The commutative diagram

$$\begin{tikzcd}
C_{j+1} \arrow[rr, "d_{j+1}"] \arrow[dr] & & C_j \\
& K_j \arrow[ur] \arrow[dr] & \\
0 \arrow[ur] & & 0
\end{tikzcd}$$

gives rise to the commutative diagram

$$\begin{tikzcd}
\mathfrak{F}C_{j+1} \arrow[rr, "d_{j+1}"] \arrow[dr] & & \mathfrak{F}C_j \\
& \mathfrak{F}K_j \arrow[ur] \arrow[dr] & \\
& & 0
\end{tikzcd}$$

Using this and (1.5) we see that

$$\mathrm{B}_j(\mathfrak{F}C_\bullet) = \mathrm{im}\{\mathfrak{F}K_j \to \mathfrak{F}C_j\} = \ker\{\mathfrak{F}C_j \to \mathfrak{F}K_{j-1}\}.$$

By Exercise 8.1.2 there is an exact sequence

$$0 \to \mathrm{Z}_j(\mathfrak{F}C_\bullet) \to \mathfrak{F}C_j \to \mathrm{B}_{j-1}(\mathfrak{F}C_\bullet) \to 0. \tag{1.6}$$

Combine (1.5) and (1.6) to get the commutative diagram with exact rows and columns

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{B}_j(\mathfrak{F}C_\bullet) \arrow[r] \arrow[d] & \mathrm{B}_j(\mathfrak{F}C_\bullet) \arrow[r] \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & \mathrm{Z}_j(\mathfrak{F}C_\bullet) \arrow[r] \arrow[d] & \mathfrak{F}C_j \arrow[r] \arrow[d] & \mathrm{B}_{j-1}(\mathfrak{F}C_\bullet) \arrow[d] \\
0 \arrow[r] & X_{j-1} \arrow[r] \arrow[d] & \mathfrak{F}K_{j-1} \arrow[r] \arrow[d] & \mathfrak{F}C_{j-1} \\
& 0 & 0 &
\end{tikzcd}$$

the first column of which shows $\mathrm{H}_j(\mathfrak{F}C_\bullet) \cong X_{j-1}$ for each $j \geq 0$. The reader should verify that Step 1 did not use the fact that the modules C_j are acyclic.

Step 2: By Theorem 8.1.11, the short exact sequence (1.4) gives rise to the long exact sequence

$$\cdots \to \mathrm{L}_{n+1}\mathfrak{F}(C_j) \to \mathrm{L}_{n+1}\mathfrak{F}(K_{j-1}) \xrightarrow{\partial} \mathrm{L}_n\mathfrak{F}(K_j) \to \mathrm{L}_n\mathfrak{F}(C_j) \to \cdots. \tag{1.7}$$

Because the modules C_j are acyclic, the boundary maps in (1.7) are isomorphisms

$$\mathrm{L}_{n+1}\mathfrak{F}(K_{j-1}) \cong \mathrm{L}_n\mathfrak{F}(K_j) \tag{1.8}$$

for all $n \geq 1$ and $j \geq 0$. Iterate (1.8) to get

$$\mathrm{L}_{n+1}\mathfrak{F}(M) = \mathrm{L}_{n+1}\mathfrak{F}(K_{-1}) \cong \mathrm{L}_n\mathfrak{F}(K_0) \cong \mathrm{L}_{n-1}\mathfrak{F}(K_1) \cong \cdots \cong \mathrm{L}_1\mathfrak{F}(K_{n-1}). \tag{1.9}$$

When $n = 0$, (1.7) looks like

$$0 \to \mathrm{L}_1\mathfrak{F}(K_{j-1}) \to \mathfrak{F}K_j \to \mathfrak{F}C_j \to \mathfrak{F}K_{j-1} \to 0. \tag{1.10}$$

Comparing (1.10) and (1.9) with Step 1 we get

$$\mathrm{L}_{j+1}\mathfrak{F}(M) \cong \mathrm{H}_{j+1}(\mathfrak{F}C_\bullet)$$

which finishes the proof. □

1.10. Bifunctors.

DEFINITION 8.1.16. Suppose $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$ are categories, and $\mathfrak{F} : \mathfrak{A} \times \mathfrak{B} \to \mathfrak{C}$ is a correspondence which maps a pair of objects (A,B) to the object $\mathfrak{F}(A,B)$. Let A be an object of $\mathfrak{A}$ and B an object of $\mathfrak{B}$. Denote by $\mathfrak{F}_2(A,\cdot)$ the assignment $B \mapsto \mathfrak{F}(A,B)$ which keeps the first variable fixed. Denote by $\mathfrak{F}_1(\cdot,B)$ the assignment $A \mapsto \mathfrak{F}(A,B)$ which keeps the second variable fixed. We call $\mathfrak{F}$ a *bifunctor* if the following three properties are satisfied.

(1) $\mathfrak{F}_1(\cdot,B)$ is a covariant functor from $\mathfrak{A}$ to $\mathfrak{C}$, and
(2) $\mathfrak{F}_2(A,\cdot)$ is a covariant functor from $\mathfrak{B}$ to $\mathfrak{C}$.
(3) For any pair of morphisms $\phi : A_1 \to A_2$ in $\mathfrak{A}$, $\psi : B_1 \to B_2$ in $\mathfrak{B}$, the diagram

$$\begin{tikzcd}
\mathfrak{F}(A_1,B_1) \arrow[r, "\phi"] \arrow[d, "\psi"'] & \mathfrak{F}(A_2,B_1) \arrow[d, "\psi"] \\
\mathfrak{F}(A_1,B_2) \arrow[r, "\phi"] & \mathfrak{F}(A_2,B_2)
\end{tikzcd}$$

commutes in $\mathfrak{C}$,

A bifunctor may also be contravariant in one or both variables, in which case the reader should make the necessary changes to the commutative square in number (3).

EXAMPLE 8.1.17. Let R be a ring. The assignment $(A,B) \mapsto A \otimes_R B$ is a bifunctor from $\mathfrak{M}_R \times {}_R\mathfrak{M}$ to the category of $\mathbb{Z}$-modules. This bifunctor is right exact covariant in each variable (Lemma 2.3.18).

EXAMPLE 8.1.18. Let R be a ring. The assignment $(A,B) \mapsto \operatorname{Hom}_R(A,B)$ is a bifunctor from ${}_R\mathfrak{M} \times {}_R\mathfrak{M}$ to the category of $\mathbb{Z}$-modules. If the second variable is fixed, the functor is left exact contravariant in the first variable (Proposition 2.4.5). If the first variable is fixed, the functor is left exact covariant in the second variable (Proposition 2.4.5).

LEMMA 8.1.19. *Let $\mathfrak{F} : \mathfrak{M}_R \times \mathfrak{M}_R \to {}_{\mathbb{Z}}\mathfrak{M}$ be a bifunctor which in each variable is covariant right exact and additive. Let M be a fixed R-module. For any short exact sequence of R-modules $0 \to A \to B \to C \to 0$, there is a long exact sequence of groups*

$$\cdots \xrightarrow{\partial} \mathrm{L}_1\mathfrak{F}_1(A,M) \to \mathrm{L}_1\mathfrak{F}_1(B,M) \to \mathrm{L}_1\mathfrak{F}_1(C,M) \xrightarrow{\partial} \mathfrak{F}(A,M) \to \mathfrak{F}(B,M) \to \mathfrak{F}(C,M) \to 0$$

The counterpart of this sequence is exact for the groups $\mathrm{L}_i\mathfrak{F}_2(M,\cdot)$.

PROOF. Follows straight from Exercise 8.1.13. □

THEOREM 8.1.20. *Let $\mathfrak{F} : \mathfrak{M}_R \times \mathfrak{M}_R \to {}_{\mathbb{Z}}\mathfrak{M}$ be a bifunctor which in each variable is covariant right exact and additive. Assume $\mathrm{L}_1\mathfrak{F}_2(P,B) = 0$ and $\mathrm{L}_1\mathfrak{F}_1(A,P) = 0$ for any projective module P and any modules A and B. Then the two left derived groups $\mathrm{L}_n\mathfrak{F}_1(A,B)$ and $\mathrm{L}_n\mathfrak{F}_2(A,B)$ are naturally isomorphic for all R-modules A and B and all $n \geq 0$.*

PROOF. By Exercise 8.1.13 we know $\mathrm{L}_0\mathfrak{F}_1(A,B) = \mathfrak{F}(A,B) = \mathrm{L}_0\mathfrak{F}_2(A,B)$. Let $P_\bullet \to A \to 0$ be a projective resolution for A and $Q_\bullet \to B \to 0$ a projective resolution for B. Define P_{-1} to be A and K_j to be $\ker\{d_j : P_j \to P_{j-1}\}$. Define Q_{-1} to be B and L_j to be $\ker\{d_j : Q_j \to Q_{j-1}\}$.

For each pair (i,j), consider the two short exact sequences

$$0 \to K_i \to P_i \to K_{i-1} \to 0 \tag{1.11}$$

$$0 \to L_j \to Q_j \to L_{j-1} \to 0 \tag{1.12}$$

To sequence (1.11) apply Lemma 8.1.19 three times to to get three exact sequences

$$\mathrm{L}_1\,\mathfrak{F}_1(P_i,L_j) \to \mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_j) \xrightarrow{\partial} \mathfrak{F}(K_i,L_j) \xrightarrow{\alpha} \mathfrak{F}(P_i,L_j) \to \mathfrak{F}(K_{i-1},L_j) \to 0$$

$$\mathrm{L}_1\,\mathfrak{F}_1(P_i,Q_j) \to \mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},Q_j) \xrightarrow{\partial} \mathfrak{F}(K_i,Q_j) \xrightarrow{\beta} \mathfrak{F}(P_i,Q_j) \to \mathfrak{F}(K_{i-1},Q_j) \to 0$$

$$\mathrm{L}_1\,\mathfrak{F}_1(P_i,L_{j-1}) \to \mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_{j-1}) \xrightarrow{\partial} \mathfrak{F}(K_i,L_{j-1}) \xrightarrow{\gamma} \mathfrak{F}(P_i,L_{j-1}) \to \mathfrak{F}(K_{i-1},L_{j-1}) \to 0$$

By assumption $\mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},Q_j) = 0$ because Q_j is projective, hence β is one-to-one. By Exercise 8.1.14, $\mathrm{L}_1\,\mathfrak{F}_1(P_i,L_j) = 0$ and $\mathrm{L}_1\,\mathfrak{F}_1(P_i,L_{j-1}) = 0$ because P_i is projective.

To sequence (1.12) apply Lemma 8.1.19 three times to to get three exact sequences

$$\mathrm{L}_1\,\mathfrak{F}_2(K_i,Q_j) \to \mathrm{L}_1\,\mathfrak{F}_2(K_i,L_{j-1}) \xrightarrow{\partial} \mathfrak{F}(K_i,L_j) \xrightarrow{\sigma} \mathfrak{F}(K_i,Q_j) \to \mathfrak{F}(K_i,L_{j-1}) \to 0$$

$$\mathrm{L}_1\,\mathfrak{F}_2(P_i,Q_j) \to \mathrm{L}_1\,\mathfrak{F}_2(P_i,L_{j-1}) \xrightarrow{\partial} \mathfrak{F}(P_i,L_j) \xrightarrow{\tau} \mathfrak{F}(P_i,Q_j) \to \mathfrak{F}(P_i,L_{j-1}) \to 0$$

$$\mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},Q_j) \to \mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},L_{j-1}) \xrightarrow{\partial} \mathfrak{F}(K_{i-1},L_j) \xrightarrow{\rho} \mathfrak{F}(K_{i-1},Q_j) \to \mathfrak{F}(K_{i-1},L_{j-1}) \to 0$$

By assumption $\mathrm{L}_1\,\mathfrak{F}_2(P_i,L_{j-1}) = 0$ because P_i is projective, hence τ is one-to-one. By Exercise 8.1.14, $\mathrm{L}_1\,\mathfrak{F}_2(K_i,Q_j) = 0$ and $\mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},Q_j) = 0$ because Q_j is projective. The diagram

$$\begin{tikzcd}
 & \mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_j) \arrow[d] & 0 \arrow[d] & \mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_{j-1}) \arrow[d] \\
\mathrm{L}_1\,\mathfrak{F}_2(K_i,L_{j-1}) \arrow[r] & \mathfrak{F}(K_i,L_j) \arrow[r, "\sigma"] \arrow[d, "\alpha"] & \mathfrak{F}(K_i,Q_j)\beta \arrow[r] \arrow[d] & \mathfrak{F}(K_i,L_{j-1}) \arrow[d, "\gamma"] \\
0 \arrow[r] & \mathfrak{F}(P_i,L_j) \arrow[r, "\tau"] \arrow[d] & \mathfrak{F}(P_i,Q_j) \arrow[r] \arrow[d] & \mathfrak{F}(P_i,L_{j-1}) \arrow[d] \\
\mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},L_{j-1}) \arrow[r] & \mathfrak{F}(K_{i-1},L_j) \arrow[r] & \mathfrak{F}(K_{i-1},Q_j) \arrow[r] & \mathfrak{F}(K_{i-1},L_{j-1})
\end{tikzcd}$$

commutes, where the three rows and three columns are the exact sequences from above. Apply the Snake Lemma (Theorem 2.5.2) to see that

$$\mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_{j-1}) \cong \mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},L_{j-1}) \tag{1.13}$$

Since β and τ are one-to-one it follows that

$$\mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_j) = \mathrm{L}_1\,\mathfrak{F}_2(K_i,L_{j-1}) \tag{1.14}$$

Combine (1.14) and (1.13) to get

$$\mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_j) \cong \mathrm{L}_1\,\mathfrak{F}_2(K_i,L_{j-1}) \cong \mathrm{L}_1\,\mathfrak{F}_1(K_i,L_{j-1})$$

Iterate this n times to get

$$\mathrm{L}_1\,\mathfrak{F}_1(A,L_{n-1}) \cong \mathrm{L}_1\,\mathfrak{F}_1(K_{-1},L_{n-1}) \cong \mathrm{L}_1\,\mathfrak{F}_1(K_{n-1},L_{-1}) \cong \mathrm{L}_1\,\mathfrak{F}_1(K_{n-1},B) \tag{1.15}$$

Combine (1.15) with (1.13) and Theorem 8.1.9 to get

$$\begin{aligned} \mathrm{L}_{n+1}\mathfrak{F}_1(A,B) &\cong \mathrm{L}_1\mathfrak{F}_1(K_{n-1},B) \quad \text{(by Theorem 8.1.9)} \\ &\cong \mathrm{L}_1\mathfrak{F}_1(A,L_{n-1}) \quad (1.15) \\ &\cong \mathrm{L}_1\mathfrak{F}_2(A,L_{n-1}) \quad (1.13) \\ &\cong \mathrm{L}_{n+1}\mathfrak{F}_2(A,B) \quad \text{(by Theorem 8.1.9)} \end{aligned}$$

□

2. Cohomology Group Functors

2.1. Cochain Complexes. A *cochain complex* in ${}_R\mathfrak{M}$ is a sequence of R-modules $\{A^i \mid i \in \mathbb{Z}\}$ and homomorphisms $d^i : A^i \to A^{i+1}$ such that $d^{i+1}d^i = 0$ for all $i \in \mathbb{Z}$. The maps d^i are called the *coboundary maps*. The notation $A^\bullet$ denotes a cochain complex. If it is important to reference the coboundary maps, we will write $(A^\bullet, d^\bullet)$. If the modules A^i are specified for some range $n_0 \le i \le n_1$, then it is understood that $A_i = 0$ for $i < n_0$ or $i > n_1$. Let $A^\bullet$ and $B^\bullet$ be cochain complexes. A *morphism of cochain complexes* is a sequence of homomorphisms $f = \{f^i : A^i \to B^i \mid i \in \mathbb{Z}\}$ such that for each i the diagram

$$\begin{tikzcd} A^{i-1} \arrow[r, "d^{i-1}"] \arrow[d, "f^{i-1}"] & A^i \arrow[r, "d^i"] \arrow[d, "f^i"] & A^{i+1} \arrow[d, "f^{i-1}"] \\ B^{i-1} \arrow[r, "d^{i-1}"] & B^i \arrow[r, "d^i"] & B^{i+1} \end{tikzcd}$$

commutes. In this case we write $f : A^\bullet \to B^\bullet$. The reader should verify that the collection of all cochain complexes over R together with morphisms is a category. In some of the exercises listed below the reader is asked to verify many of the important features of this category.

Suppose $A^\bullet$ is a cochain complex and $n \in \mathbb{Z}$. Elements of A^n are called *n-cochains*. The module A^n contains the two submodules

$$\begin{aligned} \mathrm{B}^n(A^\bullet) &= \operatorname{im} d^{n-1}, \quad \text{and} \\ \mathrm{Z}^n(A^\bullet) &= \ker d^n. \end{aligned}$$

Elements of $\mathrm{B}^n(A^\bullet)$ are called *n-coboundaries*. Elements of $\mathrm{Z}^n(A^\bullet)$ are called *n-cocycles*. The condition $d^{i-1}d^i = 0$ translates into $\mathrm{B}^n(A^\bullet) \subseteq \mathrm{Z}^n(A^\bullet)$. The *nth cohomology module* of $A^\bullet$ is defined to be the quotient

$$\mathrm{H}^n(A^\bullet) = \mathrm{Z}^n(A^\bullet)/\mathrm{B}^n(A^\bullet) = \ker d^n / \operatorname{im} d^{n-1}.$$

EXAMPLE 8.2.1. (1) A short exact sequence $0 \to A^0 \to A^1 \to A^2 \to 0$ is a cochain complex. It is understood that the sequence is extended with 0 terms.

(2) If M is an R-module, then an injective resolution

$$0 \to M \to E^0 \to E^1 \to E^2 \to \cdots$$

of M is a cochain complex (see Exercise 2.6.4). It is understood that the sequence is extended with 0 terms.

(3) If $A^\bullet$ is a cochain complex, the reader should verify that the following are equivalent
  (a) $\mathrm{H}^n(A^\bullet) = 0$ for all $n \in \mathbb{Z}$.
  (b) $A^\bullet$ is an exact sequence.

EXAMPLE 8.2.2. As in Example 8.1.2, if $A^\bullet$ is a cochain complex, and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is a covariant additive functor, then $\mathfrak{F}(A^\bullet)$ is a cochain complex. If $A_\bullet$ is a chain complex, and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is a contravariant additive functor, then $\mathfrak{F}(A_\bullet)$ is a cochain complex.

LEMMA 8.2.3. *Let n be an arbitrary integer.*

(1) If $f : A^\bullet \to B^\bullet$ is a morphism of cochain complexes, then the assignment

$$z + \mathrm{B}^n(A^\bullet) \mapsto f^n(z) + \mathrm{B}^n(B^\bullet)$$

defines an R-module homomorphism

$$\mathrm{H}^n(f) : \mathrm{H}^n(A^\bullet) \to \mathrm{H}^n(B^\bullet).$$

(2) The assignment $A^\bullet \mapsto \mathrm{H}^n(A^\bullet)$ defines a functor from the category of cochain complexes to the category of R-modules.

PROOF. Use Lemma 8.1.3. The details are left to the reader. □

2.2. Exercises.

EXERCISE 8.2.1. For the category of cochain complexes, the reader should give appropriate definitions for the following terminology.

(1) The *kernel* of a morphism.
(2) The *cokernel* of a morphism.
(3) The *image* of a morphism.
(4) A *subcochain complex* of a cochain complex and the *quotient* of a cochain complex modulo a subcochain complex.
(5) *monomorphism*, *epimorphism*, and *isomorphism*.
(6) *short exact sequence*.

EXERCISE 8.2.2. Let $A^\bullet$ be a cochain complex. For each $n \in \mathbb{Z}$ there are short exact sequences of R-modules.

(1) $0 \to \mathrm{B}^n(A^\bullet) \to \mathrm{Z}^n(A^\bullet) \to \mathrm{H}^n(A^\bullet) \to 0$
(2) $0 \to \mathrm{Z}^n(A^\bullet) \to A^n \to \mathrm{B}^{n+1}(A^\bullet) \to 0$
(3) $0 \to \mathrm{H}^n(A^\bullet) \to A^n/\mathrm{B}^n(A^\bullet) \to \mathrm{B}^{n+1}(A^\bullet) \to 0$

EXERCISE 8.2.3. Let $A^\bullet$ be a cochain complex. For each $n \in \mathbb{Z}$ there is an exact sequence of R-modules.

$$0 \to \mathrm{H}^n(A^\bullet) \to A^n/\mathrm{B}^n(A^\bullet) \xrightarrow{d^n} \mathrm{Z}^{n+1}(A^\bullet) \to \mathrm{H}^{n+1}(A^\bullet) \to 0$$

EXERCISE 8.2.4. Let $\mathfrak{F}$ be an exact covariant functor from ${}_R\mathfrak{M}$ to ${}_{\mathbb{Z}}\mathfrak{M}$. If $A^\bullet$ is a cochain complex, then $\mathfrak{F}(\mathrm{H}^n(A^\bullet)) \cong \mathrm{H}^n(\mathfrak{F}(A^\bullet))$.

EXERCISE 8.2.5. Let J be an index set and $\{(A_j)^\bullet \mid j \in J\}$ a collection of cochain complexes.

(1) Show that

$$\cdots \xrightarrow{\oplus d^{n-1}} \bigoplus_{j\in J}(A_j)^n \xrightarrow{\oplus d^n} \bigoplus_{j\in J}(A_j)^{n+1} \xrightarrow{\oplus d^{n+1}} \cdots$$

is a cochain complex, which is called the *direct sum cochain complex*.

(2) Show that cohomology commutes with a direct sum. That is

$$\mathrm{H}^n\left(\bigoplus_{j\in J}(A_j)^\bullet\right) \cong \bigoplus_{j\in J}\mathrm{H}^n\left((A_j)^\bullet\right).$$

EXERCISE 8.2.6. Let $\{(A_j)^\bullet, \phi^i_j\}$ be a directed system of cochain complexes for a directed index set I.

(1) Show that
$$\cdots \xrightarrow{\vec{d}^{n-1}} \varinjlim (A_j)^n \xrightarrow{\vec{d}^n} \varinjlim (A_j)^{n+1} \xrightarrow{\vec{d}^{n+1}} \cdots$$
is a cochain complex, which is called the *direct limit cochain complex*.

(2) Show that cohomology commutes with a direct limit. That is
$$\mathrm{H}^n\left(\varinjlim (A_j)^\bullet\right) \cong \varinjlim \mathrm{H}^n\big((A_j)^\bullet\big).$$

2.3. The Long Exact Sequence of Cohomology.

THEOREM 8.2.4. *Let*
$$0 \to A^\bullet \xrightarrow{f} B^\bullet \xrightarrow{g} C^\bullet \to 0$$
be an exact sequence of cochain complexes. Then there is a long exact sequence of cohomology modules
$$\cdots \to \mathrm{H}^n(A^\bullet) \xrightarrow{\mathrm{H}(f)} \mathrm{H}^n(B^\bullet) \xrightarrow{\mathrm{H}(g)} \mathrm{H}^n(C^\bullet) \xrightarrow{\delta^n} \mathrm{H}^{n+1}(A^\bullet) \xrightarrow{\mathrm{H}(f)} \mathrm{H}^{n+1}(B^\bullet) \xrightarrow{\mathrm{H}(g)} \cdots$$

PROOF. Use Theorem 8.1.4. The details are left to the reader. □

THEOREM 8.2.5. *In the context of Theorem 8.2.4, the connecting homomorphism* $\delta^n : \mathrm{H}^n(C^\bullet) \to \mathrm{H}^{n+1}(A^\bullet)$ *is natural. More specifically, if*
$$\begin{tikzcd}
0 \arrow[r] & A^\bullet \arrow[r, "f"] \arrow[d, "\chi"] & B^\bullet \arrow[r, "g"] \arrow[d, "\rho"] & C^\bullet \arrow[r] \arrow[d, "\sigma"] & 0 \\
0 \arrow[r] & D^\bullet \arrow[r, "\phi"] & E^\bullet \arrow[r, "\psi"] & F^\bullet \arrow[r] & 0
\end{tikzcd}$$
is a commutative diagram of cochain complexes with exact rows, then there is a commutative diagram
$$\begin{tikzcd}
\mathrm{H}^n(A^\bullet) \arrow[r, "\mathrm{H}(f)"] \arrow[d, "\mathrm{H}(\chi)"] & \mathrm{H}^n(B^\bullet) \arrow[r, "\mathrm{H}(g)"] \arrow[d, "\mathrm{H}(\rho)"] & \mathrm{H}^n(C^\bullet) \arrow[r, "\delta^n"] \arrow[d, "\mathrm{H}(\sigma)"] & \mathrm{H}^{n+1}(A^\bullet) \arrow[d, "\mathrm{H}(\chi)"] \\
\mathrm{H}^n(D^\bullet) \arrow[r, "\mathrm{H}(\phi)"] & \mathrm{H}^n(E^\bullet) \arrow[r, "\mathrm{H}(\psi)"] & \mathrm{H}^n(F^\bullet) \arrow[r, "\delta^n"] & \mathrm{H}^{n+1}(D^\bullet)
\end{tikzcd}$$
with exact rows for each $n \in \mathbb{Z}$.

PROOF. Use Theorem 8.1.5. The details are left to the reader. □

2.4. Homotopy Equivalence. Let $A^\bullet$ and $B^\bullet$ be cochain complexes. By $\mathrm{Hom}(A^\bullet, B^\bullet)$ we denote the set of all morphisms $f : A^\bullet \to B^\bullet$. For each $i \in \mathbb{Z}$, $f^i : A^i \to B^i$ is an R-module homomorphism. We can turn $\mathrm{Hom}(A^\bullet, B^\bullet)$ into a $\mathbb{Z}$-module. Two morphisms $f, g \in \mathrm{Hom}(A^\bullet, B^\bullet)$ are said to be *homotopic* if there exists a sequence of R-module homomorphisms $\{k^i : A^i \to B^{i-1} \mid i \in \mathbb{Z}\}$ such that $f^n - g^n = d^{n-1}k^n + k^{n+1}d^n$ for each $n \in \mathbb{Z}$. If f and g are homotopic, then we write $f \sim g$ and the sequence $\{k^i\}$ is called a *homotopy operator*. The reader should verify that homotopy equivalence is an equivalence relation on $\mathrm{Hom}(A^\bullet, B^\bullet)$.

THEOREM 8.2.6. *Let $A^\bullet$ and $B^\bullet$ be cochain complexes. For each $n \in \mathbb{Z}$, the functor* $\mathrm{H}^n()$ *is constant on homotopy equivalence classes. In other words, if f and g are homotopic in* $\mathrm{Hom}(A^\bullet, B^\bullet)$*, then $H(f)$ is equal to $H(g)$ in* $\mathrm{Hom}_R(\mathrm{H}^n(A^\bullet), \mathrm{H}^n(B^\bullet))$.

PROOF. Use Theorem 8.1.6. The details are left to the reader. □

THEOREM 8.2.7. *Consider the diagram of R-modules*

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\varepsilon"] \arrow[d, "f"] & X^0 \arrow[r, "d^0"] \arrow[d, dashed, "\exists f^0"] & X^1 \arrow[r, "d^1"] \arrow[d, dashed, "\exists f^1"] & X^2 \arrow[r, "d^2"] \arrow[d, dashed, "\exists f^2"] & \cdots \\ 0 \arrow[r] & N \arrow[r, "\varphi"] & Y^0 \arrow[r, "d^0"] & Y^1 \arrow[r, "d^1"] & Y^2 \arrow[r, "d^2"] & \cdots \end{tikzcd}$$

in which the following are satisfied.

(A) *The top row is an exact sequence.*
(B) *The second row is a cochain complex and each Y_i is an injective R-module.*

Then the following are true.

(1) *There exists a morphism $f : X^\bullet \to Y^\bullet$ which commutes with f on the augmented cochain complexes. That is, $f^0\varepsilon = \varphi f$.*
(2) *The morphism f is unique up to homotopy equivalence.*

PROOF. (1): The morphism f is constructed recursively. To construct f^0, consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\varepsilon"] \arrow[dr, "\varphi f"'] & X^0 \arrow[d, dashed, "\exists f^0"] \\ & & Y^0 \end{tikzcd}$$

with top row exact. Since Y^0 is injective, there exists $f^0 : X^0 \to Y^0$ such that $\varphi f = f^0\varepsilon$.

To construct f^1, start with the commutative diagram

$$\begin{tikzcd} M \arrow[r, "\varepsilon"] \arrow[d, "f"] & X^0 \arrow[r, "d^0"] \arrow[d, "f^0"] & X^1 \arrow[d, dashed, "\exists f^1"] \\ N \arrow[r, "\varphi"] & Y^0 \arrow[r, "d^0"] & Y^1 \end{tikzcd}$$

The top row is exact, the bottom row is a cochain complex. Because $d^0 f^0\varepsilon = d^0\varphi f = 0$, it follows that $\ker(d^0) = \operatorname{im}(\varepsilon) \subseteq \ker(d^0 f^0)$. Consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & X^0/\operatorname{im}(\varepsilon) \arrow[r, "d^0"] \arrow[dr, "d^0 f^0"'] & X^1 \arrow[d, dashed, "\exists f^1"] \\ & & Y^1 \end{tikzcd}$$

with top row exact. Since Y^1 is injective, there exists $f^1 : X^1 \to Y^1$ such that $d^0 f^0 = f^1 d^0$.

Recursively construct f^{n+1} using f^n and f^{n-1}. Start with the commutative diagram

$$\begin{tikzcd} X^{n-1} \arrow[r, "d^{n-1}"] \arrow[d, "f^{n-1}"] & X^n \arrow[r, "d^n"] \arrow[d, "f^n"] & X^{n+1} \arrow[d, dashed, "\exists f^{n+1}"] \\ Y^{n-1} \arrow[r, "d^{n-1}"] & Y^n \arrow[r, "d^n"] & Y^{n+1} \end{tikzcd}$$

The top row is exact, the bottom row is a cochain complex. Since the diagram commutes, $d^n f^n d^{n-1} = d^n d^{n-1} f^{n-1} = 0$. It follows that $\ker(d^n) = \operatorname{im}(d^{n-1}) \subseteq \ker(d^n f^n)$. Consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & X^n/\operatorname{im}(d^{n-1}) \arrow[r, "d^n"] \arrow[dr, "d^{n-1}f^{n-1}"'] & X^{n+1} \arrow[d, dashed, "\exists f^{n+1}"] \\ & & Y^{n+1} \end{tikzcd}$$

with top row exact. Since Y^{n+1} is injective, there exists $f^{n+1} : X^{n+1} \to Y^{n+1}$ such that $d^n f^n = f^{n+1} d^n$. This proves Part (1).

(2): Assume that $g : X^\bullet \to Y^\bullet$ is another morphism such that $g^0\varepsilon = \varphi f$. We construct a homotopy operator $\{k^i : X^i \to Y^{i-1}\}$ recursively. Start by setting $k^i = 0$ for all $i \leq 0$.

To construct k^1, start with the commutative diagram

$$\begin{tikzcd} M \arrow[r, "\varepsilon"] \arrow[d, "f"'] & X^0 \arrow[r, "d^0"] \arrow[d, "f^0-g^0"'] & X^1 \arrow[dl, dashed, "\exists k^1"] \\ N \arrow[r, "\varphi"'] & Y^0 & \end{tikzcd}$$

in which the top row is exact. Because $f^0\varepsilon = g^0\varepsilon = \varphi f$, it follows that $\operatorname{im}(\varepsilon) = \ker(d^0) \subseteq \ker(f^0 - g^0)$. Consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & X^0/\ker(d^0) \arrow[r, "d^0"] \arrow[d, "f^0-g^0"'] & X^1 \arrow[dl, dashed, "\exists k^1"] \\ & Y^0 & \end{tikzcd}$$

in which the top row is exact. Since Y^0 is injective, there exists $k^1 : X^1 \to Y^0$ such that $k^1 d^0 = f_0 - g_0$.

Recursively construct k^{n+1} using k^{n-1} and k^n. Start with the commutative diagram

$$\begin{tikzcd} & X^{n-1} \arrow[r, "d^{n-1}"] \arrow[dl, "k^{n-1}"'] \arrow[d, "f^{n-1}-g^{n-1}"'] & X^n \arrow[r, "d^n"] \arrow[dl, "k^n"'] \arrow[d, "f^n-g^n"'] & X^{n+1} \arrow[dl, dashed, "\exists k^{n+1}"] \\ Y^{n-2} \arrow[r, "d^{n-2}"'] & Y^{n-1} \arrow[r, "d^{n-1}"'] & Y^n & \end{tikzcd}$$

The top row is exact, the bottom row is a cochain complex. Since

$$(f^n - g^n)d^{n-1} = d^{n-1}(f^{n-1} - g^{n-1}) = d^{n-1}(k^n d^{n-1} + d^{n-2}k^{n-1}) = d^{n-1}k^n d^{n-1}$$

it follows that $\ker(d^n) = \operatorname{im}(d^{n-1}) \subseteq \ker(f^n - g^n - d^{n-1}k^n)$. Consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & X^n/\ker(d^n) \arrow[r, "d^n"] \arrow[d, "f^n-g^n-d^{n-1}k^n"'] & X^{n+1} \arrow[dl, dashed, "\exists k^{n+1}"] \\ & Y^n & \end{tikzcd}$$

in which the top row is exact. Since Y^n is injective, there exists $k^{n+1} : X^{n+1} \to Y^n$ such that $k^{n+1}d^n = f^n - g^n - d^{n-1}k^n)$. This proves Part (2). $\square$

2.5. Exercises.

EXERCISE 8.2.7. Suppose f and g are homotopic morphisms from $A^\bullet$ to $B^\bullet$ and $\mathfrak{F}$ is an additive covariant functor on R-modules. Prove that $\mathfrak{F}(f)$ and $\mathfrak{F}(g)$ are homotopic morphisms from $\mathfrak{F}(A^\bullet)$ to $\mathfrak{F}(B^\bullet)$.

EXERCISE 8.2.8. Suppose f and g are homotopic morphisms from $A_\bullet$ to $B_\bullet$ and $\mathfrak{F}$ is an additive contravariant functor on R-modules. Prove that $\mathfrak{F}(f)$ and $\mathfrak{F}(g)$ are homotopic morphisms from $\mathfrak{F}(B_\bullet)$ to $\mathfrak{F}(A_\bullet)$.

2.6. Right Derived Functors. The right derived functors are defined by taking cohomology groups of cochain complexes. The situation for right derived functors is different than that for left derived functors. For right derived functors we consider both covariant and contravariant functors.

2.6.1. *Covariant Functors.* Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$ be an additive covariant functor. To $\mathfrak{F}$ we associate a sequence of functors $\mathrm{R}^n\mathfrak{F} : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$, one for each $n \geq 0$, called the *right derived functors* of $\mathfrak{F}$. For any left R-module M, if $0 \to M \to I^\bullet$ is an injective resolution of M, define $\mathrm{R}^n\mathfrak{F}(M)$ to be the nth cohomology group of the cochain complex $\mathfrak{F}(I^\bullet)$. In Theorem 8.2.8, we show that this definition does not depend on the choice of $I^\bullet$. Given any R-module homomorphism $\phi : M \to N$, let $M \to I^\bullet$ be an injective resolution of M and $N \to J^\bullet$ an injective resolution of N. According to Theorem 8.2.7 there is an induced morphism of cochain complexes $\phi : I^\bullet \to J^\bullet$ which is unique up to homotopy equivalence. Applying the functor $\mathfrak{F}$, we get a morphism of cochain complexes $\mathfrak{F}(\phi) : \mathfrak{F}(I^\bullet) \to \mathfrak{F}(J^\bullet)$. According to Exercise 8.2.7, this morphism preserves the homotopy class of $\phi : I^\bullet \to J^\bullet$. This morphism induces a $\mathbb{Z}$-module homomorphism $\mathrm{R}^n\mathfrak{F}(\phi) : \mathrm{R}^n\mathfrak{F}(M) \to \mathrm{R}^n\mathfrak{F}(N)$ for each n. In Theorem 8.2.8, we show that this definition does not depend on the choice of $I^\bullet$ and $J^\bullet$.

THEOREM 8.2.8. *Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$ be an additive covariant functor. For each $n \geq 0$ there is an additive covariant functor $\mathrm{R}^n\mathfrak{F} : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$.*

PROOF. First we show that the definition of right derived functors does not depend on the choice of injective resolution. Let M be an R-module and suppose we are given two injective resolutions $M \to I^\bullet$ and $M \to J^\bullet$. Starting with the identity map $1 : M \to M$, apply Theorem 8.2.7 (1) from both directions to get morphisms $f : I^\bullet \to J^\bullet$ and $g : J^\bullet \to I^\bullet$. Theorem 8.2.7 (2) (from both directions) says $fg \sim 1$ and $gf \sim 1$. By Exercise 8.2.7, $\mathfrak{F}(fg) \sim 1$ and $\mathfrak{F}(gf) \sim 1$. In conclusion, there is an isomorphism

$$\psi(I^\bullet, J^\bullet) : \mathrm{H}^n(\mathfrak{F}(I^\bullet)) \cong \mathrm{H}^n(\mathfrak{F}(J^\bullet))$$

which is uniquely determined by the module M and the two resolutions $I^\bullet$ and $J^\bullet$. The inverse function is $\psi(J^\bullet, I^\bullet)$.

Secondly, suppose $\phi : M \to N$ is any R-module homomorphism. We show that

$$\mathrm{R}^n\mathfrak{F}(\phi) : \mathrm{R}^n\mathfrak{F}(M) \to \mathrm{R}^n\mathfrak{F}(N)$$

is well defined. Start with an injective resolution $M \to I^\bullet$ of M and an injective resolution $N \to K^\bullet$ of N. In the paragraph preceding this theorem it was shown that ϕ, $I^\bullet$ and $K^\bullet$ uniquely determine a homomorphism

$$\phi(I^\bullet, K^\bullet) : \mathrm{H}^n(\mathfrak{F}(I^\bullet)) \to \mathrm{H}^n(\mathfrak{F}(K^\bullet)).$$

Suppose $M \to J^\bullet$ is another injective resolution of M, and $N \to L^\bullet$ is another injective resolution of N, and

$$\phi(J^\bullet, L^\bullet) : \mathrm{H}^n(\mathfrak{F}(J^\bullet)) \to \mathrm{H}^n(\mathfrak{F}(L^\bullet))$$

is the associated homomorphism. By the first paragraph of this proof, there are isomorphisms $\psi(I^\bullet, J^\bullet) : \mathrm{H}^n(\mathfrak{F}(I^\bullet)) \cong \mathrm{H}^n(\mathfrak{F}(J^\bullet))$ and $\psi(K^\bullet, L^\bullet) : \mathrm{H}^n(\mathfrak{F}(K^\bullet)) \cong \mathrm{H}^n(\mathfrak{F}(L^\bullet))$. To show that $\mathrm{R}^n\mathfrak{F}(\phi)$ is well defined, it suffices to show that the square

$$\begin{tikzcd}
\mathrm{H}^n(\mathfrak{F}(I^\bullet)) \arrow[r, "\psi(I^\bullet,J^\bullet)"] \arrow[d, "\phi(I^\bullet,K^\bullet)"'] & \mathrm{H}^n(\mathfrak{F}(J^\bullet)) \arrow[d, "\phi(J^\bullet,L^\bullet)"] \\
\mathrm{H}^n(\mathfrak{F}(K^\bullet)) \arrow[r, "\psi(K^\bullet,L^\bullet)"] & \mathrm{H}^n(\mathfrak{F}(L^\bullet))
\end{tikzcd}$$

commutes. The $\mathbb{Z}$-module homomorphisms in this square are uniquely determined by morphisms in the category of cochain complexes which make up a square

$$\begin{tikzcd}
I^\bullet \arrow[r, "\alpha"] \arrow[d, "\gamma"'] & J^\bullet \arrow[d, "\delta"] \\
K^\bullet \arrow[r, "\beta"] & L^\bullet
\end{tikzcd}$$

which is not necessarily commutative. Nevertheless, up to homotopy equivalence, this square is commutative. That is, by Theorem 8.2.7, $\delta\alpha \sim \beta\gamma$.

The rest of the details are left to the reader. □

THEOREM 8.2.9. *Let*

$$0 \to M \xrightarrow{\varepsilon} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

be an injective resolution of the R-module M. Define $K^n = \ker d^n$, for each $n \geq 0$. If $\mathfrak{F} : {}_R\mathfrak{M} \to {}_\mathbb{Z}\mathfrak{M}$ is an additive covariant functor, then

$$\mathrm{R}^n\mathfrak{F}(M) = \mathrm{R}^{n-i}\mathfrak{F}(K^i)$$

for $0 \leq i < n$.

PROOF. Suppose $0 \leq \ell < n$. Notice that

$$0 \to K^\ell \to I^\ell \xrightarrow{d^\ell} I^{\ell+1} \xrightarrow{d^{\ell+1}} \cdots \to I^n \xrightarrow{d^n} I^{n+1} \to \cdots \tag{2.1}$$

is an injective resolution for K^ℓ. Define a cochain complex $I(-\ell)^\bullet$ by truncating $I^\bullet$ and shifting the indices. That is, $I(-\ell)^i = I^{\ell+i}$ and $d(-\ell)^i = d^{\ell+i}$, for each $i \geq 0$. Using this notation, (2.1) becomes

$$0 \to K^\ell \to I(-\ell)^0 \xrightarrow{d(-\ell)^0} I(-\ell)^1 \xrightarrow{d(-\ell)^1} \cdots \to I(-\ell)^{n-\ell} \xrightarrow{d(-\ell)^{n-\ell}} I(-\ell)^{n-\ell+1} \to \cdots \tag{2.2}$$

By Theorem 8.2.8 we may compute the $(n-\ell)$th right derived of K^ℓ using the injective resolution (2.2). The sequences (2.1) and (2.2) agree if we ignore the indexes. Applying $\mathfrak{F}$ and taking cohomology yields

$$\mathrm{R}^{n-\ell}\mathfrak{F}(K^\ell) = \mathrm{R}^n\mathfrak{F}(M)$$

as required. □

2.6.2. *Contravariant Functors.* Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be an additive contravariant functor. To $\mathfrak{F}$ we associate a sequence of contravariant functors $\mathrm{R}^n\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$, one for each $n \geq 0$, called the *right derived functors* of $\mathfrak{F}$. For any left R-module M, if

$$\cdots \to P_3 \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$$

is a projective resolution of M, define $\mathrm{R}^n\mathfrak{F}(M)$ to be the nth cohomology group of the cochain complex

$$0 \to \mathfrak{F}P_0 \xrightarrow{\mathfrak{F}d_1} \mathfrak{F}P_1 \xrightarrow{\mathfrak{F}d_2} \mathfrak{F}P_2 \xrightarrow{\mathfrak{F}d_3} \mathfrak{F}P_3 \to \cdots.$$

That is,

$$\mathrm{R}^n\mathfrak{F}(M) = \ker(\mathfrak{F}d_{n+1})/\operatorname{im}(\mathfrak{F}d_n)$$

where the indices are shifted because the contravariant functor reversed the arrows. As in the proof of Theorem 8.1.8, this definition does not depend on the choice of $P_\bullet$. Given any R-module homomorphism $\phi : M \to N$, let $P_\bullet \to M$ be a projective resolution of M and $Q_\bullet \to N$ a projective resolution of N. According to Theorem 8.1.7 there is an induced morphism of chain complexes $\phi : P_\bullet \to Q_\bullet$ which is unique up to homotopy equivalence. Applying the functor $\mathfrak{F}$, we get a morphism of cochain complexes $\mathfrak{F}(\phi) : \mathfrak{F}(Q_\bullet) \to \mathfrak{F}(P_\bullet)$. According to Exercise 8.2.8, this morphism preserves the homotopy class of $\phi : P_\bullet \to Q_\bullet$. This morphism induces a $\mathbb{Z}$-module homomorphism $\mathrm{R}^n\mathfrak{F}(\phi) : \mathrm{R}^n\mathfrak{F}(N) \to \mathrm{R}^n\mathfrak{F}(M)$ for each n. As in the proof of Theorem 8.1.8, this definition does not depend on the choice of $P_\bullet$ and $Q_\bullet$.

THEOREM 8.2.10. *Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be an additive contravariant functor. For each $n \geq 0$ there is an additive contravariant functor $\mathrm{R}^n\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$.*

PROOF. Use Theorem 8.1.8. The details are left to the reader. □

THEOREM 8.2.11. *Let*

$$\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$$

be a projective resolution of the R-module M. Define $K_0 = \ker\varepsilon$, and for each $n > 0$, define $K_n = \ker d_n$. If $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is an additive contravariant functor, then

$$\mathrm{R}^n\mathfrak{F}(M) = \mathrm{R}^{n-i}\mathfrak{F}(K_{i-1})$$

for $0 \leq i < n$.

PROOF. Suppose $0 < \ell \leq n$. Notice that

$$\cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \to \cdots \xrightarrow{d_{\ell+1}} P_\ell \xrightarrow{d_\ell} K_{\ell-1} \to 0 \tag{2.3}$$

is a projective resolution for $K_{\ell-1}$. Define a chain complex $P(-\ell)_\bullet$ by truncating $P_\bullet$ and shifting the indices. That is, $P(-\ell)_i = P_{\ell+i}$ and $d(-\ell)_i = d_{\ell+i}$, for each $i \geq 0$. Using this notation, (2.3) becomes

$$\cdots \to P(-\ell)_{n-\ell+1} \xrightarrow{d(-\ell)_{n-\ell+1}} P(-\ell)_{n-\ell} \to \cdots \xrightarrow{d(-\ell)_1} P(-\ell)_0 \xrightarrow{d(-\ell)_0} K_{\ell-1} \to 0 \tag{2.4}$$

By Theorem 8.2.10, we may compute the $(n-\ell)$th right derived group of $K_{\ell-1}$ using the projective resolution (2.4). The sequences (2.3) and (2.4) agree if we ignore the indexes. Applying $\mathfrak{F}$ and taking cohomology yields

$$\mathrm{R}^{n-\ell}\mathfrak{F}(K_{\ell-1}) = \mathrm{R}^n\mathfrak{F}(M)$$

as required. □

2.7. The Long Exact Sequence.

LEMMA 8.2.12. *Suppose*

$$0 \to A \xrightarrow{\sigma} B \xrightarrow{\tau} C \to 0$$

is a short exact sequence of R-modules, $A \to I^\bullet$ is an injective resolution of A, and $C \to K^\bullet$ is an injective resolution of C. Then there exists an injective resolution $B \to J^\bullet$ for B and morphisms σ and τ such that

$$0 \to I^\bullet \xrightarrow{\sigma} J^\bullet \xrightarrow{\tau} K^\bullet \to 0$$

is a short exact sequence of cochain complexes. Moreover, for each $n \geq 0$ the short exact sequence

$$0 \to I^n \xrightarrow{\sigma_n} J^n \xrightarrow{\tau_n} K^n \to 0$$

is split exact.

PROOF. Start with the diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "\alpha"] & B \arrow[r, "\tau"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
 & I^0 & & K^0 &
\end{tikzcd}$$

where the horizontal row is exact, and I^0 and K^0 are injectives. Because I^0 is injective, there exists $\beta^1 : B \to I^0$ such that $\beta^1\sigma = \alpha$. Let $\beta^2 = \gamma\tau$. Let $\beta : B \to I^0 \oplus K^0$ be defined by $x \mapsto (\beta^1(x), \beta^2(x))$. Let $J^0 = I^0 \oplus K^0$ and let σ^0 and τ^0 be the injection and projection maps. The diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "\alpha"] & B \arrow[r, "\tau"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & I^0 \arrow[r, "\sigma^0"] & J^0 \arrow[r, "\tau^0"] & K^0 \arrow[r] & 0
\end{tikzcd}$$

commutes and the rows are exact. Since α and γ are one-to-one and the diagram commutes, β is one-to-one. The Snake Lemma (Theorem 2.5.2) says that

$$0 \to \operatorname{coker}\alpha \xrightarrow{\sigma} \operatorname{coker}\beta \xrightarrow{\tau} \operatorname{coker}\gamma \to 0$$

is a short exact sequence. The proof follows by induction. □

THEOREM 8.2.13. *Suppose*

$$0 \to A \xrightarrow{\sigma} B \xrightarrow{\tau} C \to 0$$

is a short exact sequence of R-modules and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is an additive functor.

(1) If $\mathfrak{F}$ is covariant, then there exists a long exact sequence of right derived groups

$$0 \to \mathrm{R}^0\mathfrak{F}(A) \xrightarrow{\sigma} \mathrm{R}^0\mathfrak{F}(B) \xrightarrow{\tau} \mathrm{R}^0\mathfrak{F}(C) \xrightarrow{\delta^0} \mathrm{R}^1\mathfrak{F}(A) \xrightarrow{\sigma} \mathrm{R}^1\mathfrak{F}(B) \xrightarrow{\tau} \mathrm{R}^1\mathfrak{F}(C) \xrightarrow{\delta^1} \cdots$$

$$\cdots \xrightarrow{\tau} \mathrm{R}^{n-1}\mathfrak{F}(C) \xrightarrow{\delta^{n-1}} \mathrm{R}^n\mathfrak{F}(A) \xrightarrow{\sigma} \mathrm{R}^n\mathfrak{F}(B) \xrightarrow{\tau} \mathrm{R}^n\mathfrak{F}(C) \xrightarrow{\delta^n} \mathrm{R}^{n+1}\mathfrak{F}(A) \to \cdots.$$

(2) *If $\mathfrak{F}$ is contravariant, then there exists a long exact sequence of right derived groups*

$$\begin{aligned} 0 \to \mathrm{R}^0\,\mathfrak{F}(C) \xrightarrow{\tau} \mathrm{R}^0\,\mathfrak{F}(B) \xrightarrow{\sigma} \mathrm{R}^0\,\mathfrak{F}(A) \xrightarrow{\delta^0} \mathrm{R}^1\,\mathfrak{F}(C) \xrightarrow{\tau} \mathrm{R}^1\,\mathfrak{F}(B) \xrightarrow{\sigma} \mathrm{R}^1\,\mathfrak{F}(A) \xrightarrow{\delta^1} \cdots \\ \cdots \xrightarrow{\sigma} \mathrm{R}^{n-1}\,\mathfrak{F}(A) \xrightarrow{\delta^{n-1}} \mathrm{R}^n\,\mathfrak{F}(C) \xrightarrow{\tau} \mathrm{R}^n\,\mathfrak{F}(B) \xrightarrow{\sigma} \mathrm{R}^n\,\mathfrak{F}(A) \xrightarrow{\delta^n} \mathrm{R}^{n+1}\,\mathfrak{F}(C) \to \cdots. \end{aligned}$$

(3) *In either case, the functor $\mathrm{R}^0\,\mathfrak{F}$ is left exact.*

PROOF. (1): Start with injective resolutions $A \to I^\bullet$ for A and $C \to K^\bullet$ for C. Use Lemma 8.2.12 to construct an injective resolution $B \to J^\bullet$ for B and morphisms σ and τ such that

$$0 \to I^\bullet \xrightarrow{\sigma} J^\bullet \xrightarrow{\tau} K^\bullet \to 0$$

is a short exact sequence of cochain complexes. Applying the functor,

$$0 \to \mathfrak{F}(I^\bullet) \xrightarrow{\sigma} \mathfrak{F}(J^\bullet) \xrightarrow{\tau} \mathfrak{F}(K^\bullet) \to 0 \tag{2.5}$$

is a short exact sequence of cochain complexes because for each n

$$0 \to I^n \xrightarrow{\sigma_n} J^n \xrightarrow{\tau_n} K^n \to 0$$

is split exact. The result follows from Theorem 8.2.4 applied to (2.5).

(2): Start with projective resolutions $P_\bullet \to A$ for A and $R_\bullet \to C$ for C. Use Lemma 8.1.10 to construct a projective resolution $Q_\bullet \to B$ for B and morphisms σ and τ such that

$$0 \to P_\bullet \xrightarrow{\sigma} Q_\bullet \xrightarrow{\tau} R_\bullet \to 0$$

is a short exact sequence of chain complexes. Applying the functor,

$$0 \to \mathfrak{F}(R_\bullet) \xrightarrow{\sigma} \mathfrak{F}(Q_\bullet) \xrightarrow{\tau} \mathfrak{F}(P_\bullet) \to 0 \tag{2.6}$$

is a short exact sequence of cochain complexes because for each n

$$0 \to P_n \xrightarrow{\sigma_n} Q_n \xrightarrow{\tau_n} R_n \to 0$$

is split exact. The result follows from Theorem 8.2.4 applied to (2.6).

(3): This follows from Theorem 8.2.4. The cochain complex $A^\bullet$ is zero in degrees $i < 0$, hence the sequence

$$0 \to \mathrm{R}^0\,\mathfrak{F}(A) \to \mathrm{R}^0\,\mathfrak{F}(B) \to \mathrm{R}^0\,\mathfrak{F}(C)$$

is exact. $\square$

LEMMA 8.2.14. *(The Cube Lemma) Let*

$$\begin{tikzcd}
A \arrow[rrrrr] \arrow[dr, "\alpha"] \arrow[ddddd] &&&&& B \arrow[dl, "\beta"'] \arrow[ddddd] \\
& E \arrow[rrr] \arrow[dr] \arrow[ddd] &&& F \arrow[dl] \arrow[ddd] & \\
&& K \arrow[r, dashed, "a"] \arrow[d, dashed, "b"'] & L \arrow[d, dashed, "d"] && \\
&& M \arrow[r, dashed, "c"] & N && \\
& G \arrow[rrr] \arrow[ur] &&& H \arrow[ul] & \\
C \arrow[rrrrr] \arrow[ur, "\gamma"] &&&&& D \arrow[ul, "\delta"']
\end{tikzcd}$$

be a diagram of R-module homomorphisms. Let K,L,M,N be the cokernels of $\alpha,\beta,\gamma,\delta$ respectively. If the outer cube is commutative, then there exist unique homomorphisms a,b,c,d such that the overall diagram commutes.

PROOF. There is a unique $a : K \to L$ such that the diagram

$$\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d] & E \arrow[r] \arrow[d] & K \arrow[r] \arrow[d, dashed, "a"'] & 0 \\
B \arrow[r, "\beta"] & F \arrow[r] & L \arrow[r] & 0
\end{tikzcd}$$

commutes. Likewise for $b : K \to M$, $c : M \to N$, and $d : L \to N$. To finish the proof, we show that the square

$$\begin{tikzcd}
K \arrow[r, "a"] \arrow[d, "b"'] & L \arrow[d, "d"] \\
M \arrow[r, "c"] & N
\end{tikzcd}$$

commutes. Look at the composite homomorphism

$$E \to K \xrightarrow{a} L \xrightarrow{d} N$$

which factors into

$$E \to F \to L \xrightarrow{d} N$$

which factors into

$$E \to F \to H \to N$$

which factors into

$$E \to G \to H \to N$$

which factors into

$$E \to G \to M \xrightarrow{c} N$$

which factors into

$$E \to K \xrightarrow{b} M \xrightarrow{c} N.$$

Since $E \to K$ is onto, this proves $da = cb$. □

LEMMA 8.2.15. *Suppose*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "a"] & B \arrow[r, "\tau"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\sigma'"] & B' \arrow[r, "\tau'"] & C' \arrow[r] & 0
\end{tikzcd}$$

is a commutative diagram of R*-modules, with exact rows. Suppose we are given injective resolutions for the four corners* $A \to I^{\bullet}$, $C \to K^{\bullet}$, $A' \to I'^{\bullet}$, *and* $C' \to K'^{\bullet}$. *Then there exist injective resolutions* $B \to J^{\bullet}$ *and* $B' \to J'^{\bullet}$ *and morphisms such that the diagram of cochain complexes*

$$\begin{tikzcd}
0 \arrow[r] & I^{\bullet} \arrow[r, "\sigma"] \arrow[d, "a"] & J^{\bullet} \arrow[r, "\tau"] \arrow[d, "b"] & K^{\bullet} \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & I'^{\bullet} \arrow[r, "\sigma'"] & J'^{\bullet} \arrow[r, "\tau'"] & K'^{\bullet} \arrow[r] & 0
\end{tikzcd}$$

is commutative with exact rows.

PROOF. The morphisms $a : I^{\bullet} \to I'^{\bullet}$ and $c : K^{\bullet} \to K'^{\bullet}$ exist by Theorem 8.2.7. The injective resolutions $B \to J^{\bullet}$, $B' \to J'^{\bullet}$ and the remaining morphisms are constructed iteratively. The reader should verify the inductive step, which is similar to the basis step given below.

Start with the commutative diagram

$$\begin{tikzcd}
& A \arrow[rr, "\sigma"] \arrow[dl, "a"'] \arrow[dd, "d"] & & B \arrow[rr, "\tau"] \arrow[dl, "b"'] & & C \arrow[dl, "c"'] \arrow[dd, "f"] \\
A' \arrow[rr, "\sigma'"] \arrow[dd, "d'"'] & & B' \arrow[rr, "\tau'"] & & C' \arrow[dd, "f'"] & \\
& I^0 \arrow[dl, "a^0"] & & & & K^0 \arrow[dl, "c^0"] \\
I'^0 & & & & K'^0 &
\end{tikzcd}$$

The maps $d, d', f, f', \sigma, \sigma'$ are one-to-one and τ, τ' are onto. The R-modules I^0, K^0, I'^0, K'^0 are injective. Because I^0 is injective, there exists $e^1 : B \to I^0$ such that $e^1\sigma = d$. Let $e^2 = f\tau$. Because I'^0 is injective, there exists $e'^1 : B' \to I'^0$ such that $e'^1\sigma' = d'$. Let $e'^2 = f'\tau'$. The diagram

$$\begin{tikzcd}
I^0 \arrow[ddd, "a^0"'] & & & \\
& A \arrow[ul, "d"] \arrow[r, "\sigma"] \arrow[d, "a"] & B \arrow[ull, "e^1"'] \arrow[r, "f\tau"] \arrow[d, "b"] & K^0 \\
& A' \arrow[r, "\tau'"] \arrow[dl, "d'"'] & B' \arrow[dll, "e'^1"] & \\
I'^0 & & &
\end{tikzcd}$$

is not necessarily commutative. The row $A \to B \to K^0$ is exact. Notice that

$$\begin{aligned}(a^0e^1 - e^1_{\prime}b)\sigma &= a^0d - e^1_{\prime}\tau_{\prime}a\\ &= a^0d - d_{\prime}a\\ &= 0\end{aligned}$$

so $(a^0e^1 - e^1_{\prime}b) : B/A \to I^0_{\prime}$ is well defined. Since $I^0_{\prime}$ is injective, there exists $e^3 : K^0 \to I^0_{\prime}$ such that $e^3 f\tau = a^0e^1 - e^1_{\prime}b$. Set $J^0 = I^0 \oplus K^0$ and define $e : B \to J^0$ by $x \mapsto (e^1(x), e^2(x))$. Set $J^0_{\prime} = I^0_{\prime} \oplus K^0_{\prime}$ and define $e_{\prime} : B_{\prime} \to J^0_{\prime}$ by $x \mapsto (e^1_{\prime}(x), e^2_{\prime}(y))$. Let $\sigma^0, \sigma^0_{\prime}$ be the injection maps and let $\tau^0, \tau^0_{\prime}$ be the projection maps. The diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "d"] & B \arrow[r, "\tau"] \arrow[d, "e"] & C \arrow[r] \arrow[d, "f"] & 0\\
0 \arrow[r] & I^0 \arrow[r, "\sigma^0"] & J^0 \arrow[r, "\tau^0"] & K^0 \arrow[r] & 0
\end{tikzcd}$$

commutes, the top row is split exact and e is one-to-one. The diagram

$$\begin{tikzcd}
0 \arrow[r] & A_{\prime} \arrow[r, "\sigma_{\prime}"] \arrow[d, "d_{\prime}"] & B_{\prime} \arrow[r, "\tau_{\prime}"] \arrow[d, "e_{\prime}"] & C_{\prime} \arrow[r] \arrow[d, "f_{\prime}"] & 0\\
0 \arrow[r] & I^0_{\prime} \arrow[r, "\sigma^0_{\prime}"] & J^0_{\prime} \arrow[r, "\tau^0_{\prime}"] & K^0_{\prime} \arrow[r] & 0
\end{tikzcd}$$

commutes, the top row is split exact, and $e_{\prime}$ is one-to-one. Define $b^0 : J^0 \to J^0_{\prime}$ by the assignment $(x,y) \mapsto (a^0(x) - e^3(y), c^0(y))$. The reader should verify that the diagram

$$\begin{tikzcd}
B \arrow[r, "b"] \arrow[d, "e"'] & B_{\prime} \arrow[d, "e_{\prime}"]\\
J^0 \arrow[r, "b^0"] & J^0_{\prime}
\end{tikzcd}$$

commutes. Let K, L, M be the cokernels of d, e, f respectively. Let $K_{\prime}, L_{\prime}, M_{\prime}$ be the cokernels of $d_{\prime}, e_{\prime}, f_{\prime}$ respectively. According to Lemma 8.2.14 there are unique homomorphisms connecting the cokernels to the rest of the diagram. The overall diagram

$$
\begin{tikzcd}
& A \arrow[rr] \arrow[dl] \arrow[dd] & & B \arrow[rr] \arrow[dl] \arrow[dd] & & C \arrow[dl] \arrow[dd] \\
A_\prime \arrow[rr] \arrow[dd] & & B_\prime \arrow[rr] \arrow[dd] & & C_\prime \arrow[dd] & \\
& I^0 \arrow[rr] \arrow[dl] \arrow[dd] & & J^0 \arrow[rr] \arrow[dl] \arrow[dd] & & K^0 \arrow[dl] \arrow[dd] \\
I^0_\prime \arrow[rr] \arrow[dd] & & J^0_\prime \arrow[rr] \arrow[dd] & & K^0_\prime \arrow[dd] & \\
& K \arrow[rr] \arrow[dl] & & L \arrow[rr] \arrow[dl] & & M \arrow[dl] \\
K_\prime \arrow[rr] & & L_\prime \arrow[rr] & & M_\prime &
\end{tikzcd}
$$

commutes, which completes the basis step. The reader should verify the inductive step and complete the proof. □

THEOREM 8.2.16. *In the long exact sequence of Theorem 8.2.13, the connecting homomorphisms δ are natural. That is, given a commutative diagram*

$$
\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "a"] & B \arrow[r, "\tau"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A_\prime \arrow[r, "\sigma_\prime"] & B_\prime \arrow[r, "\tau_\prime"] & C_\prime \arrow[r] & 0
\end{tikzcd}
$$

of R-modules, with exact rows the following are true.

(1) *If $\mathfrak{F}$ is covariant, the diagram*

$$
\begin{tikzcd}
\mathrm{R}^n\,\mathfrak{F}(C) \arrow[r, "\delta^n"] \arrow[d, "c"'] & \mathrm{R}^{n+1}\,\mathfrak{F}(A) \arrow[d, "a"] \\
\mathrm{R}^n\,\mathfrak{F}(C_\prime) \arrow[r, "\delta^n"] & \mathrm{R}^{n+1}\,\mathfrak{F}(A_\prime)
\end{tikzcd}
$$

commutes for all $n \geq 0$.

(2) *If $\mathfrak{F}$ is contravariant, the diagram*

$$
\begin{tikzcd}
\mathrm{R}^n\,\mathfrak{F}(A) \arrow[r, "\delta^n"] \arrow[d, "c"'] & \mathrm{R}^{n+1}\,\mathfrak{F}(C) \arrow[d, "a"] \\
\mathrm{R}^n\,\mathfrak{F}(A_\prime) \arrow[r, "\delta^n"] & \mathrm{R}^{n+1}\,\mathfrak{F}(C_\prime)
\end{tikzcd}
$$

commutes for all $n \geq 0$.

PROOF. (1): Use Lemma 8.2.15 to get the two short exact sequences of injective resolutions. The split exact rows remain exact after applying $\mathfrak{F}$. Use Theorem 8.2.5.

(2) Use Lemma 8.1.13 to get the two short exact sequences of projective resolutions. The split exact rows remain exact after applying $\mathfrak{F}$. Use Theorem 8.2.5. $\square$

2.8. Exercises.

EXERCISE 8.2.9. If $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is an exact covariant functor, then for any left R-module A, $\mathrm{R}^i\mathfrak{F}(A) = 0$ for all $i \geq 1$.

EXERCISE 8.2.10. If $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is an exact contravariant functor, then for any left R-module A, $\mathrm{R}^i\mathfrak{F}(A) = 0$ for all $i \geq 1$.

EXERCISE 8.2.11. Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be a left exact covariant functor.

(1) For any left R-module A, $\mathrm{R}^0\mathfrak{F}(A) = \mathfrak{F}(A)$.
(2) For any short exact sequence of R-modules $0 \to A \to B \to C \to 0$, there is a long exact sequence of cohomology groups
$$0 \to \mathfrak{F}(A) \to \mathfrak{F}(B) \to \mathfrak{F}(C) \xrightarrow{\delta^0} \mathrm{R}^1\mathfrak{F}(A) \to \mathrm{R}^1\mathfrak{F}(B) \to \mathrm{R}^1\mathfrak{F}(C) \xrightarrow{\delta^1} \cdots$$

EXERCISE 8.2.12. Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be a left exact contravariant functor.

(1) For any left R-module A, $\mathrm{R}^0\mathfrak{F}(A) = \mathfrak{F}(A)$.
(2) For any short exact sequence of R-modules $0 \to A \to B \to C \to 0$, there is a long exact sequence of cohomology groups
$$0 \to \mathfrak{F}(C) \to \mathfrak{F}(B) \to \mathfrak{F}(A) \xrightarrow{\delta^0} \mathrm{R}^1\mathfrak{F}(C) \to \mathrm{R}^1\mathfrak{F}(B) \to \mathrm{R}^1\mathfrak{F}(A) \xrightarrow{\delta^1} \cdots$$

EXERCISE 8.2.13. If E is an injective R-module, and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is a covariant functor, then $\mathrm{R}^i\mathfrak{F}(E) = 0$ for all $i \geq 1$.

EXERCISE 8.2.14. If P is a projective R-module, and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is a contravariant functor, then $\mathrm{R}^i\mathfrak{F}(P) = 0$ for all $i \geq 1$.

2.9. Right Derived Groups of an Acyclic Resolution. Let $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ be a left exact additive functor. We say that the left R-module C is $\mathfrak{F}$-acyclic in case $\mathrm{R}^n\mathfrak{F}(C) = 0$ for all $n \geq 1$. Theorem 8.2.17 says that the right derived groups $\mathrm{R}^n\mathfrak{F}(M)$ may be computed using a resolution of M by $\mathfrak{F}$-acyclic modules.

THEOREM 8.2.17. *Let M be a left R-module and $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ a left exact functor.*

(1) If $\mathfrak{F}$ is covariant and $0 \to M \to C^\bullet$ is a resolution of M by $\mathfrak{F}$-acyclic modules, then
$$\mathrm{R}^n\mathfrak{F}(M) \cong \mathrm{H}^n(\mathfrak{F}(C^\bullet))$$
for all $n \geq 0$.
(2) If $\mathfrak{F}$ is contravariant and $C_\bullet \to M \to 0$ is a resolution of M by $\mathfrak{F}$-acyclic modules, then
$$\mathrm{R}^n\mathfrak{F}(M) \cong \mathrm{H}^n(\mathfrak{F}(C_\bullet))$$
for all $n \geq 0$.

PROOF. (1): Define K^j to be $\ker\{d^j : C^j \to C^{j+1}\}$, then $K^0 = M$ and there is a short exact sequence

$$0 \to K^j \to C^j \to K^{j+1} \to 0 \tag{2.7}$$

for each $j \geq 0$.

Step 1: There is an exact sequence
$$0 \to \mathfrak{F}K^j \to \mathfrak{F}C^j \to \mathfrak{F}K^{j+1} \to \mathrm{H}^{j+1}(\mathfrak{F}(C_\bullet)) \to 0$$

for each $j \geq 0$. Since $\mathfrak{F}$ is left exact, (2.7) gives rise to the exact sequence

$$0 \to \mathfrak{F}K^j \to \mathfrak{F}C^j \to \mathfrak{F}K^{j+1} \to X^j \to 0$$

where we take X^j to be the group that makes the sequence exact. The goal is to prove $X^j \cong \mathrm{H}^{j+1}(\mathfrak{F}(C^\bullet))$. Apply the left exact functor $\mathfrak{F}$ to the exact sequence $0 \to K^j \to C^j \to C^{j+1}$ to get the exact sequence $0 \to \mathfrak{F}K^j \to \mathfrak{F}C^j \to \mathfrak{F}C^{j+1}$. This shows $\mathfrak{F}K^j = \mathrm{Z}^j(\mathfrak{F}C^\bullet)$ for all $j \geq 0$. The commutative diagram

$$\begin{tikzcd}
C^j \arrow[rr, "d^j"] \arrow[dr] & & C^{j+1} \\
& K^{j+1} \arrow[ur] \arrow[dr] & \\
0 \arrow[ur] & & 0
\end{tikzcd}$$

gives rise to the commutative diagram

$$\begin{tikzcd}
\mathfrak{F}C^j \arrow[rr, "d^j"] \arrow[dr] & & \mathfrak{F}C^{j+1} \\
& \mathfrak{F}K^{j+1} \arrow[ur] & \\
0 \arrow[ur] & &
\end{tikzcd}$$

Using this we see that $\mathrm{B}^j(\mathfrak{F}C^\bullet) \subseteq \operatorname{im}\{\mathfrak{F}K^{j+1} \to \mathfrak{F}C^{j+1}\}$. Therefore the diagram

$$\begin{tikzcd}
\mathfrak{F}C^j \arrow[rr] \arrow[dr] & & \mathfrak{F}K^{j+1} \arrow[r] & X^j \arrow[r] & 0 \\
& \mathrm{B}^{j+1}(\mathfrak{F}C^\bullet) \arrow[ur] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

commutes. But $\mathfrak{F}K^{j+1} = \mathrm{Z}^{j+1}(\mathfrak{F}C^\bullet)$, which shows $X^j \cong \mathrm{H}^{j+1}(\mathfrak{F}C^\bullet)$ for each $j \geq 0$. The reader should verify that Step 1 did not use the fact that the modules C^j are acyclic.

Step 2: By Theorem 8.2.13, the short exact sequence (2.7) gives rise to the long exact sequence

$$\cdots \to \mathrm{R}^n\,\mathfrak{F}(C^j) \to \mathrm{R}^n\,\mathfrak{F}(K^{j+1}) \xrightarrow{\delta^n} \mathrm{R}^{n+1}\,\mathfrak{F}(K^j) \to \mathrm{R}^{n+1}\,\mathfrak{F}(C^j) \to \cdots. \tag{2.8}$$

Because the modules C^j are acyclic, the connecting homomorphisms in (2.8) are isomorphisms

$$\mathrm{R}^n\,\mathfrak{F}(K^{j+1}) \cong \mathrm{R}^{n+1}\,\mathfrak{F}(K^j) \tag{2.9}$$

for all $n \geq 1$ and $j \geq 0$. Iterate (2.9) to get

$$\mathrm{R}^{n+1}\,\mathfrak{F}(M) = \mathrm{R}^{n+1}\,\mathfrak{F}(K^0) \cong \mathrm{R}^n\,\mathfrak{F}(K^1) \cong \mathrm{R}^{n-1}\,\mathfrak{F}(K^2) \cong \cdots \cong \mathrm{R}^1\,\mathfrak{F}(K^n). \tag{2.10}$$

When $n = 0$, (2.8) looks like

$$0 \to \mathfrak{F}K^j \to \mathfrak{F}C^j \to \mathfrak{F}K^{j+1} \xrightarrow{\delta^0} \mathrm{R}^1\,\mathfrak{F}K^j \to 0. \tag{2.11}$$

Comparing (2.11) and (2.10) with Step 1 we get

$$\mathrm{R}^{j+1}\,\mathfrak{F}(M) \cong \mathrm{H}^{j+1}(\mathfrak{F}C^\bullet)$$

which finishes the proof of Part (1).

(2): Assume $\mathfrak{F}$ is contravariant and

$$\cdots \xrightarrow{d_3} C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \to M \to 0$$

is a long exact sequence of R-modules. Define C_{-1} to be M and take K_j to be $\ker\{d_j : C_j \to C_{j-1}\}$. There are short exact sequences

$$0 \to K_j \to C_j \to K_{j-1} \to 0, \tag{2.12}$$

one for each $j \geq 0$.

Step 1: There is an exact sequence

$$0 \to \mathfrak{F}K_{j-1} \to \mathfrak{F}C_j \to \mathfrak{F}K_j \to \mathrm{H}^{j+1}(\mathfrak{F}(C_\bullet)) \to 0$$

for each $j \geq 0$. Since $\mathfrak{F}$ is left exact, (2.12) gives rise to the exact sequence

$$0 \to \mathfrak{F}K_{j-1} \to \mathfrak{F}C_j \to \mathfrak{F}K_j \to X^j \to 0$$

where we take X_j to be the group that makes the sequence exact. The goal is to prove $X^j \cong \mathrm{H}^{j+1}(\mathfrak{F}(C_\bullet))$. Apply the left exact contravariant functor $\mathfrak{F}$ to the exact sequence

$$C_{j+1} \xrightarrow{d_{j+1}} C_j \xrightarrow{d_j} K_{j-1} \to 0$$

to get the exact sequence

$$0 \to \mathfrak{F}K_{j-1} \to \mathfrak{F}C_j \xrightarrow{\mathfrak{F}d_{j+1}} \mathfrak{F}C_{j+1}.$$

This shows

$$\mathfrak{F}K_{j-1} = \ker(\mathfrak{F}d_{j+1}) = \mathrm{Z}^j(\mathfrak{F}C_\bullet)$$

for all $j \geq 0$. The commutative diagram

$$\begin{tikzcd}
C_{j+1} \arrow[rr, "d_{j+1}"] \arrow[dr] & & C_j \\
& K_j \arrow[ur] \arrow[dr] & \\
0 \arrow[ur] & & 0
\end{tikzcd}$$

gives rise to the commutative diagram

$$\begin{tikzcd}
0 \arrow[dr] & & \\
& \mathfrak{F}K_j \arrow[dr] & \\
\mathfrak{F}C_j \arrow[ur] \arrow[rr, "\mathfrak{F}d_{j+1}"] & & \mathfrak{F}C_{j+1}
\end{tikzcd}$$

Using this we see that $\operatorname{im}(\mathfrak{F}d_{j+1}) = \mathrm{B}^{j+1}(\mathfrak{F}C_\bullet) \subseteq \operatorname{im}\{\mathfrak{F}K_j \to \mathfrak{F}C_{j+1}\} = \mathrm{Z}^{j+1}(\mathfrak{F}C_\bullet)$. Therefore the diagram

$$\begin{tikzcd}
\mathfrak{F}C_j \arrow[rr] \arrow[dr] & & \mathfrak{F}K_j \arrow[r] & X^j \arrow[r] & 0 \\
& \mathrm{B}^{j+1}(\mathfrak{F}C_\bullet) \arrow[ur] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

commutes. But $\mathfrak{F}K^j = \mathrm{Z}^{j+1}(\mathfrak{F}C_\bullet)$, which shows $X^j \cong \mathrm{H}^{j+1}(\mathfrak{F}C_\bullet)$ for each $j \geq 0$. The reader should verify that Step 1 did not use the fact that the modules C_j are acyclic.

Step 2: By Theorem 8.2.13, the short exact sequence (2.12) gives rise to the long exact sequence

$$\cdots \to \mathrm{R}^n\,\mathfrak{F}(C_j) \to \mathrm{R}^n\,\mathfrak{F}(K_j) \xrightarrow{\delta^n} \mathrm{R}^{n+1}\,\mathfrak{F}(K_{j-1}) \to \mathrm{R}^{n+1}\,\mathfrak{F}(C_j) \to \cdots. \tag{2.13}$$

Because the modules C^j are acyclic, the connecting homomorphisms δ^n are isomorphisms

$$\mathrm{R}^n\,\mathfrak{F}(K_j) \cong \mathrm{R}^{n+1}\,\mathfrak{F}(K_{j-1}) \tag{2.14}$$

for all $n \geq 1$ and $j \geq 0$. Iterate (2.14) to get

$$\mathrm{R}^{n+1}\,\mathfrak{F}(M) = \mathrm{R}^{n+1}\,\mathfrak{F}(K_{-1}) \cong \mathrm{R}^n\,\mathfrak{F}(K_0) \cong \mathrm{R}^{n-1}\,\mathfrak{F}(K_1) \cong \cdots \cong \mathrm{R}^1\,\mathfrak{F}(K_{n-1}). \tag{2.15}$$

When $n = 0$, (2.13) looks like

$$0 \to \mathfrak{F}K_{j-1} \to \mathfrak{F}C_j \to \mathfrak{F}K_j \xrightarrow{\delta^0} \mathrm{R}^1\,\mathfrak{F}K_{j-1} \to 0. \tag{2.16}$$

Comparing (2.16) and (2.15) with the exact sequence of Step 1 we get

$$\mathrm{R}^{j+1}\,\mathfrak{F}(M) \cong \mathrm{H}^{j+1}(\mathfrak{F}C_\bullet)$$

which finishes the proof of Part (2). □

2.10. Bifunctors. The reader is referred to Definition 8.1.16 for the definition of a bifunctor. In this section we restrict our attention to a bifunctor $\mathfrak{F} : {}_R\mathfrak{M} \times {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ which is left exact contravariant in the first variable and left exact covariant in the second variable.

LEMMA 8.2.18. *Let M be a fixed R-module. Suppose $\mathfrak{F} : {}_R\mathfrak{M} \times {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ is a bifunctor such that $\mathfrak{F}_1(\cdot, M)$ is left exact contravariant and $\mathfrak{F}_2(M, \cdot)$ is left exact covariant. For any short exact sequence of R-modules $0 \to A \to B \to C \to 0$, there are long exact sequences of groups*

$$0 \to \mathfrak{F}(C,M) \to \mathfrak{F}(B,M) \to \mathfrak{F}(A,M) \xrightarrow{\delta^0}$$
$$\mathrm{R}^1\,\mathfrak{F}_1(C,M) \to \mathrm{R}^1\,\mathfrak{F}_1(B,M) \to \mathrm{R}^1\,\mathfrak{F}_1(A,M) \xrightarrow{\delta^1} \cdots$$

and

$$0 \to \mathfrak{F}(M,A) \to \mathfrak{F}(M,B) \to \mathfrak{F}(M,C) \xrightarrow{\delta^0}$$
$$\mathrm{R}^1\,\mathfrak{F}_2(M,A) \to \mathrm{R}^1\,\mathfrak{F}_2(M,B) \to \mathrm{R}^1\,\mathfrak{F}_2(M,C) \xrightarrow{\delta^1} \cdots.$$

PROOF. Follows straight from Exercises 8.2.11 and Exercises 8.2.12. □

THEOREM 8.2.19. *Suppose* $\mathfrak{F} : {}_R\mathfrak{M} \times {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ *is a bifunctor which satisfies the following.*

(1) *For any R-module M,* $\mathfrak{F}_1(\cdot, M)$ *is left exact contravariant and* $\mathrm{R}^1\mathfrak{F}_1(M, I) = 0$ *for any injective R-module I.*
(2) *For any R-module M,* $\mathfrak{F}_2(M, \cdot)$ *is left exact covariant and* $\mathrm{R}^1\mathfrak{F}_2(P, M) = 0$ *for any projective R-module P.*

Then the two right derived groups $\mathrm{R}^n\mathfrak{F}_1(A, B)$ *and* $\mathrm{R}^n\mathfrak{F}_2(A, B)$ *are naturally isomorphic for all R-modules A and B and all* $n \geq 0$*.*

PROOF. By Exercises 8.2.11 and Exercises 8.2.12, we know $\mathrm{R}^0\mathfrak{F}_1(A,B) = \mathfrak{F}(A,B) = \mathrm{R}^0\mathfrak{F}_2(A,B)$. Let $P_\bullet \to A \to 0$ be a projective resolution for A and $0 \to B \to Q^\bullet$ an injective resolution for B. Define P_{-1} to be A and K_j to be $\ker\{d_j : P_j \to P_{j-1}\}$. Define L^j to be $\ker\{d^j : Q^j \to Q^{j+1}\}$. For each pair (i, j), consider the two short exact sequences

$$0 \to K_i \to P_i \to K_{i-1} \to 0 \tag{2.17}$$

$$0 \to L^j \to Q^j \to L^{j+1} \to 0 \tag{2.18}$$

To sequence (2.17) apply Lemma 8.2.18 three times to get three exact sequences

$$0 \to \mathfrak{F}(K_{i-1}, L^j) \to \mathfrak{F}(P_i, L^j) \xrightarrow{\alpha} \mathfrak{F}(K_i, L^j) \xrightarrow{\delta} \mathrm{R}^1\mathfrak{F}_1(K_{i-1}, L^j) \to \mathrm{R}^1\mathfrak{F}_1(P_i, L^j)$$

$$0 \to \mathfrak{F}(K_{i-1}, Q^j) \to \mathfrak{F}(P_i, Q^j) \xrightarrow{\beta} \mathfrak{F}(K_i, Q^j) \xrightarrow{\delta} \mathrm{R}^1\mathfrak{F}_1(K_{i-1}, Q^j) \to \mathrm{R}^1\mathfrak{F}_1(P_i, Q^j)$$

$$0 \to \mathfrak{F}(K_{i-1}, L^{j+1}) \to \mathfrak{F}(P_i, L^{j+1}) \xrightarrow{\gamma} \mathfrak{F}(K_i, L^{j+1}) \xrightarrow{\delta} \mathrm{R}^1\mathfrak{F}_1(K_{i-1}, L^{j+1}) \to \mathrm{R}^1\mathfrak{F}_1(P_i, L^{j+1})$$

By assumption, $\mathrm{R}^1\mathfrak{F}_1(K_{i-1}, Q^j) = 0$ because Q^j is injective, hence β is onto. By Exercise 8.2.14, $\mathrm{R}^1\mathfrak{F}_1(P_i, L^j) = \mathrm{R}^1\mathfrak{F}_1(P_i, L^{j+1}) = 0$ because P_i is projective. To sequence (2.18) apply Lemma 8.2.18 three times to get three exact sequences

$$0 \to \mathfrak{F}(K_{i-1}, L^j) \to \mathfrak{F}(K_{i-1}, Q^j) \xrightarrow{\rho} \mathfrak{F}(K_{i-1}, L^{j+1}) \xrightarrow{\delta} \mathrm{R}^1\mathfrak{F}_2(K_{i-1}, L^j) \to \mathrm{R}^1\mathfrak{F}_2(K_{i-1}, Q^j)$$

$$0 \to \mathfrak{F}(P_i, L^j) \to \mathfrak{F}(P_i, Q^j) \xrightarrow{\sigma} \mathfrak{F}(P_i, L^{j+1}) \xrightarrow{\delta} \mathrm{R}^1\mathfrak{F}_2(P_i, L^j) \to \mathrm{R}^1\mathfrak{F}_2(P_i, Q^j)$$

$$0 \to \mathfrak{F}(K_i, L^j) \to \mathfrak{F}(K_i, Q^j) \xrightarrow{\tau} \mathfrak{F}(K_i, L^{j+1}) \xrightarrow{\delta} \mathrm{R}^1\mathfrak{F}_2(K_i, L^j) \to \mathrm{R}^1\mathfrak{F}_2(K_i, Q^j)$$

By assumption $\mathrm{R}^1\mathfrak{F}_2(P_i, L^j) = 0$ because P_i is projective, hence σ is onto. By Exercise 8.2.13, $\mathrm{R}^1\mathfrak{F}_2(K_i, Q^j) = \mathrm{R}^1\mathfrak{F}_2(K_{i-1}, Q^j) = 0$ because Q^j is injective. The diagram

$$\begin{tikzcd}
\mathfrak{F}(K_{i-1}, L^j) \arrow[r] \arrow[d] & \mathfrak{F}(K_{i-1}, Q^j) \arrow[r, "\rho"] \arrow[d] & \mathfrak{F}(K_{i-1}, L^{j+1}) \arrow[r] \arrow[d] & \mathrm{R}^1\mathfrak{F}_2(K_{i-1}, L^j) \\
\mathfrak{F}(P_i, L^j) \arrow[r] \arrow[d, "\alpha"] & \mathfrak{F}(P_i, Q^j) \arrow[r, "\sigma"] \arrow[d, "\beta"] & \mathfrak{F}(P_i, L^{j+1}) \arrow[r] \arrow[d, "\gamma"] & 0 \\
\mathfrak{F}(K_i, L^j) \arrow[r] \arrow[d] & \mathfrak{F}(K_i, Q^j) \arrow[r, "\tau"] \arrow[d] & \mathfrak{F}(K_i, L^{j+1}) \arrow[r] \arrow[d] & \mathrm{R}^1\mathfrak{F}_2(K_i, L^j) \\
\mathrm{R}^1\mathfrak{F}_1(K_{i-1}, L^j) & 0 & \mathrm{R}^1\mathfrak{F}_1(K_{i-1}, L^{j+1}) &
\end{tikzcd}$$

commutes, where the three rows and three columns are the exact sequences from above. Apply the Snake Lemma (Theorem 2.5.2) to see that

$$\mathrm{R}^1\,\mathfrak{F}_2(K_{i-1},L^j)\cong \mathrm{R}^1\,\mathfrak{F}_1(K_{i-1},L^j). \tag{2.19}$$

Since β and σ are onto, it follows that

$$\mathrm{R}^1\,\mathfrak{F}_2(K_i,L^j)=\mathrm{R}^1\,\mathfrak{F}_1(K_{i-1},L^{j+1}). \tag{2.20}$$

Combine (2.20) and (2.19) to get

$$\mathrm{R}^1\,\mathfrak{F}_1(K_{i-1},L^{j+1})\cong \mathrm{R}^1\,\mathfrak{F}_2(K_i,L^j)\cong \mathrm{R}^1\,\mathfrak{F}_1(K_i,L^j).$$

Iterate this n times to get

$$\mathrm{R}^1\,\mathfrak{F}_1(A,L^{n-1})\cong \mathrm{R}^1\,\mathfrak{F}_1(K_{-1},L^{n-1})\cong \mathrm{R}^1\,\mathfrak{F}_1(K_{n-2},L^0)\cong \mathrm{R}^1\,\mathfrak{F}_1(K_{n-2},B). \tag{2.21}$$

Combine (2.21), (2.19), Theorem 8.2.9, and Theorem 8.2.11 to get

$$\begin{aligned}
\mathrm{R}^n\,\mathfrak{F}_2(A,B) &\cong \mathrm{R}^1\,\mathfrak{F}_2(A,L^{n-1}) \quad \text{(Theorem 8.2.9)}\\
&\cong \mathrm{R}^1\,\mathfrak{F}_1(A,L^{n-1}) \quad (2.19)\\
&\cong \mathrm{R}^1\,\mathfrak{F}_1(K_{n-2},B) \quad (2.21)\\
&\cong \mathrm{R}^n\,\mathfrak{F}_1(A,B) \quad \text{(Theorem 8.2.11).}
\end{aligned}$$

□

3. Introduction to Tor and Ext Groups

3.1. Introduction to Tor groups. Throughout this section, R is an arbitrary ring. Let A be a right R-module and B a left R-module. The assignment $(A,B)\mapsto A\otimes_R B$ is a bifunctor $\mathfrak{T}:\mathfrak{M}_R\times {}_R\mathfrak{M}\to {}_{\mathbb{Z}}\mathfrak{M}$ which is covariant, additive (Exercise 8.1.9), and right exact (Lemma 2.3.18) in both variables. If P is a projective right R-module, then $\mathfrak{T}_2(P,\cdot)$ is an exact functor (Exercise 2.3.6). By Exercise 8.1.12, $\mathrm{L}_n\,\mathfrak{T}_2(P,B)=0$ for all $n\geq 1$ and all B. Likewise, if Q is a projective left R-module, then $\mathrm{L}_n\,\mathfrak{T}_1(A,Q)=0$ for all $n\geq 1$ and all A.

DEFINITION 8.3.1. For $n\geq 0$ define

$$\mathrm{Tor}_n^R(A,B)=\mathrm{L}_n\,\mathfrak{T}_1(A,B)\cong \mathrm{L}_n\,\mathfrak{T}_2(A,B)$$

where the last isomorphism is due to Theorem 8.1.20. More specifically, if $P_\bullet\to A$ is a projective resolution for A and $Q_\bullet\to B$ is a projective resolution for B, then

$$\begin{aligned}
\mathrm{Tor}_n^R(A,B)&=\mathrm{H}_n(P_\bullet\otimes_R B)\\
&=\mathrm{H}_n(A\otimes_R Q_\bullet).
\end{aligned}$$

LEMMA 8.3.2. *Let M be a right R-module and N a left R-module.*

(1) If M is flat or N is flat, then $\mathrm{Tor}_n^R(M,N)=0$ for all $n\geq 1$.
(2) If $0\to A\to B\to C\to 0$ is a short exact sequence of left R-modules, then

$$\begin{aligned}
\cdots\to \mathrm{Tor}_n^R(M,A)\to \mathrm{Tor}_n^R(M,B)\to \mathrm{Tor}_n^R(M,C)\xrightarrow{\partial}\mathrm{Tor}_{n-1}^R(M,A)\to\cdots\\
\cdots\to \mathrm{Tor}_1^R(M,C)\xrightarrow{\partial} M\otimes_R A\to M\otimes_R B\to M\otimes_R C\to 0
\end{aligned}$$

is a long exact sequence of abelian groups.

(3) *If* $0 \to A \to B \to C \to 0$ *is a short exact sequence of right R-modules, then*

$$\cdots \to \operatorname{Tor}_n^R(A,N) \to \operatorname{Tor}_n^R(B,N) \to \operatorname{Tor}_n^R(C,N) \xrightarrow{\partial} \operatorname{Tor}_{n-1}^R(A,N) \to \cdots$$
$$\cdots \to \operatorname{Tor}_1^R(C,N) \xrightarrow{\partial} A \otimes_R N \to B \otimes_R N \to C \otimes_R N \to 0$$

is a long exact sequence of abelian groups.

(4) *If* $C_\bullet \to M \to 0$ *is a resolution of M by flat R-modules* C_i *and if* $D_\bullet \to N \to 0$ *is a resolution of N by flat R-modules* D_i*, then*

$$\begin{aligned} \operatorname{Tor}_n^R(M,N) &= \operatorname{H}_n(C_\bullet \otimes_R N) \\ &= \operatorname{H}_n(M \otimes_R D_\bullet). \end{aligned}$$

(5) *For all* $n \geq 0$, $\operatorname{Tor}_n^R(M,N) \cong \operatorname{Tor}_n^{R^o}(N,M)$.

(6) *For a fixed M, if* $\operatorname{Tor}_1^R(M,N) = 0$ *for all N, then M is flat.*

(7) *If I is an index set and* $\{M_i\}$ *is a collection of right R-modules, then*

$$\operatorname{Tor}_n^R\left(\bigoplus_i M_i, N\right) \cong \bigoplus_i \operatorname{Tor}_n^R(M_i,N)$$

for all $n \geq 0$.

(8) *If I is a directed index set and* $\{M_i\}$ *is a directed system of right R-modules, then*

$$\operatorname{Tor}_n^R\left(\varinjlim M_i, N\right) \cong \varinjlim \operatorname{Tor}_n^R(M_i,N)$$

for all $n \geq 0$.

PROOF. (1): Tensoring with a flat R-module defines an exact functor. This follows from Exercise 8.1.12.

(2) and (3): Follow straight from Exercise 8.1.13.

(4): By Part (1) flat modules are acyclic for the tensor functor. This follows from Theorem 8.1.15.

(5): Start with a projective resolution $P_\bullet \to M$ and use Lemma 2.3.16 to show

$$\operatorname{H}_n(P_\bullet \otimes_R N) \cong \operatorname{H}_n(N \otimes_{R^o} P_\bullet).$$

(6): Follows from Part (2).

(7): Let $0 \to K \to P \to N \to 0$ be a short exact sequence, where P is projective. By Part (1) $\operatorname{Tor}_n(X,P) = 0$ for all X and for all $n \geq 1$. By Part (2), for each $i \in I$ there is a long exact sequence

$$(3.1)\quad 0 \to \operatorname{Tor}_{n+1}^R(M_i,N) \xrightarrow{\partial} \operatorname{Tor}_n^R(M_i,K) \to 0 \to \cdots$$
$$\cdots \to 0 \to \operatorname{Tor}_1^R(M_i,N) \xrightarrow{\partial} M_i \otimes_R K \to M_i \otimes_R P \to M \otimes_R N \to 0$$

Another long exact sequence is

$$(3.2)\quad 0 \to \operatorname{Tor}_{n+1}^R\left(\bigoplus_i M_i, N\right) \xrightarrow{\partial} \operatorname{Tor}_n^R\left(\bigoplus_i M_i, K\right) \to 0 \to \cdots$$
$$\cdots \to 0 \to \operatorname{Tor}_1^R\left(\bigoplus_i M_i, N\right) \xrightarrow{\partial} \bigoplus_i M_i \otimes_R K \to \bigoplus_i M_i \otimes_R P \to \bigoplus_i M_i \otimes_R N \to 0.$$

Take direct sums of (3.1) and combine with (3.2). In degrees one and zero, we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus_i \operatorname{Tor}_1^R(M_i,N) \arrow[r, "\partial"] \arrow[d, "\gamma"] & \bigoplus_i \left(M_i \otimes_R K\right) \arrow[r] \arrow[d, "\alpha"] & \bigoplus_i \left(M_i \otimes_R P\right) \arrow[d, "\beta"] \\
0 \arrow[r] & \operatorname{Tor}_1^R\left(\bigoplus_i M_i, N\right) \arrow[r, "\partial"] & \bigoplus_i M_i \otimes_R K \arrow[r] & \bigoplus_i M_i \otimes_R P
\end{tikzcd}$$

which is commutative and has exact rows. By Lemma 2.3.15, α and β are isomorphisms. Therefore γ is an isomorphism. In degrees $n+1$ and n, we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus_i \operatorname{Tor}_{n+1}^R(M_i,N) \arrow[r, "\partial"] \arrow[d, "\gamma"] & \bigoplus_i \operatorname{Tor}_n^R(M_i,K) \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & \operatorname{Tor}_{n+1}^R\left(\bigoplus_i M_i, N\right) \arrow[r, "\partial"] & \operatorname{Tor}_n^R\left(\bigoplus_i M_i, K\right) \arrow[r] & 0
\end{tikzcd}$$

which is commutative and has exact rows. By induction on n we assume α is an isomorphism. Therefore γ is an isomorphism.

(8): Use the same notation as in the proof of Part (7). Another long exact sequence is

$$\begin{aligned}
(3.3)\quad & 0 \to \operatorname{Tor}_{n+1}^R\left(\varinjlim M_i, N\right) \xrightarrow{\partial} \operatorname{Tor}_n^R\left(\varinjlim M_i, K\right) \to 0 \to \cdots \\
& \cdots \to 0 \to \operatorname{Tor}_1^R\left(\varinjlim M_i, N\right) \xrightarrow{\partial} \varinjlim M_i \otimes_R K \to \varinjlim M_i \otimes_R P \to \varinjlim M_i \otimes_R N \to 0.
\end{aligned}$$

Take direct limits of (3.1) and combine with (3.3). By Theorem 2.7.6, in degrees one and zero, we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \varinjlim \operatorname{Tor}_1^R(M_i,N) \arrow[r, "\partial"] \arrow[d, "\gamma"] & \varinjlim \left(M_i \otimes_R K\right) \arrow[r] \arrow[d, "\alpha"] & \varinjlim \left(M_i \otimes_R P\right) \arrow[d, "\beta"] \\
0 \arrow[r] & \operatorname{Tor}_1^R\left(\varinjlim M_i, N\right) \arrow[r, "\partial"] & \varinjlim M_i \otimes_R K \arrow[r] & \varinjlim M_i \otimes_R P
\end{tikzcd}$$

which is commutative and has exact rows. By Corollary 2.7.10, α and β are isomorphisms. Therefore γ is an isomorphism. In degrees $n+1$ and n, we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \varinjlim \operatorname{Tor}_{n+1}^R(M_i,N) \arrow[r, "\partial"] \arrow[d, "\gamma"] & \varinjlim \operatorname{Tor}_n^R(M_i,K) \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & \operatorname{Tor}_{n+1}^R\left(\varinjlim M_i, N\right) \arrow[r, "\partial"] & \operatorname{Tor}_n^R\left(\varinjlim M_i, K\right) \arrow[r] & 0
\end{tikzcd}$$

which is commutative and has exact rows. By induction on n we assume α is an isomorphism. Therefore γ is an isomorphism. ☐

LEMMA 8.3.3. *Let R be any ring and M a left R-module. The following are equivalent.*

1. *M is a flat R-module.*
2. *For every right ideal I of R, $\operatorname{Tor}_1^R(R/I, M) = 0$.*

(3) *For every finitely generated right ideal I of R,* $\operatorname{Tor}_1^R(R/I, M) = 0$.
(4) *For every right R-module N,* $\operatorname{Tor}_1^R(N, M) = 0$.
(5) *For every finitely generated right R-module N,* $\operatorname{Tor}_1^R(N, M) = 0$.

PROOF. Is left to the reader. $\square$

LEMMA 8.3.4. *Let R be a commutative ring and M and N two R-modules.*

(1) $\operatorname{Tor}_n^R(M, N)$ *is an R-module.*
(2) $\operatorname{Tor}_n^R(M, N) \cong \operatorname{Tor}_n^R(N, M)$.
(3) *If $R \to S$ is a homomorphism of commutative rings such that S is a flat R-algebra, then*
$$\operatorname{Tor}_n^R(M, N) \otimes_R S = \operatorname{Tor}_n^S(M \otimes_R S, N \otimes_R S)$$
for all $n \geq 0$.
(4) *If $P \in \operatorname{Spec} R$, then*
$$\operatorname{Tor}_n^R(M, N)_P = \operatorname{Tor}_n^{R_P}(M_P, N_P)$$
for all $n \geq 0$.

PROOF. (1), (2) and (4): are left to the reader.

(3): Let $P_\bullet \to M \to 0$ be a projective resolution of M. Since S is a flat R-algebra, $(\,) \otimes_R S$ is an exact functor. Therefore $P_\bullet \otimes_R S \to M \otimes_R S \to 0$ is a projective resolution of the S-module $M \otimes_R S$. It follows that
$$\operatorname{Tor}_n^R(M, N) \otimes_R S = \mathrm{H}_n(P_\bullet \otimes_R N) \otimes_R S$$
and
$$\operatorname{Tor}_n^S(M \otimes_R S, N \otimes_R S) = \mathrm{H}_n\big((P_\bullet \otimes_R S) \otimes_S (N \otimes_R S)\big) = \mathrm{H}_n\big((P_\bullet \otimes_R N) \otimes_R S\big).$$
By Exercise 8.1.4, $\mathrm{H}_n(P_\bullet \otimes_R N) \otimes_R S = \mathrm{H}_n\big((P_\bullet \otimes_R N) \otimes_R S\big)$. $\square$

LEMMA 8.3.5. *Let $R \to S$ be a homomorphism of commutative rings. Let M be an S-module and N an R-module.*

(1) *For all $n \geq 0$,* $\operatorname{Tor}_n^R(M, N)$ *is an S-module.*
(2) *If R and S are noetherian, N is finitely generated over R, and M is finitely generated over S, then* $\operatorname{Tor}_n^R(M, N)$ *is finitely generated over S.*
(3) *If $P \in \operatorname{Spec} S$ and $Q = P \cap R$, then*
$$\operatorname{Tor}_n^R(M, N) \otimes_S S_P = \operatorname{Tor}_n^{R_Q}\big(M_P, N_Q\big) = \operatorname{Tor}_n^R\big(M_P, N\big).$$

PROOF. (1): Let $A_\bullet \to N$ be a projective resolution of N. The functor $(\cdot) \otimes_R M$ maps the category $\mathfrak{M}_R$ to the category $\mathfrak{M}_S$, so for each n, $\mathrm{H}_n(A_\bullet \otimes_R M)$ is an S-module.

(2): By Exercise 8.3.3, let $A_\bullet \to N$ be a resolution of N where each A_i is a finitely generated free R-module. Then $A_i \otimes_R M$ is finitely generated over S. It follows from Corollary 4.1.12 that $\mathrm{H}_n(A_\bullet \otimes_R M)$ is a finitely generated S-module for each n.

(3): Let $A_\bullet \to N$ be a projective resolution of N. Then
$$\begin{aligned}
\operatorname{Tor}_n^R(M, N) \otimes_S S_P &= \mathrm{H}_n(A_\bullet \otimes_R M) \otimes_S S_P \\
&= \mathrm{H}_n\big(A_\bullet \otimes_R M \otimes_S S_P\big) \quad \text{(by Exercise 8.1.4)} \\
&= \operatorname{Tor}_n^R\big(M_P, N\big).
\end{aligned}$$

Continue from the same starting point,

$$\begin{aligned}
\operatorname{Tor}_n^R(M,N)\otimes_S S_P &= \mathrm{H}_n(A_\bullet \otimes_R M)\otimes_S S_P\\
&= \mathrm{H}_n\bigl(A_\bullet \otimes_R M \otimes_S S_P\bigr) \quad \text{(by Exercise 8.1.4)}\\
&= \mathrm{H}_n\bigl((A_\bullet \otimes_R R_Q)\otimes_{R_Q}(M\otimes_S S_P)\bigr)\\
&= \operatorname{Tor}_n^{R_Q}\bigl(M_P, N_Q\bigr)
\end{aligned}$$

where the last equality holds because $A_\bullet \otimes_R R_Q$ is a projective resolution of the R_Q-module $N \otimes_R R_Q$. □

COROLLARY 8.3.6. *Let $R \to S$ be a homomorphism of commutative rings. Let M be an S-module. The following are equivalent.*

(1) M is flat when viewed as an R-module.
(2) M_P is a flat R_Q-module for all $P \in \operatorname{Spec} S$, if $Q = P \cap R$.
(3) $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{n}}$-module for all $\mathfrak{m} \in \operatorname{Max} S$, if $\mathfrak{n} = \mathfrak{m} \cap R$.

PROOF. (1) implies (2): Let N be any R_Q-module. Then $N_Q = N \otimes_R R_Q = N$. By Lemma 8.3.5, $\operatorname{Tor}_1^{R_Q}\bigl(M_P, N_Q\bigr) = \bigl(\operatorname{Tor}_1^R(M,N)\bigr)_P = 0$.

(2) implies (3): is trivially true.

(3) implies (1): Let N be any R-module, $\mathfrak{m} \in \operatorname{Max} S$, and set $\mathfrak{n} = \mathfrak{m} \cap R$. It follows from Lemma 8.3.5 that $\bigl(\operatorname{Tor}_1^R(M,N)\bigr)_{\mathfrak{m}} = \operatorname{Tor}_1^{R_{\mathfrak{n}}}\bigl(M_{\mathfrak{m}}, N_{\mathfrak{n}}\bigr) = 0$. □

3.2. Tor and Torsion. In this section R is an integral domain and K is the field of fractions of R. The reader is referred to Definition 1.7.13 for the definition of torsion module.

LEMMA 8.3.7. *Let R be an integral domain, K the field of fractions of R, and M an R-module.*

(1) $\operatorname{Tor}_n^R(K/R, M) = 0$ for all $n \geq 2$.
(2) If M is torsion free, then $\operatorname{Tor}_1^R(K/R, M) = 0$.
(3) If M is a torsion R-module, then the connecting homomorphism induces a natural isomorphism $\operatorname{Tor}_1^R(K/R, M) \cong M$ of R-modules.

PROOF. (1): The exact sequence of R-modules $0 \to R \to K \to K/R \to 0$ gives rise to the long exact sequence

$$(3.4) \qquad \cdots \to \operatorname{Tor}_n^R(K,M) \to \operatorname{Tor}_n^R(K/R,M) \xrightarrow{\partial_n} \operatorname{Tor}_{n-1}^R(K/R,M) \to \dots$$
$$\cdots \to \operatorname{Tor}_1^R(K,M) \to \operatorname{Tor}_1^R(K/R,M) \xrightarrow{\partial_1} R\otimes_R M \to K \otimes_R M \to K/R \otimes_R M \to 0$$

of R-modules (Lemma 8.3.2). Clearly R is flat, and by Lemma 3.1.7, K is flat. It follows from Lemma 8.3.3 that $\operatorname{Tor}_i^R(R,M) = \operatorname{Tor}_i^R(K,M) = 0$ for $i \geq 1$.

(2): Since $\operatorname{Tor}_1^R(K,M) = 0$, ∂_1 is one-to-one. By Lemma 3.1.4, $M \to K \otimes_R M$ is one-to-one, so $\partial_1 = 0$.

(3): By Exercise 2.3.20, $K \otimes_R M = 0$. The connecting homomorphism ∂_1, which is natural by Theorem 8.1.14, is an isomorphism. □

3.3. Exercises.

EXERCISE 8.3.1. Let $0 \to A \to B \to C \to 0$ be a short exact sequence of R-modules. If A and C are flat, then B is flat.

EXERCISE 8.3.2. Use Lemma 8.3.5 to give another proof of Proposition 3.7.2.

EXERCISE 8.3.3. If R is noetherian and M is a finitely generated R-module, then there exists a resolution $P_\bullet \to M \to 0$ of M such that each P_i is a finitely generated free R-module.

3.4. Introduction to Ext Groups. Throughout this section, R is an arbitrary ring. The assignment $(A,B) \mapsto \operatorname{Hom}_R(A,B)$ is a bifunctor $\mathfrak{E} : {}_R\mathfrak{M} \times {}_R\mathfrak{M} \to \mathbb{Z}$-modules. Let A and B be left R-modules. By Proposition 2.4.5, the functor $\mathfrak{E}_1(\cdot,B)$ is left exact contravariant whereas the functor $\mathfrak{E}_2(A,\cdot)$ is left exact covariant. By Proposition 2.4.5, if P is a projective R-module, the functor $\mathfrak{E}_2(P,\cdot)$ is exact. By Exercise 8.2.9, $\mathrm{R}^n\,\mathfrak{E}_2(P,B) = 0$ for all $n \geq 1$ and all B. By Theorem 2.6.2, if Q is an injective R-module, the functor $\mathfrak{E}_1(\cdot,Q)$ is exact. By Exercise 8.2.10, $\mathrm{R}^n\,\mathfrak{E}_1(A,Q) = 0$ for all $n \geq 1$ and all A.

DEFINITION 8.3.8. Let A and B be left R-modules. For $n \geq 0$ define

$$\operatorname{Ext}^n_R(A,B) = \mathrm{R}^n\,\mathfrak{E}_1(A,B) \cong \mathrm{R}^n\,\mathfrak{E}_2(A,B)$$

where the last isomorphism is due to Theorem 8.2.19. More specifically, if $P_\bullet \to A$ is a projective resolution for A and $B \to Q^\bullet$ is an injective resolution for B, then

$$\begin{aligned}\operatorname{Ext}^n_R(A,B) &= \mathrm{H}^n\big(\operatorname{Hom}_R(P_\bullet,B)\big)\\ &= \mathrm{H}^n\big(\operatorname{Hom}_R(A,Q^\bullet)\big).\end{aligned}$$

PROPOSITION 8.3.9. *Let M and N be left R-modules.*

(1) $\operatorname{Ext}^0_R(M,\cdot) = \operatorname{Hom}_R(M,\cdot)$ *and* $\operatorname{Ext}^0_R(\cdot,N) = \operatorname{Hom}_R(\cdot,N)$.

(2) If $0 \to A \to B \to C \to 0$ is a short exact sequence of left R-modules, then there are long exact sequences

$$\begin{aligned}0 \to \operatorname{Hom}_R(M,A) \to \operatorname{Hom}_R(M,B) \to \operatorname{Hom}_R(M,C) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(M,A) \to \cdots\\ \cdots \to \operatorname{Ext}^n_R(M,A) \to \operatorname{Ext}^n_R(M,B) \to \operatorname{Ext}^n_R(M,C) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R(M,A) \to \cdots\end{aligned}$$

and

$$\begin{aligned}0 \to \operatorname{Hom}_R(C,N) \to \operatorname{Hom}_R(B,N) \to \operatorname{Hom}_R(A,N) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(C,N) \to \cdots\\ \cdots \to \operatorname{Ext}^n_R(C,N) \to \operatorname{Ext}^n_R(B,N) \to \operatorname{Ext}^n_R(A,N) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R(C,N) \to \cdots\end{aligned}$$

of abelian groups.

(3) If M is projective, then $\operatorname{Ext}^n_R(M,N) = 0$ for all $n \geq 1$. Conversely, if $\operatorname{Ext}^1_R(M,N) = 0$ for all N, then M is projective.

(4) If N is injective, then $\operatorname{Ext}^n_R(M,N) = 0$ for all $n \geq 1$. Conversely, if $\operatorname{Ext}^1_R(M,N) = 0$ for all M, then N is injective.

(5) If $\{M_i \mid i \in I\}$ is a collection of R-modules, then

$$\operatorname{Ext}^n_R\Big(\bigoplus_{i\in I} M_i, N\Big) \cong \prod_{i \in I} \operatorname{Ext}^n_R(M_i,N)$$

for all $n \geq 0$.

(6) If $\{N_j \mid j \in J\}$ is a collection of R-modules, then

$$\operatorname{Ext}^n_R\Big(M, \prod_{j\in J} N_j\Big) \cong \prod_{j \in J} \operatorname{Ext}^n_R(M,N_j)$$

for all $n \geq 0$.

PROOF. (1): Follows straight from Exercise 8.2.11 (1) and Exercise 8.2.12 (1).

(2): Follows straight from Exercise 8.2.11 (2) and Exercise 8.2.12 (2).

(3): Follows straight from Exercise 8.2.14, Proposition 2.4.5 (2), and the exact sequence of Part (2).

(4): Follows straight from Exercise 8.2.13, Theorem 2.6.2, and the exact sequence of Part (2).

(5): Let $0 \to N \to Q \to C \to 0$ be a short exact sequence, where Q is injective. By Part (4) $\operatorname{Ext}^n_R(X,Q) = 0$ for all X and for all $n \geq 1$. By Part (2), for each $i \in I$ there is a long exact sequence

$$\begin{aligned} 0 \to \operatorname{Hom}_R(M_i,N) \to \operatorname{Hom}_R(M_i,Q) \to \operatorname{Hom}_R(M_i,C) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(M_i,N) \to 0 \to \\ \cdots \to 0 \to \operatorname{Ext}^n_R(M_j,C) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R(M_j,N) \to 0 \to \cdots \end{aligned} \tag{3.5}$$

Another long exact sequence is

$$\begin{aligned} 0 \to \operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i,N\Big) \to \operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i,Q\Big) \to \\ \operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i,C\Big) \xrightarrow{\delta^0} \operatorname{Ext}^1_R\Big(\bigoplus_{i\in I} M_i,N\Big) \to 0 \to \\ \cdots \to 0 \to \operatorname{Ext}^n_R\Big(\bigoplus_{i\in I} M_i,C\Big) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R\Big(\bigoplus_{i\in I} M_i,N\Big) \to 0 \to \cdots \end{aligned} \tag{3.6}$$

Take direct products of (3.5) and combine with (3.6). In degrees zero and one we get the diagram

$$\begin{tikzcd}
\operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i,Q\Big) \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i,C\Big) \arrow[r, "\delta^0"] \arrow[d, "\beta"] & \operatorname{Ext}^1_R\Big(\bigoplus_{i\in I} M_i,N\Big) \arrow[r] \arrow[d, "\gamma"] & 0 \\
\prod_{i\in I} \operatorname{Hom}_R(M_i,Q) \arrow[r] & \prod_{i\in I} \operatorname{Hom}_R(M_i,C) \arrow[r, "\delta^0"] & \prod_{i\in I} \operatorname{Ext}^1_R(M_i,N) \arrow[r] & 0
\end{tikzcd}$$

which commutes and has exact rows. By Proposition 2.4.8, α and β are isomorphisms. Therefore γ is an isomorphism. In degrees n and $n+1$ we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ext}^n_R\Big(\bigoplus_{i\in I} M_i,C\Big) \arrow[r, "\delta^n"] \arrow[d, "\beta"] & \operatorname{Ext}^{n+1}_R\Big(\bigoplus_{i\in I} M_i,N\Big) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & \prod_{i\in I} \operatorname{Ext}^n_R(M_j,C) \arrow[r, "\delta^n"] & \prod_{i\in I} \operatorname{Ext}^{n+1}_R(M_j,N) \arrow[r] & 0
\end{tikzcd}$$

which commutes and has exact rows. By induction on n we assume β is an isomorphism. Therefore γ is an isomorphism.

(6): Start with a short exact sequence $0 \to K \to P \to M \to 0$ where P is projective. Proceed as in Part (5). $\square$

LEMMA 8.3.10. *Let R be a commutative ring and M and N two R-modules.*

1. *For all $n \geq 0$ $\operatorname{Ext}^n_R(M,N)$ is an R-module.*
2. *If R is noetherian, and M and N are finitely generated R-modules, then for all $n \geq 0$, $\operatorname{Ext}^n_R(M,N)$ is a finitely generated R-module.*

(3) *If R is noetherian, M is a finitely generated R-module, and $R \to S$ is a homomorphism of commutative rings such that S is a flat R-algebra, then*

$$\operatorname{Ext}^n_R(M,N) \otimes_R S = \operatorname{Ext}^n_S(M \otimes_R S, N \otimes_R S)$$

for all $n \geq 0$. In particular, if $P \in \operatorname{Spec} R$, then

$$\operatorname{Ext}^n_R(M,N)_P = \operatorname{Ext}^n_{R_P}(M_P, N_P)$$

for all $n \geq 0$.

PROOF. (1) and (2): Are left to the reader.

(3): By Exercise 8.3.3 there exists a projective resolution $P_\bullet \to M \to 0$ of M such that each P_i is a finitely generated free R-module. Since $(\cdot) \otimes_R S$ is an exact functor, $P_\bullet \otimes_R S \to M \otimes_R S \to 0$ is a projective resolution of the S-module $M \otimes_R S$.

$$\begin{aligned}
\operatorname{Ext}^n_S(M \otimes_R S, N \otimes_R S) &= \mathrm{H}^n(\operatorname{Hom}_S(P_\bullet \otimes_R S, N \otimes_R S)) \\
&= \mathrm{H}^n(\operatorname{Hom}_R(P_\bullet, N) \otimes_R S) \quad \text{(Proposition 3.5.8)} \\
&= \mathrm{H}^n(\operatorname{Hom}_R(P_\bullet, N)) \otimes_R S \quad \text{(Exercise 8.2.4)} \\
&= \operatorname{Ext}^n_R(M,N) \otimes_R S
\end{aligned}$$

□

LEMMA 8.3.11. *Let $A \in {}_R\mathfrak{M}$, $B \in {}_S\mathfrak{M}_R$ and $C \in {}_S\mathfrak{M}$.*

(1) *If A is a projective left R-module, then there are isomorphisms of $\mathbb{Z}$-modules*

$$\operatorname{Ext}^n_S(B \otimes_R A, C) \cong \operatorname{Hom}_R(A, \operatorname{Ext}^n_S(B,C))$$

for all $n \geq 0$.

(2) *If the functor $B \otimes_R (\cdot) : {}_R\mathfrak{M} \to {}_S\mathfrak{M}$ maps projective R-modules to projective S-modules, then there are isomorphisms of $\mathbb{Z}$-modules*

$$\operatorname{Ext}^n_S(B \otimes_R A, C) \cong \operatorname{Ext}^n_R(A, \operatorname{Hom}_S(B,C))$$

for all $n \geq 0$.

In both instances, the isomorphisms are induced by the adjoint isomorphisms of Theorem 2.4.10.

PROOF. (1): Let $C \to I_\bullet$ be an injective resolution of C. By the adjoint isomorphism,

$$\operatorname{Hom}_S(B \otimes_R A, I_\bullet) \cong \operatorname{Hom}_R(A, \operatorname{Hom}_S(B, I_\bullet)) \tag{3.7}$$

is an isomorphism of complexes. Then $\operatorname{Ext}^n_S(B \otimes_R A, C)$ is the nth homology group of the complex on the left hand side of (3.7). Since A is projective, $\operatorname{Hom}_R(A,\cdot)$ is an exact covariant functor. Using Exercise 8.1.4, the nth homology group of the complex on the right hand side of (3.7) is isomorphic to $\operatorname{Hom}_R(A, \operatorname{Ext}^n_S(B,C))$.

(2): Let $P_\bullet \to A$ be a projective resolution of the left R-module A. Then $B \otimes_R P_\bullet \to B \otimes_R A$ is a projective resolution of the left S-module $B \otimes_R A$. By the adjoint isomorphism,

$$\operatorname{Hom}_S(B \otimes_R P_\bullet, C) \cong \operatorname{Hom}_R(P_\bullet, \operatorname{Hom}_S(B,C)) \tag{3.8}$$

is an isomorphism of complexes. Then $\operatorname{Ext}^n_S(B \otimes_R A, C)$, which is the nth homology group of the complex on the left hand side of (3.8), is isomorphic to $\operatorname{Ext}^n_R(A, \operatorname{Hom}_S(B,C))$, which is the nth homology group of the complex on the right hand side of (3.8). □

4. Cohomological Dimension of a Ring

The results of this section will be applied when we study regular local rings in Section 11.3.5. The material presented in this section is based on various sources, including [**51**], [**41**], and [**23**].

Let R be a ring and M a left R-module. The *projective dimension* of M, written $\operatorname{proj.dim}_R M$, is the length of a shortest projective resolution for M. If $0 \to P_n \to \cdots \to P_1 \to P_0 \to M \to 0$ is a projective resolution of M, then $\operatorname{proj.dim}_R(M) \le n$. It follows that M is projective if and only if $\operatorname{proj.dim}_R(M) = 0$. The *injective dimension* of M, written $\operatorname{inj.dim}_R M$, is the length of a shortest injective resolution for M.

LEMMA 8.4.1. *(Schanuel's Lemma) Let R be any ring and M a left R-module. Suppose P and Q are projective R-modules such that the sequences*

$$0 \to K \to P \to M \to 0$$

$$0 \to L \to Q \to M \to 0$$

are exact. The R-modules $K \oplus Q$ and $L \oplus P$ are isomorphic.

PROOF. Consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r, "\phi"] \arrow[d, dashed, "\exists\rho"] & P \arrow[r, "\psi"] \arrow[d, dashed, "\exists\eta"] & M \arrow[r] \arrow[d, "="] & 0 \\ 0 \arrow[r] & L \arrow[r, "\alpha"] & Q \arrow[r, "\beta"] & M \arrow[r] & 0 \end{tikzcd}$$

with rows given. By Proposition 2.1.1 (3), there exists a homomorphism η such that $\beta\eta = \psi$ because P is projective. Now $\beta\eta\phi = \psi\phi = 0$ so $\operatorname{im}\eta\phi \subseteq \ker\beta = \operatorname{im}\alpha$. Since α is one-to-one, there exists ρ making the diagram commute. Define $\delta : K \to P \oplus L$ by $\delta(x) = (\phi(x), \rho(x))$. Since ϕ is one-to-one, so is δ. Define $\pi : P \oplus L \to Q$ by $\pi(u,v) = \eta(u) - \alpha(v)$. Since the diagram commutes, $\pi\delta = 0$. The reader should verify that the sequence

$$0 \to K \xrightarrow{\delta} P \oplus L \xrightarrow{\pi} Q \to 0 \tag{4.1}$$

is exact. Since Q is projective, sequence (4.1) splits. □

DEFINITION 8.4.2. Let R be any ring and M a left R-module. Let $P_\bullet \to M$ be a projective resolution of M. Define K_{n-1} to be the kernel of d_{n-1}. Then

$$0 \to K_{n-1} \to P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0$$

is exact. Let K_0 be the kernel of ε. We say K_n is the nth *syzygy* of M with respect to the projective resolution $P_\bullet$.

DEFINITION 8.4.3. If R is a ring and M and N are two left R-modules, then we say M and N are *projectively equivalent* in case there exist projective R-modules P and Q such that $M \oplus P \cong N \oplus Q$.

THEOREM 8.4.4. *Let R be any ring and M a left R-module. Given a projective resolution $P_\bullet \to M$ with syzygies $\{K_n\}$ and another projective resolution $Q_\bullet \to M$ with syzygies $\{L_n\}$, for each $n \ge 0$, K_n and L_n are projectively equivalent.*

PROOF. Use induction on n. For $n = 0$, this is Lemma 8.4.1. The rest is left to the reader. □

THEOREM 8.4.5. *Let R be any ring and M a left R-module. For any $n \geq 0$, the following are equivalent.*

(1) $\operatorname{proj.dim}_R(M) \leq n$.
(2) *For all R-modules N, $\operatorname{Ext}_R^k(M,N) = 0$ for all $k \geq n+1$.*
(3) *For all R-modules N, $\operatorname{Ext}_R^{n+1}(M,N) = 0$.*
(4) *There exists a projective resolution $P_\bullet \to M$ with syzygies $\{K_n\}$ such that K_{n-1} is projective.*
(5) *For any projective resolution $P_\bullet \to M$ with syzygies $\{K_n\}$, K_{n-1} is projective.*

PROOF. (1) implies (2): Use a projective resolution for M of length n to compute $\operatorname{Ext}_R^k(M,N) = 0$ for all $k \geq n+1$.

(2) implies (3): Is trivial.

(3) implies (4): Let $P_\bullet \to M$ be a projective resolution of M with syzygies $\{K_n\}$. Then

$$0 \to K_{n-1} \to P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0 \tag{4.2}$$

is exact. By Theorem 8.2.11, the groups $\operatorname{Ext}_R^{n+1}(M,N)$ and $\operatorname{Ext}_R^1(K_{n-1},N)$ are naturally isomorphic. By (3), both groups are zero and by Proposition 8.3.9 (3), K_{n-1} is a projective R-module.

(4) implies (5): Suppose we are given a projective resolution $P_\bullet \to M$ with syzygies $\{K_n\}$ such that K_{n-1} is projective. Let $Q_\bullet \to M$ be another projective resolution with syzygies $\{L_n\}$. By Theorem 8.4.4, there exist projectives P and Q such that $K_{n-1} \oplus P \cong L_{n-1} \oplus Q$. Being a direct summand of a projective, L_{n-1} is projective by Proposition 2.1.1 (1).

(5) implies (1): Let $P_\bullet \to M$ be a projective resolution with syzygies $\{K_n\}$. Then K_{n-1} is projective. It follows that (4.2) is a projective resolution of M of length less than or equal to n. $\square$

LEMMA 8.4.6. *Let R be a commutative ring and M an R-module. For any $n \geq 0$, the following are equivalent.*

(1) $\operatorname{inj.dim}_R(M) \leq n$.
(2) *For every ideal I of R, $\operatorname{Ext}_R^{n+1}(R/I,M) = 0$.*

PROOF. (1) implies (2): Follows from Exercise 8.4.1.

(2) implies (1): Let $M \to E^\bullet$ be an injective resolution of the R-module M. Define K^n to be the kernel of d^n. The sequence

$$0 \to M \xrightarrow{\varepsilon} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} \cdots \to E^{n-1} \to K^n \to 0$$

is exact. Let I be an ideal of R. By Theorem 8.2.9, $\operatorname{Ext}_R^{n+1}(R/I,M)$ is naturally isomorphic to $\operatorname{Ext}_R^1(R/I,K^n)$. By (2), $\operatorname{Ext}_R^{n+1}(R/I,M) = 0$. By Exercise 8.4.2, K^n is an injective R-module. There exists an injective resolution of M of length less than or equal to n. $\square$

LEMMA 8.4.7. *Let R be a noetherian ring and M a finitely generated left R-module. The following are equivalent.*

(1) *M is a projective R-module.*
(2) $\operatorname{Ext}_R^1(M,N) = 0$ *for all finitely generated left R-modules N.*

PROOF. (1) implies (2): Follows from Proposition 8.3.9 (3).

(2) implies (1): By Corollary 4.1.12, M is finitely presented, so there exists an exact sequence

$$0 \to A \xrightarrow{\alpha} B \to M \to 0 \tag{4.3}$$

such that B is a finitely generated free R-module and A is a finitely generated R-module. By (2), $\operatorname{Ext}^1_R(M,A) = 0$. The long exact sequence of Proposition 8.3.9 (2) degenerates into the short exact sequence

$$0 \to \operatorname{Hom}_R(M,A) \to \operatorname{Hom}_R(B,A) \xrightarrow{\mathrm{H}\alpha} \operatorname{Hom}_R(A,A) \to 0.$$

There exists $\phi \in \operatorname{Hom}_R(B,A)$ such that $\phi\alpha$ is the identity map on A. The sequence (4.3) splits, so M is projective by Proposition 2.1.1 (1). □

LEMMA 8.4.8. *Let R be a commutative noetherian ring and M a finitely generated R-module. For any $n \geq 0$, the following are equivalent.*

(1) $\operatorname{proj.dim}_R(M) \leq n$.
(2) For every ideal I of R, $\operatorname{Ext}^{n+1}_R(M,R/I) = 0$.

PROOF. (1) implies (2): Follows from Exercise 8.4.1.

(2) implies (1): Let N be an arbitrary finitely generated R-module. By Exercise 8.4.6, it suffices to show $\operatorname{Ext}^{n+1}_R(M,N) = 0$. Proceed by induction on the number of generators of N. Suppose $N = Rx_1 + \cdots + Rx_m$. Let $N_0 = Rx_1$. By (2), $\operatorname{Ext}^{n+1}_R(M,N_0) = 0$ and by induction on m, $\operatorname{Ext}^{n+1}_R(M,N/N_0) = 0$. The long exact sequence of Proposition 8.3.9 (2) becomes

$$\cdots \to \operatorname{Ext}^{n+1}_R(M,N_0) \to \operatorname{Ext}^{n+1}_R(M,N) \to \operatorname{Ext}^{n+1}_R(M,N/N_0) \to \dots$$

which proves $\operatorname{Ext}^{n+1}_R(M,N) = 0$. □

COROLLARY 8.4.9. *Let R be a commutative noetherian ring.*

(1) For any R-module M,

$$\begin{aligned}\operatorname{inj.dim}_R(M) &= \sup\{\operatorname{inj.dim}_{R_P}(M \otimes_R R_P) \mid P \in \operatorname{Spec}(R)\}\\ &= \sup\{\operatorname{inj.dim}_{R_\mathfrak{m}}(M \otimes_R R_\mathfrak{m}) \mid \mathfrak{m} \in \operatorname{Max}(R)\}.\end{aligned}$$

(2) For any finitely generated R-module M,

$$\begin{aligned}\operatorname{proj.dim}_R(M) &= \sup\{\operatorname{proj.dim}_{R_P}(M \otimes_R R_P) \mid P \in \operatorname{Spec} R\}\\ &= \sup\{\operatorname{proj.dim}_{R_\mathfrak{m}}(M \otimes_R R_\mathfrak{m}) \mid \mathfrak{m} \in \operatorname{Max} R\}.\end{aligned}$$

PROOF. (1): Suppose $\operatorname{inj.dim}_R(M) \leq n$. Let P be a prime ideal of R. Every ideal of R_P is of the form IR_P for some ideal I of R. By Lemma 8.4.6 and Lemma 8.3.10, $0 = \operatorname{Ext}^{n+1}_R(R/I,M)_P = \operatorname{Ext}^{n+1}_{R_P}(R_P/IR_P, M_P)$. Lemma 8.4.6 implies $\operatorname{inj.dim}_{R_P}(M_P) \leq n$.

Suppose $n = \operatorname{inj.dim}_R(M)$ is finite. By Lemma 8.4.6, there exists an ideal I in R such that $\operatorname{Ext}^n_R(R/I,M) \neq 0$. By Proposition 3.1.9 there exists a maximal ideal $\mathfrak{m} \in \operatorname{Max} R$ such that $\operatorname{Ext}^n_R(R/I,M)_\mathfrak{m} = \operatorname{Ext}^n_{R_\mathfrak{m}}(R_\mathfrak{m}/IR_\mathfrak{m}, M_\mathfrak{m}) \neq 0$. In follows from Lemma 8.4.6, $\operatorname{inj.dim}_{R_\mathfrak{m}}(M_\mathfrak{m}) \geq n$.

(2): Is left to the reader. □

PROPOSITION 8.4.10. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let M be a finitely generated R-module.*

(1) If $\operatorname{Tor}^R_1(M,k) = 0$, then M is a free R-module.
(2) For all $n \geq 0$, $\operatorname{proj.dim}(M) \leq n$ *if and only if* $\operatorname{Tor}^R_{n+1}(M,k) = 0$.
(3) If M is of finite projective dimension, then

$$\operatorname{proj.dim}_R(M/aM) = \operatorname{proj.dim}_R(M) + 1$$

for any M-regular element $a \in \mathfrak{m}$.

PROOF. (1): By Exercise 8.4.4, there exists a free R-module R^{ν} and an exact sequence

$$0 \to K \to R^{\nu} \xrightarrow{f} M \to 0$$

such that $f \otimes 1$ is an isomorphism. The long exact sequence of Theorem 8.3.2 (3) is

$$\operatorname{Tor}_1^R(M,k) \to K \otimes_R k \to k^{\nu} \xrightarrow{f} M \otimes_R k \to 0.$$

Therefore, $K \otimes_R k = 0$. By Corollary 2.2.2, $K = 0$, hence M is free.

(2): Assume $n \geq 0$ and $\operatorname{Tor}_{n+1}^R(M,k) = 0$. If $n = 0$, this is Part (1). Assume $n > 0$. By Exercise 8.3.3, let $P_\bullet \to M$ be a projective resolution of M such that each P_i is finitely generated. Let $K_{n-1} = \ker d_{n-1}$. By Theorem 8.1.9, $0 = \operatorname{Tor}_{n+1}^R(M,k) = \operatorname{Tor}_1^R(K_{n-1},k)$. Since R is noetherian, by Part (1) applied to the finitely generated R-module K_{n-1}, it follows that K_{n-1} is free. Therefore, $\operatorname{proj.dim}(M) \leq n$. The converse is Exercise 8.4.1.

(3): By definition, left multiplication by a is one-to-one, so the sequence

$$0 \to M \xrightarrow{\ell_a} M \to M/aM \to 0$$

is exact. By Lemma 8.3.2 (3) and Lemma 8.3.4 (1), there is a long-exact sequence

$$\dots \xrightarrow{\ell_a} \operatorname{Tor}_{n+1}^R(M,k) \to \operatorname{Tor}_{n+1}^R(M/aM,k) \xrightarrow{\partial}$$
$$\operatorname{Tor}_n^R(M,k) \xrightarrow{\ell_a} \operatorname{Tor}_n^R(M,k) \to \operatorname{Tor}_n^R(M/aM,k) \xrightarrow{\partial}$$

of R-modules. Left multiplication by a annihilates k, hence the long-exact sequence breaks down into short exact sequences

$$0 \to \operatorname{Tor}_{n+1}^R(M,k) \to \operatorname{Tor}_{n+1}^R(M/aM,k) \xrightarrow{\partial} \operatorname{Tor}_n^R(M,k) \xrightarrow{\ell_a} 0. \tag{4.4}$$

Let $d = \operatorname{proj.dim}_R(M)$. By Part (2) and Exercise 8.4.1,

$$\operatorname{Tor}_n^R(M,k) \begin{cases} = 0 & \text{if } n > d \\ \neq 0 & \text{if } n = d. \end{cases}$$

By (4.4),

$$\operatorname{Tor}_n^R(M/aM,k) \begin{cases} = 0 & \text{if } n > d+1 \\ \neq 0 & \text{if } n = d+1. \end{cases}$$

By Part (2), $\operatorname{proj.dim}_R(M/aM) = d+1$. □

LEMMA 8.4.11. *Let R be a commutative noetherian ring. The following are equivalent, for any finitely generated R-module M.*

(1) $\operatorname{proj.dim}_R(M) \leq n$.
(2) $\operatorname{Tor}_{n+1}^R(M,R/\mathfrak{m}) = 0$ *for all* $\mathfrak{m} \in \operatorname{Max} R$.

PROOF. By Corollary 8.4.9, (1) is equivalent to $\operatorname{proj.dim}_{R_\mathfrak{m}}(M_\mathfrak{m}) \leq n$ for all $\mathfrak{m} \in \operatorname{Max} R$. By Proposition 8.4.10, this is equivalent to $\operatorname{Tor}_{n+1}^{R_\mathfrak{m}}(M_\mathfrak{m}, R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}) = 0$ for all $\mathfrak{m} \in \operatorname{Max} R$. By Lemma 8.3.4 this is equivalent to (2). □

PROPOSITION 8.4.12. *(M. Auslander) Let R be a commutative ring and $n \geq 0$. The following are equivalent.*

(1) $\operatorname{proj.dim}_R(M) \leq n$ *for all R-modules M.*
(2) $\operatorname{proj.dim}_R(M) \leq n$ *for all finitely generated R-modules M.*
(3) $\operatorname{inj.dim}_R(M) \leq n$ *for all R-modules M.*
(4) $\operatorname{Ext}_R^{n+1}(M,N) = 0$ *for all R-modules M and N.*

PROOF. (1) implies (2): Is trivial.

(2) implies (3): Let M be an R-module. As in the proof of Lemma 8.4.6, let $M \to E^{\bullet}$ be an injective resolution of the R-module M. Define K^n to be the kernel of d^n. Let I be an ideal of R. By Theorem 8.2.9, $\operatorname{Ext}_R^{n+1}(R/I, M) = \operatorname{Ext}_R^1(R/I, K^n)$. Since R/I is finitely generated, by (2) and Exercise 8.4.1, $\operatorname{Ext}_R^{n+1}(R/I, M) = 0$. By Exercise 8.4.2, K^n is an injective R-module. This proves (3).

(3) implies (4): Follows from Exercise 8.4.1.

(4) implies (1): Follows from Theorem 8.4.5. □

DEFINITION 8.4.13. Let R be a commutative ring. The *global cohomological dimension* of R (or *cohomological dimension* of R, or *global dimension* of R) is defined to be

$$\begin{aligned} \operatorname{coh.dim}(R) &= \sup\{\operatorname{proj.dim}_R(M) \mid M \in {}_R\mathfrak{M}\} \\ &= \sup\{\operatorname{inj.dim}_R(M) \mid M \in {}_R\mathfrak{M}\} \end{aligned}$$

where the last equality follows from Proposition 8.4.12.

LEMMA 8.4.14. *Let R be a commutative noetherian ring.*

(1) The following are equivalent.
 - *(a)* $\operatorname{coh.dim}(R) \le n$.
 - *(b)* $\operatorname{proj.dim}_R(M) \le n$ *for all finitely generated R-modules M.*
 - *(c)* $\operatorname{inj.dim}_R(M) \le n$ *for all finitely generated R-modules M.*
 - *(d)* $\operatorname{Ext}_R^{n+1}(M,N) = 0$ *for all finitely generated R-modules M and N.*
 - *(e)* $\operatorname{Tor}_{n+1}^R(M,N) = 0$ *for all finitely generated R-modules M and N.*

(2) $\operatorname{coh.dim}(R) = \sup\{\operatorname{coh.dim}(R_P) \mid P \in \operatorname{Spec} R\} = \sup\{\operatorname{coh.dim}(R_{\mathfrak{m}}) \mid \mathfrak{m} \in \operatorname{Max} R\}$.

PROOF. (1): (a) is equivalent to (b), by Proposition 8.4.12.
(b) implies (c), by Proposition 8.4.12.
(c) implies (d): Follows from Exercise 8.4.1.
(b) implies (e): Follows from Exercise 8.4.1.
(e) implies (b): Follows from Lemma 8.4.11.
(d) implies (b): Follows from Exercise 8.4.6.
(2): Follows from Part (1) and Corollary 8.4.9. □

THEOREM 8.4.15. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$.*

(1) For a nonnegative integer n, the following are equivalent.
 - *(a)* $\operatorname{coh.dim} R \le n$.
 - *(b)* $\operatorname{Tor}_{n+1}^R(k,k) = 0$.

(2) $\operatorname{coh.dim} R = \operatorname{proj.dim}_R(k)$.

PROOF. (1): (a) implies (b): Follows directly from Definition 8.4.13.

(b) implies (a): Assume $\operatorname{Tor}_{n+1}^R(k,k) = 0$. By Proposition 8.4.10 (2), $\operatorname{proj.dim}_R(k) \le n$. By Exercise 8.4.1, $\operatorname{Tor}_{n+1}^R(M,k) = 0$. By Proposition 8.4.10 (2), $\operatorname{proj.dim}_R(M) \le n$. By Lemma 8.4.14, $\operatorname{coh.dim} R \le n$.

(2): Is left to the reader. □

PROPOSITION 8.4.16. *Let $\phi : R \to S$ be a local homomorphism of commutative noetherian local rings. If S is a flat R-module, then* $\operatorname{coh.dim}(R) \le \operatorname{coh.dim}(S)$.

PROOF. Let M and N be arbitrary finitely generated R-modules. By Lemma 8.3.4,

$$\operatorname{Tor}_n^R(M,N) \otimes_R S = \operatorname{Tor}_n^S(M \otimes_R S, N \otimes_R S) \tag{4.5}$$

for all $n \geq 0$. If $\operatorname{coh.dim}(S) = d$ is finite, then by Lemma 8.4.14, the groups in (4.5) are zero for $n > d$. By Exercise 3.5.12, S is a faithfully flat R-module, hence $\operatorname{Tor}_{d+1}^R(M,N) = 0$. By Lemma 8.4.14, $\operatorname{coh.dim}(R) \leq d$. □

4.1. Exercises.

EXERCISE 8.4.1. Let R be a commutative ring, $\mathfrak{F} : {}_R\mathfrak{M} \to {}_{\mathbb{Z}}\mathfrak{M}$ a covariant additive functor, and M an R-module.

(1) If $\operatorname{proj.dim}_R(M) \leq n$, then $\mathrm{L}_i\mathfrak{F}(M) = 0$ for all $i > n$.
(2) If $\operatorname{inj.dim}_R(M) \leq n$, then $\mathrm{R}^i\mathfrak{F}(M) = 0$ for all $i > n$.

EXERCISE 8.4.2. Let R be a commutative ring and E an R-module. Then E is injective if and only if $\operatorname{Ext}_R^1(R/I, E) = (0)$ for all ideals I in R.

EXERCISE 8.4.3. Let R be a commutative local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let M and N be finitely generated R-modules and $f \in \operatorname{Hom}_R(M,N)$. The following are equivalent.

(1) $f \otimes 1 : M \otimes_R k \to N \otimes_R k$ is an isomorphism.
(2) $\ker f \subseteq \mathfrak{m}M$ and f is onto.

EXERCISE 8.4.4. Let R be a commutative local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let M be a finitely generated R-module. Show that there exists an exact sequence
$$0 \to K \to R^n \xrightarrow{f} M \to 0$$
such that $f \otimes 1 : k^n \to M \otimes_R k$ is an isomorphism.

EXERCISE 8.4.5. Let R be a noetherian commutative local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let M be a finitely generated R-module. Show that there exists a resolution
$$\cdots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M \to 0$$
such that for all $i \geq 0$, F_i is a finitely generated free R-module and $\operatorname{im} d_{i+1} \subseteq \mathfrak{m}F_i$.

EXERCISE 8.4.6. Let R be a commutative noetherian ring, n a nonnegative integer, and M a finitely generated R-module. The following are equivalent.

(1) $\operatorname{proj.dim}_R(M) \leq n$.
(2) $\operatorname{Ext}_R^{n+1}(M,N) = 0$ for all finitely generated R-modules N.

EXERCISE 8.4.7. Let k be a field. Prove that $\operatorname{coh.dim}(k) = 0$.

EXERCISE 8.4.8. Let R be a PID. Prove that $\operatorname{coh.dim}(R) \leq 1$. Prove that R is a field if and only if $\operatorname{coh.dim}(R) = 0$.

EXERCISE 8.4.9. Let R be a commutative ring and M an R-module. If S is a submodule of M which is a direct summand of M, then $\operatorname{proj.dim}_R(S) \leq \operatorname{proj.dim}_R(M)$.

5. Group Cohomology

Let G be a group, written multiplicatively, with identity element denoted 1. Let $\mathbb{Z}G$ denote the group ring, as defined in Example 1.1.4. A left $\mathbb{Z}G$-module is also called a *G-module*. The augmentation map $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ is the homomorphism of rings induced by $G \to \langle 1 \rangle$. Via ε, any $\mathbb{Z}$-module A can be made into a *trivial G-module*. In this case, for every $x \in A$ and $\sigma \in G$ we have $\sigma x = x$. That is, every $\sigma \in G$ acts as the trivial automorphism of A. In particular, ε induces the trivial left $\mathbb{Z}G$-module structure on $\mathbb{Z}$.

DEFINITION 8.5.1. Let G be a group and A a left G-module. For $n \geq 0$, the *nth cohomology group of G with coefficients in A* is defined to be $\mathrm{H}^n(G,A) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},A)$, where $\mathbb{Z}$ has the trivial left $\mathbb{Z}G$-module structure. By Definition 8.3.8, the groups $\mathrm{H}^n(G,A)$ are isomorphic to the right derived groups of the left exact contravariant functor $\mathrm{Hom}_{\mathbb{Z}G}(\cdot,A)$, as well as the right right derived groups of the left exact covariant functor $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},\cdot)$. Exercise 8.5.2 shows that the groups $\mathrm{H}^n(G,A)$ are also isomorphic to the right derived groups of the left exact covariant functor $A \mapsto A^G$.

The goal of Sections 8.5.1 and 8.5.2 is to describe $\mathrm{H}^n(G,A)$ for $n = 0,1,2,3$. We do this by presenting formulas for generators and relations for the groups. First, in Section 8.5.1 we derive two free resolutions for the $\mathbb{Z}G$-module $\mathbb{Z}$. These are called the standard resolution and the bar resolution, respectively. In Section 8.5.2, starting from the standard resolution we apply the functor $\mathrm{Hom}_{\mathbb{Z}G}(\cdot,A)$ to get a cochain complex from which formulas for cocycles and coboundaries in low degrees are derived. After that, from the bar resolution of $\mathbb{Z}$, we repeat this process to get a cochain complex that leads us to the familiar normalized factor sets that are useful for the crossed product construction, for example.

In Section 8.5.3 some of the basic functorial properties of group cohomology are proved.

EXAMPLE 8.5.2. Suppose $G = \langle 1 \rangle$ is the trivial group and A is a $\mathbb{Z}$-module. Then $\mathrm{H}^n(G,A) = \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z},A)$. From Proposition 8.3.9 we find

$$\mathrm{H}^n(G,A) = \begin{cases} A & \text{if } n = 0, \\ 0 & \text{if } n > 0. \end{cases}$$

5.1. The Resolutions of $\mathbb{Z}$ by Free G-Modules. Throughout this section, G denotes a group. The group ring $\mathbb{Z}G$ is a free $\mathbb{Z}$-module on the index set G (see Example 1.6.10). For any $r \geq 1$, let $G^r = \prod_{i=1}^r G$ be the product of r copies of G. Elements of G^r are written as $(\sigma_1,\dots,\sigma_n)$, or sometimes as $(\sigma_0,\dots,\sigma_{n-1})$.

DEFINITION 8.5.3. By P_n we denote the free $\mathbb{Z}$-module on the index set G^{n+1}. The diagonal map $\delta : G \to G^{n+1}$, which is defined by $\sigma \mapsto (\sigma,\dots,\sigma)$ is a homomorphism of groups. By virtue of δ, G acts as a group of permutations of G^{n+1} by $\sigma(\sigma_0,\dots,\sigma_n) = (\sigma\sigma_0,\dots,\sigma\sigma_n)$. By this action, P_n is a left $\mathbb{Z}G$-module. For $0 \leq i \leq n$, the projection homomorphism $\pi_{n,i} : G^{n+1} \to G^n$ is defined by reducing modulo the ith factor. We signify this projection map on $n+1$-tuples by the "hat" notation: $\pi_{n,i}(\sigma_0,\dots,\sigma_n) = (\sigma_0,\dots,\hat{\sigma}_i,\dots,\sigma_n)$. For $n \geq 1$ define a boundary map $\partial_n : P_n \to P_{n-1}$ by specifying its value on a $\mathbb{Z}$-basis element to be

$$\partial_n(\sigma_0,\dots,\sigma_n) = \sum_{i=0}^{n} (-1)^i \pi_{n,i}(\sigma_0,\dots,\sigma_n).$$

Theorem 8.5.4 shows that when augmented by ε, we have a resolution

$$\cdots \to P_n \xrightarrow{\partial_n} P_{n-1} \xrightarrow{\partial_{n-1}} \cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

of $\mathbb{Z}$ by free $\mathbb{Z}G$-modules. This complex will be denoted $P_\bullet$.

THEOREM 8.5.4. *In the above context,*

(1) *$\pi_{n,i}$ induces a $\mathbb{Z}G$-module epimorphism $\pi_{n,i} : P_n \to P_{n-1}$.*
(2) *P_n is a free $\mathbb{Z}G$-module with basis $\{(1,\sigma_1,\dots,\sigma_n) \mid \sigma_i \in G\}$.*
(3) *∂_n is a $\mathbb{Z}G$-module homomorphism.*
(4) *$\partial_{n-1}\partial_n = 0$.*
(5) *The sequence $P_\bullet$ of Definition 8.5.3 is a free resolution of the $\mathbb{Z}G$-module $\mathbb{Z}$.*

PROOF. (1), (2), (3): Are left to the reader.

(4): The reader should verify that

$$\pi_{n-1,j}\pi_{n,i}(\sigma_0,\dots,\sigma_n) = \begin{cases} (\sigma_0,\dots,\hat{\sigma}_i,\dots,\hat{\sigma}_{j+1},\dots,\sigma_n) & \text{if } 0 \le i \le j < n \\ (\sigma_0,\dots,\hat{\sigma}_j,\dots,\hat{\sigma}_i,\dots,\sigma_n) & \text{if } 0 \le j < i \le n. \end{cases}$$

We have

$$\begin{aligned}
\partial_{n-1}\partial_n(\sigma_0,\dots,\sigma_n) &= \sum_{i=0}^{n}(-1)^i\partial_{n-1}(\pi_{n,i}(\sigma_0,\dots,\sigma_n)) \\
&= \sum_{i=0}^{n}(-1)^i\sum_{j=0}^{n-1}(-1)^j\pi_{n-1,j}\pi_{n,i}(\sigma_0,\dots,\sigma_n) \\
&= \sum_{i\le j}(-1)^{i+j}\pi_{n-1,j}\pi_{n,i}(\sigma_0,\dots,\sigma_n) + \sum_{i>j}(-1)^{i+j}\pi_{n-1,j}\pi_{n,i}(\sigma_0,\dots,\sigma_n)
\end{aligned}$$

and

$$\begin{aligned}
\sum_{i\le j}(-1)^{i+j}\pi_{n-1,j}\pi_{n,i}(\sigma_0,\dots,\sigma_n) &= \sum_{i\le j}(-1)^{i+j}(\sigma_0,\dots,\hat{\sigma}_i,\dots,\hat{\sigma}_{j+1},\dots,\sigma_n) \\
&= \sum_{i=0}^{n-1}\sum_{k=i+1}^{n}(-1)^{i+k+1}(\sigma_0,\dots,\hat{\sigma}_i,\dots,\hat{\sigma}_k,\dots,\sigma_n)
\end{aligned}$$

and

$$\begin{aligned}
\sum_{i>j}(-1)^{i+j}\pi_{n-1,j}\pi_{n,i}(\sigma_0,\dots,\sigma_n) &= \sum_{i>j}(-1)^{i+j}(\sigma_0,\dots,\hat{\sigma}_j,\dots,\hat{\sigma}_i,\dots,\sigma_n) \\
&= \sum_{j=0}^{n-1}\sum_{\ell=j+1}^{n}(-1)^{j+\ell}(\sigma_0,\dots,\hat{\sigma}_j,\dots,\hat{\sigma}_\ell,\dots,\sigma_n)
\end{aligned}$$

from which (4) follows.

(5): It follows from (4) and the fact that $\varepsilon(\sigma) = 1$, that $P_\bullet$ is a complex. To show that $P_\bullet$ is exact, we construct a contracting homotopy and apply Exercise 8.1.8. If $n \ge 0$, define $k_n : P_n \to P_{n+1}$ by specifying its value on a $\mathbb{Z}$-basis element: $k_n(\sigma_0,\dots,\sigma_n) = (1,\sigma_0,\dots,\sigma_n)$. Define $k_{-1} : \mathbb{Z} \to P_0$ by $k_{-1}(n) = (n\cdot 1)$. Notice that k_n is a $\mathbb{Z}$-module homomorphism, not a $\mathbb{Z}G$-module homomorphism. Nevertheless, to prove (5), this is sufficient. Extending the complex with 0 and taking $\partial_0 = \varepsilon$, we must verify that $\partial_{n+1}k_n + k_{n-1}\partial_n$ is the identity map on P_n, for all n. The first non-trivial case is $n = -1$. Since

$$\varepsilon k_{-1}(n) = \varepsilon(n\cdot 1) = n$$

the identity holds. For $n \ge 0$ we check the identity on a typical basis element. Then

$$\begin{aligned}
(\partial_{n+1}k_n + k_{n-1}\partial_n)(\sigma_0,\dots,\sigma_n) &= \partial_{n+1}(1,\sigma_0,\dots,\sigma_n) + k_{n-1}\sum_{i=0}^{n}(-1)^i(\sigma_0,\dots,\hat{\sigma}_i,\dots,\sigma_n) \\
&= (\sigma_0,\dots,\sigma_n) + \sum_{j=0}^{n}(-1)^{j+1}(1,\sigma_0,\dots,\hat{\sigma}_i,\dots,\sigma_n) \\
&\quad + \sum_{i=0}^{n}(-1)^i(1,\sigma_0,\dots,\hat{\sigma}_i,\dots,\sigma_n) \\
&= (\sigma_0,\dots,\sigma_n)
\end{aligned}$$

which completes the proof. $\square$

DEFINITION 8.5.5. For $n \geq 1$, we define Q_n to be the free $\mathbb{Z}G$-module on the index set G^n. To distinguish the basis elements of Q_n from those of P_n (see Definition 8.5.3), we use brackets instead of parentheses. The basis for Q_n is the set $\{[\sigma_1,\dots,\sigma_n] \mid \sigma_i \in G\}$. For consistency, define Q_0 to be the free $\mathbb{Z}G$-module on the singleton set $\{[\,]\}$. For $n \geq 1$ define a boundary map $d_n : Q_n \to Q_{n-1}$ by specifying its value on a typical basis element:

$$d_n[\sigma_1,\dots,\sigma_n] = \sigma_1[\sigma_2,\dots,\sigma_n] + \sum_{i=1}^{n-1}(-1)^i[\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\dots,\sigma_n] + (-1)^n[\sigma_1,\dots,\sigma_{n-1}].$$

Theorem 8.5.6 shows that when augmented by ε, we have a resolution of $\mathbb{Z}$ by free $\mathbb{Z}G$-modules. This complex will be denoted $Q_\bullet$ and is called the *unnormalized, or homogeneous, standard resolution*.

THEOREM 8.5.6. *The sequence*

$$\cdots \to Q_n \xrightarrow{d_n} Q_{n-1} \xrightarrow{d_{n-1}} \cdots \to Q_1 \xrightarrow{d_1} Q_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

is a free resolution of the $\mathbb{Z}G$*-module* $\mathbb{Z}$.

PROOF. The proof consists in showing that $Q_\bullet$ is isomorphic to the free resolution $P_\bullet$. Define $f_n : P_n \to Q_n$ by the formula

$$f_n(\sigma_0,\dots,\sigma_n) = \sigma_0[\sigma_0^{-1}\sigma_1,\sigma_1^{-1}\sigma_2,\dots,\sigma_{n-1}^{-1}\sigma_n].$$

Define $g_n : Q_n \to P_n$ by the formula

$$g_n[\sigma_1,\dots,\sigma_n] = (1,\sigma_1,\sigma_1\sigma_2,\sigma_1\sigma_2\sigma_3,\dots,\sigma_1\sigma_2\cdots\sigma_n).$$

The reader should verify that f_n and g_n are $\mathbb{Z}G$-module homomorphisms and that they are inverses to each other. The square

$$\begin{array}{ccc} P_n & \xrightarrow{\partial_n} & P_{n-1} \\ \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} \\ Q_n & \xrightarrow{d_n} & Q_{n-1} \end{array}$$

commutes for all $n \geq 1$ since

$$\begin{aligned} f_{n-1}\partial_n g_n[\sigma_1,\dots,\sigma_n] &= f_{n-1}\partial_n(1,\sigma_1,\sigma_1\sigma_2,\dots,\sigma_1\sigma_2\cdots\sigma_n) \\ &= \sum_{i=0}^{n}(-1)^i f_{n-1}(1,\sigma_1,\sigma_1\sigma_2,\dots,\sigma_1\sigma_2\cdots\sigma_n) \\ &= \sigma_1[\sigma_2,\dots,\sigma_n] + \sum_{i=1}^{n-1}(-1)^i[\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\dots,\sigma_n] \\ &\quad + (-1)^n[\sigma_1,\dots,\sigma_{n-1}] \\ &= d_n[\sigma_1,\dots,\sigma_n]. \end{aligned}$$

Therefore, $Q_\bullet$ is a complex, and $f : P_\bullet \to Q_\bullet$ is an isomorphism of complexes. The rest follows from Lemma 8.2.3. □

DEFINITION 8.5.7. Let $G_1 = G - \langle 1\rangle = \{\sigma \in G \mid \sigma \neq 1\}$. For $n \geq 1$ define B_n to be the $\mathbb{Z}G$-submodule of Q_n (see Definition 8.5.5) generated by those basis elements $[\sigma_1,\dots,\sigma_n]$ which belong to G_1^n. We take $B_0 = Q_0$, the free module on $[\,]$. The set inclusion map

$G_1^n \subseteq G^n$ induces an idempotent $\eta_n \in \operatorname{Hom}_{\mathbb{Z}G}(Q_n, Q_n)$ which projects Q_n onto B_n. The boundary map $d_n : B_n \to B_{n-1}$ is defined to be the inclusion map $B_n \subseteq Q_n$ followed by the boundary map $d_n : Q_n \to Q_{n-1}$ of Definition 8.5.5 followed by η_{n-1}. By construction, the diagram

$$\begin{tikzcd} B_n \arrow[rr, "d_n"] \arrow[d, "\subseteq"] & & B_{n-1} \arrow[d, "\subseteq"] \\ Q_n \arrow[r, "d_n"] & Q_{n-1} \arrow[r, "\eta_{n-1}"] & Q_{n-1} \end{tikzcd}$$

commutes. Theorem 8.5.8 shows that when augmented with $\varepsilon : B_0 \to \mathbb{Z}$, this is a free $\mathbb{Z}G$-module resolution of $\mathbb{Z}$. This complex is denoted $B_\bullet$, and is called the *bar resolution*, or *normalized standard resolution*.

THEOREM 8.5.8. *In the context of Definition 8.5.7,*

$$\cdots \to B_n \xrightarrow{d_n} B_{n-1} \xrightarrow{d_{n-1}} \cdots \to B_1 \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

is a free resolution of the $\mathbb{Z}G$-module $\mathbb{Z}$.

PROOF. We must show that $d_{n-1}d_n = 0$, and that the homology of the complex is (0). Take B_{-1} to be $\mathbb{Z}$ and d_0 to be ε. Define $\mathbb{Z}$-module homomorphisms $h_n : B_n \to B_{n+1}$ for each $n \geq -1$. The map $h_{-1} : \mathbb{Z} \to B_0$ is induced by the natural homomorphism of rings $\mathbb{Z} \to \mathbb{Z}G$. For $n \geq 0$, B_n is generated as a free $\mathbb{Z}$-module by elements of the form $\sigma[\sigma_1, \dots, \sigma_n]$, where $\sigma \in G$, and $[\sigma_1, \dots, \sigma_n] \in G_1^n$. The map h_n is defined by

$$h_n(\sigma[\sigma_1, \dots, \sigma_n]) = \eta_{n+1}[\sigma, \sigma_1, \dots, \sigma_n].$$

First we check that the contracting homotopy relations

$$d_{n+1}h_n + h_{n-1}d_n = 1_{B_n}$$

are satisfied. For $n = 0$ we get

$$d_0 h_{-1}(1) = d_0[\,] = \varepsilon(1) = 1$$

For $n = 1$,

$$(d_1h_0 + h_{-1}d_0)(\sigma[\,]) = d_0\eta_1[\sigma] + \varepsilon(\sigma) = \begin{cases} \varepsilon(1) = [\,] & \text{if } \sigma = 1 \\ d_1[\sigma] = \sigma[\,] & \text{if } \sigma \neq 1 \end{cases}$$

Now suppose $n > 1$. First assume $\sigma = 1$. The reader should verify that

$$d_{n+1}h_n[\sigma_1, \dots, \sigma_n] = 0$$

and

$$h_{n-1}d_n[\sigma_1, \dots, \sigma_n] = [\sigma_1, \dots, \sigma_n]$$

so the formula holds. Now assume $\sigma \neq 1$. Then

$$\begin{aligned} d_{n+1}h_n(\sigma[\sigma_1, \dots, \sigma_n]) &= d_{n+1}[\sigma, \sigma_1, \dots, \sigma_n] \\ &= \sigma[\sigma_1, \dots, \sigma_n] - [\sigma\sigma_1, \sigma_2, \dots, \sigma_n] \\ &\quad + \sum_{i=1}^{n-1} (-1)^{i+1}[\sigma, \sigma_1, \dots, \sigma_i\sigma_{i+1}, \dots, \sigma_n] \\ &\quad + (-1)^{n+1}[\sigma, \sigma_1, \dots, \sigma_{n-1}] \end{aligned}$$

and

$$\begin{aligned}h_{n-1}d_n(\sigma[\sigma_1,\dots,\sigma_n]) &= h_{n-1}\Big(\sigma\sigma_1[\sigma_2,\dots,\sigma_n]+\sum_{i=1}^{n-1}(-1)^i\sigma[\sigma_1,\dots,\sigma_i\sigma_{i+1},\dots,\sigma_n]\\ &\qquad +(-1)^n\sigma[\sigma_1,\dots,\sigma_{n-1}]\Big)\\ &= [\sigma\sigma_1,\sigma_2,\dots,\sigma_n]+\sum_{i=1}^{n-1}(-1)^i[\sigma,\sigma_1,\dots,\sigma_i\sigma_{i+1},\dots,\sigma_n]\\ &\qquad +(-1)^n[\sigma,\sigma_1,\dots,\sigma_{n-1}]\end{aligned}$$

From this we get $d_{n+1}h_n + h_{n-1}d_n = 1_{B_n}$. To finish, we must show $d_nd_{n+1} = 0$. The proof is by induction on n. The basis step follows from $d_0d_1[\sigma] = \varepsilon\sigma[] = 0$, since $\sigma \neq 1$. Notice that the image of h_n contains a $\mathbb{Z}G$-basis for B_{n+1}. Inductively assume $n > 0$ and $d_{n-1}d_n = 0$. Using the identity $d_{n+1}h_n + h_{n-1}d_n = 1_{B_n}$, we get

$$\begin{aligned}d_nd_{n+1}h_n &= d_n(1_{B_n} - h_{n-1}d_n)\\ &= d_n1_{B_n} - d_nh_{n-1}d_n)\\ &= d_n - (1_{B_n} - h_{n-2}d_{n-1})d_n\\ &= d_n - d_n + h_{n-2}d_{n-1}d_n\\ &= 0.\end{aligned}$$

Applying Exercise 8.1.8 completes the proof. □

5.2. Cocycle and Coboundary Groups in Low Degree. Let A be a $\mathbb{Z}G$-module. So A is an abelian group with binary operation written additively, and G acts as a group on A. The cohomology groups $\mathrm{H}^n(G,A)$ are defined to be $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},A)$. If $Q_\bullet \to \mathbb{Z}$ is the standard (homogeneous) resolution from Definition 8.5.5, and $B_\bullet \to \mathbb{Z}$ is the bar resolution from Definition 8.5.7, then by Definition 8.3.8, we have

$$\begin{aligned}\mathrm{H}^n(G,A) &= \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},A)\\ &= \mathrm{H}^n(\mathrm{Hom}_{\mathbb{Z}G}(Q_\bullet,A))\\ &= \mathrm{H}^n(\mathrm{Hom}_{\mathbb{Z}G}(B_\bullet,A)).\end{aligned}$$

Notice that $\mathrm{H}^n(\mathrm{Hom}_{\mathbb{Z}G}(Q_\bullet,A))$ is an abelian group, where functions are added point-wise: $(f+g)(x) = f(x)+g(x)$. Since $Q_0 = \mathbb{Z}G$, we have $\mathrm{Hom}_{\mathbb{Z}G}(Q_0,A) = A$ (Lemma 2.4.7). For $n \geq 1$, because Q_n is the free $\mathbb{Z}G$-module on G^n, we can identify $\mathrm{Hom}_{\mathbb{Z}G}(Q_n,A)$ with $\mathrm{Map}(G^n,A)$, the set of all functions mapping G^n to A. The cochain map

$$\mathrm{Hom}_{\mathbb{Z}G}(Q_{n-1},A) \xrightarrow{d^{n-1}} \mathrm{Hom}_{\mathbb{Z}G}(Q_n,A)$$

is defined by $d^{n-1}(f) = fd_n$. Using the formula for the boundary d_n in Definition 8.5.5, on a typical basis element of Q_n we have

$$\begin{aligned}(5.1)\quad d^{n-1}(f)[\sigma_1,\dots,\sigma_n] &= fd_n[\sigma_1,\dots,\sigma_n]\\ &= \sigma_1 f[\sigma_2,\dots,\sigma_n]+\sum_{i=1}^{n-1}(-1)^i f[\sigma_1,\dots,\sigma_i\sigma_{i+1},\dots,\sigma_n]+(-1)^n f[\sigma_1,\dots,\sigma_{n-1}].\end{aligned}$$

In the first summand, we have used the fact that f is $\mathbb{Z}G$-linear. For all $n \geq 0$,

$$\mathrm{H}^n(G,A) = \mathrm{Z}^n(G,A)/\mathrm{B}^n(G,A)$$

where $\mathrm{Z}^n(G,A) = \ker d^n$, and $\mathrm{B}^n(G,A) = \operatorname{im} d^{n-1}$. By convention, $d^{-1} = 0$ and $\mathrm{B}^0(G,A) = 0$.

PROPOSITION 8.5.9. *In the above context,*

(1) $\mathrm{H}^0(G,A) = \mathrm{Z}^0(G,A) = A^G$ *is the subset of* A *fixed by* G.
(2) $\mathrm{Z}^1(G,A)$ *is the set of all functions* $f : G \to A$ *such that*

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau),$$

for all $(\sigma, \tau) \in G^2$.
(3) $\mathrm{B}^1(G,A)$ *is the set of all functions* $f : G \to A$ *such that there exists* $x \in A$ *and* $f(\sigma) = \sigma(x) - x$, *for all* $\sigma \in G$.
(4) $\mathrm{Z}^2(G,A)$ *is the set of all functions* $f : G \times G \to A$ *such that*

$$f(\rho, \sigma) + f(\rho\sigma, \tau) = \rho f(\sigma, \tau) + f(\rho, \sigma\tau),$$

for all $(\rho, \sigma, \tau) \in G^3$.
(5) $\mathrm{B}^2(G,A)$ *is the set of all functions* $f : G \times G \to A$ *such that there exists* $g : G \to A$ *and* $f(\sigma, \tau) = \sigma g(\tau) - g(\sigma\tau) + g(\sigma)$, *for all* $(\sigma, \tau) \in G^2$.

PROOF. Follows straight from (5.1) and the definitions. □

COROLLARY 8.5.10. *In the above context, the normalized cocycles and coboundaries in degrees* 1 *and* 2 *are:*

(1) $\mathrm{Z}^1(G,A)$ *is the set of all functions* $f : G \to A$ *such that* $f(1) = 0$, *and*

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau),$$

for all $(\sigma, \tau) \in G^2$.
(2) $\mathrm{Z}^2(G,A)$ *is the set of all functions* $f : G \times G \to A$ *such that*

$$f(\rho, \sigma) + f(\rho\sigma, \tau) = \rho f(\sigma, \tau) + f(\rho, \sigma\tau),$$

and $f(1, \tau) = f(\sigma, 1) = 0$, *for all* $(\rho, \sigma, \tau) \in G^3$.
(3) $\mathrm{B}^2(G,A)$ *is the set of all functions* $f : G \times G \to A$ *such that there exists* $g : G \to A$ *where* $g(1) = 0$ *and* $f(\sigma, \tau) = \sigma g(\tau) - g(\sigma\tau) + g(\sigma)$, *for all* $(\sigma, \tau) \in G^2$.

PROOF. Use the bar resolution $B_\bullet \to \mathbb{Z}$. In (5.1), d_n is zero whenever 1 appears in the n-tuple. Notice that elements of $\mathrm{B}^1(G,A)$ are always normalized. □

REMARK 8.5.11. For the record, we mention that the group $\mathrm{Z}^3(G,A)$ is the set of all $f : G^3 \to A$ such that the 3-cocycle identity

$$f(\sigma_1\sigma_2, \sigma_3, \sigma_4) + f(\sigma_1, \sigma_2, \sigma_3\sigma_4) = f(\sigma_1, \sigma_2, \sigma_3) + \sigma_1 f(\sigma_2, \sigma_3, \sigma_4) + f(\sigma_1, \sigma_2\sigma_3, \sigma_4)$$

is satisfied for all $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in G^4$. Moreover, to compute $\mathrm{H}^3(G,A)$, normalized cocycles can be used. That is, $f(\sigma_1, \sigma_2, 1) = f(\sigma_1, 1, \sigma_3) = f(1, \sigma_2, \sigma_3) = 0$. The set of 3-coboundaries, $\mathrm{B}^3(G,A)$, consists of all $f : G^3 \to A$ for which there exists $g : G \times G \to A$ and

$$f(\rho, \sigma, \tau) = \rho g(\sigma, \tau) - g(\rho\sigma, \tau) + g(\rho, \sigma\tau) - g(\sigma, \tau)$$

for all $(\rho, \sigma, \tau) \in G^3$.

5.3. Applications and Computations. Some of the basic functorial properties of group cohomology are proved. In general $\mathrm{H}^n(G,A)$ is a covariant functor in the second variable, and a contravariant functor in the first variable. Many of the theorems and definitions are stated in the context where H is a subgroup of G and A is an H-module. Then $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)$ is called the induced G-module. Shapiro's Lemma shows that the cohomology of A as an H-module is equal to the cohomology of the induced G-module. If A is a G-module and H is a subgroup of G, then there are the restriction and corestriction homomorphisms. If H is normal, there is also an inflation homomorphism. If G is a finite cyclic group, we derive formulas for the cohomology of a G-module A in terms of the norm and difference maps on A. We prove Hilbert's Theorem 90, when G is a finite group of automorphisms of a field F.

DEFINITION 8.5.12. Let G be a group.

(1) If $\theta : G \to K$ is a homomorphism of groups, and A is a $\mathbb{Z}K$-module, then the ring homomorphism $\theta : \mathbb{Z}G \to \mathbb{Z}K$ makes A into a $\mathbb{Z}G$-module.
(2) If H is a subgroup of G and A is a $\mathbb{Z}H$-module, then $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)$ is a left $\mathbb{Z}G$-module (see Lemma 2.4.1(1)) which is called the *induced G-module*.

THEOREM 8.5.13. *(Shapiro's Lemma) Let G be a group, H a subgroup of G, and A a $\mathbb{Z}H$-module. There are isomorphisms*

$$\mathrm{H}^n(H,A) \cong \mathrm{H}^n(G,\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A))$$

which are induced by the adjoint isomorphism of Theorem 2.4.10.

PROOF. Since $\mathbb{Z}G$ is a free left $\mathbb{Z}H$-module, this follows directly from the isomorphism

$$\mathrm{Ext}^n_{\mathbb{Z}H}(\mathbb{Z}G \otimes_{\mathbb{Z}G} \mathbb{Z},A) \cong \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A))$$

of Lemma 8.3.11 (2). It is also of interest to know how this map is defined on cochains. Let $Q_\bullet \to Z$ be the standard resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module. By Proposition 2.1.13 (5), $Q_\bullet \to Z$ is also a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}H$-module. The adjoint isomorphism

$$\mathrm{Hom}_{\mathbb{Z}H}(Q_n,A) \xrightarrow{\phi} \mathrm{Hom}_{\mathbb{Z}G}(Q_n,\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A))$$

maps an n-cochain f to ϕf. If $y \in Q_n$, then $(\phi f)(y)$ is the element of $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)$ defined by $(\phi f)(y)(x) = f(xy)$. The details are left to the reader. □

LEMMA 8.5.14. *Let G be a group and A a $\mathbb{Z}G$-module.*

(1) If $\psi : A \to B$ is a homomorphism of $\mathbb{Z}G$-modules, then ψ induces a homomorphism

$$\mathrm{H}^n(G,A) \to \mathrm{H}^n(G,B)$$

of abelian groups, for each $n \geq 0$.

(2) If $\theta : H \to G$ is a homomorphism of groups, then θ induces a homomorphism

$$\mathrm{H}^n(G,A) \to \mathrm{H}^n(H,A)$$

of abelian groups, for each $n \geq 0$.

PROOF. (1): Follows from the fact that $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},\cdot)$ is a covariant functor (see Section 8.3.4).

(2): Let $(Q_G)_\bullet \to \mathbb{Z}$ be the standard resolution for the $\mathbb{Z}G$-module $\mathbb{Z}$, and $(Q_H)_\bullet \to \mathbb{Z}$ the counterpart for the $\mathbb{Z}H$-module. The homomorphism $\theta : H \to G$ induces a homomorphism $H^n \to G^n$, for each n. For each n, $(Q_H)_n$ is free on H^n and $(Q_H)_n$ is free on G^n.

Hence there is an induced morphism

$$\theta : (Q_G)_\bullet \to (Q_H)_\bullet \tag{5.2}$$

of complexes. Now suppose A is a $\mathbb{Z}G$-module, which is made into a $\mathbb{Z}H$-module by virtue of $\theta : \mathbb{Z}H \to \mathbb{Z}G$. There are morphisms of complexes

$$\operatorname{Hom}_{\mathbb{Z}G}((Q_G)_\bullet, A) \to \operatorname{Hom}_{\mathbb{Z}G}((Q_H)_\bullet, A) \to \operatorname{Hom}_{\mathbb{Z}H}((Q_H)_\bullet, A)$$

where the first morphism is induced by the functor $\operatorname{Hom}_{\mathbb{Z}G}(\cdot, A)$ applied to the morphism (5.2) and the second is induced by the map defined in Exercise 1.1.4. The rest follows from Lemma 8.1.3. □

Given a group G, a G-module A, and a subgroup H, there are two standard homomorphisms on cohomology groups. These are the restriction and corestriction maps described in Definition 8.5.15. When H is a normal subgroup, there is a third homomorphism, called the inflation map.

DEFINITION 8.5.15. Let G be a group and A a $\mathbb{Z}G$-module.

(1) If H is a subgroup of G, then the homomorphism of abelian groups

$$\operatorname{Res} : \mathrm{H}^n(G, A) \to \mathrm{H}^n(H, A)$$

defined in Lemma 8.5.14 (2) is called the *restriction homomorphism*. Suppose $f : G^n \to A$ is an n-cocycle in $\mathrm{Z}^n(G, A)$. Viewing H^n as a subset of G^n, the restriction of f defines $g : H^n \to A$ which is an n-cocycle in $\mathrm{Z}^n(H, A)$. The restriction homomorphism maps the cohomology class $\bar{f}$ to $\bar{g}$.

(2) If N is a normal subgroup of G, then A^N can be made into a $\mathbb{Z}(G/N)$-module. The multiplication rule is induced by $(gN)x = gx$. The natural map $\eta : G \to G/N$ and the set inclusion $\iota : A^N \to A$ induce homomorphisms

$$\begin{tikzcd} \mathrm{H}^n(G/N, A^N) \arrow[rr, "\mathrm{Inf}"] \arrow[dr, "\eta"'] & & \mathrm{H}^n(G, A) \\ & \mathrm{H}^n(G, A^N) \arrow[ur, "\iota"'] & \end{tikzcd}$$

and the composite map, Inf, is called the *inflation homomorphism*. Suppose $f : (G/H)^n \to A^H$ is an n-cocycle in $\mathrm{Z}^n(G/H, A^H)$. Define $g : G^n \to A$ by the rule $g(\sigma_1, \dots, \sigma_n) = f(\bar{\sigma}_1, \dots, \bar{\sigma}_n)$, where $\bar{\sigma}_i$ is the coset represented by σ_i in G/H. Then g is an n-cocycle in $\mathrm{Z}^n(G, A)$, and the inflation homomorphism maps the cohomology class $\bar{f}$ to $\bar{g}$.

(3) Suppose H is a subgroup of G of finite index $[G : H] = m$ and $x_1, \dots, x_m$ is a full set of left coset representatives for H. Let A be a left $\mathbb{Z}G$-module. The reader should verify that the map

$$\operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A) \xrightarrow{\psi} A$$

defined by $\psi(f) = \sum_{i=1}^m x_i f(x_i^{-1})$ is a homomorphism of $\mathbb{Z}G$-modules and does not depend on the choices of $x_1, \dots, x_m$. This defines a homomorphism on cohomology groups

$$\mathrm{H}^n(G, \operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)) \xrightarrow{\psi} \mathrm{H}^n(G, A).$$

The *corestriction homomorphism*, denoted Cor, is defined by composing ψ with the isomorphism from Shapiro's Lemma (Theorem 8.5.13). By definition, the diagram

$$\begin{tikzcd} \mathrm{H}^n(H,A) \arrow[rr, "\mathrm{Cor}"] \arrow[dr, "\cong"'] & & \mathrm{H}^n(G,A) \\ & \mathrm{H}^n(G, \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)) \arrow[ur, "\psi"'] & \end{tikzcd}$$

commutes. Using the description of the isomorphism in the proof of Theorem 8.5.13, we can describe the corestriction map on n-cocycles. Say f is a cocycle in $\mathrm{Hom}_{\mathbb{Z}H}(Q_n,A)$ defining a cohomology class c in $\mathrm{H}^n(H,A)$. Then $\mathrm{Cor}(f)$ is a cocycle in $\mathrm{Hom}_{\mathbb{Z}G}(Q_n,A)$ which represents a cohomology class $\mathrm{Cor}(c)$ in $\mathrm{H}^n(G,A)$. If $y \in Q_n$, then

$$\mathrm{Cor}(f)(y) = \sum_{i=1}^{m} x_i \phi(f)(y)(x_i^{-1}) = \sum_{i=1}^{m} x_i f(x_i^{-1}y).$$

For example, consider the $n = 0$ case. From Proposition 8.5.9, $\mathrm{Z}^0(H,A) = A^H$. Then f is a constant valued function, say $f(x) = a$. In this case, $\mathrm{Cor}(f)$ is the constant valued function $\sum_{i=1}^{m} x_i a$. For a Galois extension of fields K/k with group G, the corestriction homomorphism in degree zero is the trace of Section 1.8.2, when $A = K^+$, and it is the norm map when $A = K^*$.

THEOREM 8.5.16. *Let H be a subgroup of G of finite index $[G:H] = m$. If A is a left $\mathbb{Z}G$-module, then*

$$\mathrm{Cor}\,\mathrm{Res}\,\mathrm{H}^n(G,A) = m\,\mathrm{H}^n(G,A).$$

PROOF. Use the description of the corestriction given in Definition 8.5.15. Let f be a cocycle in $\mathrm{Hom}_{\mathbb{Z}H}(Q_n,A)$ defining a cohomology class c in $\mathrm{H}^n(H,A)$. If f is in the image of $\mathrm{Res} : \mathrm{H}^n(G,A)$, then f is $\mathbb{Z}G$-linear. For any $y \in Q_n$,

$$\mathrm{Cor}(f)(y) = \sum_{i=1}^{m} x_i f(x_i^{-1}y) \sum_{i=1}^{m} x_i x_i^{-1} f(y) = mf(y)$$

which proves the claim. $\square$

COROLLARY 8.5.17. *If G is a finite group of order m and A is any $\mathbb{Z}G$-module, then $m\mathrm{H}^n(G,A) = 0$ for all $n \geq 1$.*

PROOF. If $H = \langle 1 \rangle$, then $[G:H] = m$. By Theorem 8.5.16, the diagram

$$\begin{tikzcd} \mathrm{H}^n(G,A) \arrow[rr, "m"] \arrow[dr, "\mathrm{Res}"'] & & \mathrm{H}^n(G,A) \\ & \mathrm{H}^n(H,A) \arrow[ur, "\mathrm{Cor}"'] & \end{tikzcd}$$

commutes, where the horizontal map is "multiplication by m". By Proposition 8.3.9(3), the group $\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z},A) = \mathrm{H}^n(\langle 1 \rangle, A)$ is trivial for $n \geq 1$. $\square$

If $[G:H]$ is finite, we prove in Lemma 8.5.18 that the induced module is isomorphic to the tensor product $\mathbb{Z}G \otimes_{\mathbb{Z}H} A$.

LEMMA 8.5.18. *Let H be a subgroup of G of finite index $[G:H]=m$ and $x_1,\dots,x_m$ a full set of left coset representatives for H. If A is a left $\mathbb{Z}H$-module, then there is an isomorphism of $\mathbb{Z}G$-modules*

$$\operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)\xrightarrow{\psi}\mathbb{Z}G\otimes_{\mathbb{Z}H}A$$

defined by $\psi(f)=\sum_{i=1}^m x_i\otimes f(x_i^{-1})$.

PROOF. The reader should verify that the map ψ does not depend on the choices for $x_1,\dots,x_m$. Notice that $\mathbb{Z}G\cong\bigoplus_{i=1}^m x_i\mathbb{Z}H$ as right $\mathbb{Z}H$-modules. By Lemma 2.3.15,

$$\mathbb{Z}G\otimes_{\mathbb{Z}H}A\cong\bigoplus_{i=1}^m x_i\otimes_{\mathbb{Z}H}A$$

as left $\mathbb{Z}$-modules. Also, $\mathbb{Z}G\cong\bigoplus_{i=1}^m\mathbb{Z}Hx_i^{-1}$ as left $\mathbb{Z}H$-modules. By Proposition 2.4.8,

$$\operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)\cong\bigoplus_{i=1}^m\operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}Hx_i^{-1},A)$$

as left $\mathbb{Z}$-modules. The reader should verify that f in $\operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}Hx_i^{-1},A)$ is mapped by ψ to $x_i\otimes f(x_i^{-1})$ and hence ψ is bijective. We check that ψ is $\mathbb{Z}G$-linear. Let $g\in G$. Right multiplication by g is a permutation of the right cosets of H. For each i, there is a unique i' and $h_i\in H$ such that $x_i^{-1}g=h_ix_{i'}^{-1}$, or equivalently $x_ih_i=gx_{i'}$. Let $f\in\operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)$. For $x\in\mathbb{Z}G$, $(gf)(x)=f(xg)$. Therefore, $\psi(gf)=\sum x_i\otimes f(x_i^{-1}g)=\sum x_i\otimes f(h_ix_{i'}^{-1})=\sum x_ih_i\otimes f(x_{i'}^{-1})=\sum gx_{i'}\otimes f(x_{i'}^{-1})=g\psi(f)$. □

5.3.1. *Cohomology of a Finite Cyclic Group.* When G is a finite cyclic group, we see in Lemma 8.5.19 that $\mathbb{Z}$ has a free $\mathbb{Z}G$-resolution where each term is free of rank one.

LEMMA 8.5.19. *Let $G=\langle\sigma\rangle$ be a finite cyclic group of order m. In $\mathbb{Z}G$, let $D=\sigma-1$, and $N=1+\sigma+\cdots+\sigma^{m-1}$. Then multiplication by D and N, together with the augmentation map ε define an exact sequence*

$$\cdots\xrightarrow{N}\mathbb{Z}G\xrightarrow{D}\mathbb{Z}G\xrightarrow{N}\mathbb{Z}G\xrightarrow{D}\mathbb{Z}G\xrightarrow{\rho}\mathbb{Z}\to 0$$

which is a free resolution of the trivial $\mathbb{Z}G$-module $\mathbb{Z}$.

PROOF. The maps are $\mathbb{Z}G$-module homomorphisms because G is abelian. The kernel of ε is equal to the image of D, by Example 1.1.4. The sequence is a complex, since $DN=ND=0$. Let $x=\sum a_i\sigma^i$ be a typical element of $\mathbb{Z}G$. Then

$$\begin{aligned}x&=a_0+a_1\sigma+a_2\sigma^2+\cdots+a_{m-1}\sigma^{m-1}\\ \sigma x&=a_{m-1}+a_0\sigma+a_1\sigma^2+\cdots+a_{m-2}\sigma^{m-1}\\ \sigma^2x&=a_{m-2}+a_{m-1}\sigma+a_0\sigma^2+\cdots+a_{m-3}\sigma^{m-1}\\ &\vdots\\ \sigma^{m-1}x&=a_1+a_2\sigma+a_3\sigma^2+\cdots+a_0\sigma^{m-1}\end{aligned}\tag{5.3}$$

If $x=\sigma x$, then (5.3) shows that $a_0=a_1=\cdots=a_{m-1}$, hence $x=Na_0$. Thus $\ker D=\operatorname{im}N$. It follows from (5.3) that $Nx=(\sum_i a_i)N$. If $Nx=0$, then $\sum_i a_i=0$. Hence, the kernel of N is equal to the kernel of ε. Thus $\ker N=\operatorname{im}D$. □

Let $G = \langle \sigma \rangle$ be a finite cyclic group of order m. In $\mathbb{Z}G$, let $D = \sigma - 1$, and $N = 1 + \sigma + \cdots + \sigma^{m-1}$. Because G is abelian, for any $\mathbb{Z}G$-module A, left multiplication by D and N define $\mathbb{Z}G$-module endomorphisms in $\operatorname{Hom}_{\mathbb{Z}G}(A,A)$. We call D the *difference map on* A, and N the *norm map on* A. The images are denoted DA and NA, respectively. The kernel of D is A^G, and the kernel of N is denoted ${}_NA = \{x \in A \mid Nx = 0\}$. The reader should verify that the groups DA, NA and ${}_NA$ do not depend on the choice of σ.

THEOREM 8.5.20. *Let G be a finite cyclic group. For any $\mathbb{Z}G$-module A,*

$$\mathrm{H}^n(G,A) = \begin{cases} A^G & \text{if } n = 0, \\ {}_NA/DA & \text{if } n \text{ is odd,} \\ A^G/NA & \text{if } n > 0 \text{ is even.} \end{cases}$$

PROOF. Apply the functor $\operatorname{Hom}_{\mathbb{Z}G}(\cdot,A)$ to the resolution of $\mathbb{Z}$ in Lemma 8.5.19. □

COROLLARY 8.5.21. *If G is a finite cyclic group of order m and A is a trivial $\mathbb{Z}G$-module, then*

$$\mathrm{H}^n(G,A) = \begin{cases} A & \text{if } n = 0, \\ {}_mA & \text{if } n \text{ is odd,} \\ A/mA & \text{if } n > 0 \text{ is even,} \end{cases}$$

where ${}_mA = \{x \in A \mid mx = 0\}$, and $mA = \{mx \mid x \in A\}$.

PROOF. The map D is the zero operator on A, and N is the multiplication by m operator. □

COROLLARY 8.5.22. *Let $G = \langle \sigma \rangle$ be a finite cyclic group of order n and A a $\mathbb{Z}G$-module (written multiplicatively). If $m \mid n$, $\tau = \sigma^{n/m}$, and $H = \langle \tau \rangle$ is the subgroup of order m, then the image of the inflation homomorphism (Definition 8.5.15 (2))*

$$\operatorname{Inf} : \mathrm{H}^2(G/H, A^H) \to \mathrm{H}^2(G,A)$$

is divisible by m. That is, for any $z \in \mathrm{H}^2(G/H, A^H)$, there exists $y \in \mathrm{H}^2(G,A)$ such that $\operatorname{Inf}(z) = y^m$.

PROOF. Let $\bar{z} \in \mathrm{H}^2(G/H, A^H)$. Write $\bar{\sigma}$ for the coset represented by σ in G/H. By Exercise 8.5.9, there is $a \in A^G$ such that $\bar{z}$ is represented by a 2-cocycle $z : (G/H) \times (G/H) \to A^H$ of the form

$$z(\bar{\sigma}^i, \bar{\sigma}^j) = \begin{cases} 1 & \text{if } i + j < n/m \\ a & \text{if } i + j \geq n/m \end{cases}$$

for $0 \leq i, j < n/m$. The image of $\bar{z}$ under the inflation homomorphism is represented by the 2-cocycle $\xi : G \times G \to A$ defined by $\xi(\sigma^i, \sigma^j) = z(\bar{\sigma}^i, \bar{\sigma}^j)$. By Exercise 8.5.9, there is an isomorphism $\mathrm{H}^2(G,A) \to A^G/NA$ which is induced by $\xi \mapsto a_\xi$, where

$$\begin{aligned} a_\xi &= \prod_{j=0}^{n-1} \xi(\sigma^j, \sigma) \\ &= \prod_{k=0}^{m-1} \prod_{i=0}^{n/m-1} \xi\left((\sigma^{n/m})^k \sigma^i, \sigma\right) \\ &= a^m. \end{aligned}$$

By Exercise 8.5.9, ξ is cohomologous to χ_a^m, where

$$\chi_a(\sigma^i,\sigma^j) = \begin{cases} 1 & \text{if } i+j<n \\ a & \text{if } i+j \geq n \end{cases}$$

for $0 \leq i,j < n$. □

5.3.2. *Application to Galois Cohomology of Fields.* Let F be a field and G a finite group of automorphisms of F. Write F^+ for the additive group of F, and F^* for the group of units. Theorem 8.5.23 is a generalization of [**19**, Theorem 5.5.4].

THEOREM 8.5.23. *Let F be a field and G a finite group of automorphisms of F.*
(1) (Hilbert's Theorem 90) $\mathrm{H}^1(G,F^*) = \langle 1\rangle$.
(2) For all $n \geq 1$, $\mathrm{H}^n(G,F^+) = \langle 0\rangle$.

PROOF. (1): Let $f \in \mathrm{Z}^1(G,F^*)$ be a 1-cocycle. By Proposition 8.5.9, we can assume $f : G \to F^*$ and $f(\sigma\tau) = f(\sigma)\sigma f(\tau)$. By [**19**, Lemma 5.3.7], there exists $x \in F$ such that

$$\alpha = \sum_{\tau\in G} f(\tau)\tau(x) \neq 0.$$

In other words, α is a unit in F. For any $\sigma \in G$ we have $\sigma(\alpha) = \sum_{\tau\in G} \sigma f(\tau)\sigma\tau(x)$. By the 1-cocycle identity, $\sigma(\alpha) = \left(\sum_{\tau\in G} \sigma f(\sigma\tau)\sigma\tau(x)\right) f(\sigma)^{-1} = \alpha f(\sigma)^{-1}$. Therefore, $f(\sigma) = \alpha/\sigma(\alpha)$, for all $\sigma \in G$, which proves f is the 1-coboundary defined by α.
(2): By Exercise 8.5.3, $F^+ \cong \mathbb{Z}G \otimes_{\mathbb{Z}} k^+$. This follows from Exercise 8.5.5 (1). □

COROLLARY 8.5.24. *Let F be a finite field, G a group of automorphisms of F, and $k = F^G$. Then*

$$\mathrm{H}^n(G,F^*) = \begin{cases} k^* & \text{if } n = 0, \\ \langle 1\rangle & \text{if } n > 0. \end{cases}$$

PROOF. By Theorem 1.8.7, G is a finite cyclic group. If $n = 0$ or n is odd, this follows from Theorem 8.5.23 and Theorem 8.5.20. If n is even, then by Exercise 1.8.5, $NF^* = k^*$, and this follows from Theorem 8.5.20. □

5.4. Exercises.

EXERCISE 8.5.1. Let $F_n = (\mathbb{Z}G)^{\otimes(n+1)}$ be the tensor product of $n+1$ copies of the $\mathbb{Z}$-module $\mathbb{Z}G$. Make F_n into a left $\mathbb{Z}G$-module by acting on the left factor: $\sigma(\sigma_0 \otimes \sigma_1 \otimes \cdots \otimes \sigma_n) = \sigma\sigma_0 \otimes \sigma_1 \otimes \cdots \otimes \sigma_n$. Prove that F_n is isomorphic as a $\mathbb{Z}G$-module to P_n.

EXERCISE 8.5.2. Let G be a group.
(1) Show that the assignment $\mathfrak{F}^G(A) = A^G$ defines a left exact covariant functor from ${}_{\mathbb{Z}G}\mathfrak{M}$ to ${}_{\mathbb{Z}}\mathfrak{M}$.
(2) For every $A \in {}_{\mathbb{Z}G}\mathfrak{M}$, the assignment $f \mapsto f(1)$ induces an isomorphism of abelian groups $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},A) \cong A^G$.
(3) Show that the functors $\mathfrak{F}^G$ and $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},\cdot)$ are naturally equivalent.
(4) The cohomology groups $\mathrm{H}^n(G,A)$ are isomorphic to the right derived groups $R^n\mathfrak{F}^G(A)$.

EXERCISE 8.5.3. Let F/k be a Galois extension of fields with finite group G.
(1) Show that the additive group F^+ is a $\mathbb{Z}G$-module.
(2) Show that there is an isomorphism of $\mathbb{Z}G$-modules $\phi : \mathbb{Z}G \otimes_{\mathbb{Z}} k^+ \to F^+$. (Hint: By the Primitive Element Theorem (Theorem 5.5.8), $F = k(\alpha)$ for some element α. Define $\phi(\sigma \otimes a) = \sigma(\alpha)a$.)

EXERCISE 8.5.4. Let $G = \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ be the Galois group of $\mathbb{C}/\mathbb{R}$. Prove that

$$\mathrm{H}^n(G,\mathbb{C}^*) = \begin{cases} \mathbb{R}^* & \text{if } n = 0, \\ \langle 1 \rangle & \text{if } n \text{ is odd,} \\ \langle -1 \rangle & \text{if } n \text{ is even.} \end{cases}$$

EXERCISE 8.5.5. Let G be a finite group.

(1) Prove that the induced $\mathbb{Z}G$-module $\mathbb{Z}G \otimes_{\mathbb{Z}} A$ has trivial cohomology, for any abelian group A. That is, $\mathrm{H}^n(G,\mathbb{Z}G \otimes_{\mathbb{Z}} A) = (0)$, for all $n > 0$. (Hint: Use Lemma 8.5.18, Theorem 8.5.13, and Example 8.5.2.)
(2) In [**54**], a $\mathbb{Z}G$-module M is said to be *relatively projective* if M is a $\mathbb{Z}G$-module direct summand of an induced G-module $\mathbb{Z}G \otimes_{\mathbb{Z}} A$ for some $\mathbb{Z}$-module A. Prove that $\mathrm{H}^n(G,M) = (0)$, for all $n > 0$, if M is relatively projective. The reader is also referred to [**14**] where such modules are called *weakly projective*. (Hint: Proposition 8.3.9 (6).)

EXERCISE 8.5.6. Let G be a finite group and $\{A_i \mid i \in I\}$ a collection of $\mathbb{Z}G$-modules. If $\mathrm{H}^1(G,A_i) = 0$ for each $i \in I$, then $\mathrm{H}^1(G,\bigoplus_i A_i) = 0$.

EXERCISE 8.5.7. Let G be a finite group and $\{A_i \mid i \in I\}$ a collection of $\mathbb{Z}G$-modules. Then for all $r \geq 0$, $\mathrm{H}^r(G,\bigoplus_i A_i) = \bigoplus_i \mathrm{H}^r(G,A_i)$. (Hint: Apply Exercise 2.7.18 to the bar resolution of $\mathbb{Z}$.)

EXERCISE 8.5.8. Let $G = \langle \sigma \rangle$ be a finite cyclic group of order n. Let A be a left $\mathbb{Z}G$-module (written multiplicatively). In this exercise we outline a proof that $\mathrm{H}^1(G,A) \cong {}_N A/DA$ (Theorem 8.5.20) by exhibiting the isomorphism on normalized 1-cocycles. Let $\mathrm{Z}^1(G,A)$ be the normalized 1-cocycles and $\mathrm{B}^1(G,A)$ the normalized 1-coboundaries, as defined in Corollary 8.5.10. Define a function $\theta : \mathrm{Z}^1(G,A) \to A$ by the rule $\theta(\xi) = \xi(\sigma)$. Define another function $\chi : {}_N A \to \mathrm{Map}(G,A)$ by the rule $b \mapsto \chi_b$, where $\chi_b(\sigma^i) = b\sigma(b)\cdots\sigma^{i-1}(b)$, for all $0 < i$. Prove the following.

(1) θ induces a homomorphism of groups $\mathrm{H}^1(G,A) \to {}_N A/DA$.
(2) χ induces a homomorphism of groups ${}_N A/DA \to \mathrm{H}^1(G,A)$.
(3) The homomorphisms of (1) and (2) are inverses of each other.

EXERCISE 8.5.9. Let $G = \langle \sigma \rangle$ be a finite cyclic group of order n. Let A be a left $\mathbb{Z}G$-module (written multiplicatively). In this exercise we outline a proof that $\mathrm{H}^2(G,A) \cong A^G/NA$ (Theorem 8.5.20) by exhibiting the isomorphism on normalized 2-cocycles. Let $\mathrm{Z}^2(G,A)$ be the normalized 2-cocycles and $\mathrm{B}^2(G,A)$ the 2-coboundaries, as defined in Corollary 8.5.10. Define a function $\theta : \mathrm{Z}^2(G,A) \to A$ by the rule

$$\theta(\xi) = a_\xi = \prod_{j=0}^{n-1} \xi(\sigma^j,\sigma).$$

Define another function $\phi : A^G \to \mathrm{Map}(G \times G,A)$ by the rule $\phi(a) = \phi_a$, where

$$\phi_a(\sigma^i,\sigma^j) = \begin{cases} 1 & \text{if } i + j < n \\ a & \text{if } i + j \geq n \end{cases}$$

for all $0 \leq i, j \leq n-1$. Prove the following.

(1) θ and ϕ are homomorphisms of groups.
(2) The image of θ is contained in A^G.
(3) If $\xi \in \mathrm{B}^2(G,A)$, then a_ξ is in NA.

(4) θ induces a homomorphism of groups $\mathrm{H}^2(G,A) \to A^G/NA$.
(5) If $a \in A^G$, then $\phi_a(\sigma^i,\sigma^j)\phi_a(\sigma^{i+j},\sigma^k) = \phi_a(\sigma^j,\sigma^k)\phi_a(\sigma^i,\sigma^{j+k})$. Therefore, the image of ϕ is contained in $\mathrm{Z}^2(G,A)$.
(6) Let $b \in A$, and assume $a = b\sigma(b)\cdots\sigma^{n-1}(b) = N(b)$. Define $\chi : G \to A$ by

$$\chi(\sigma^i) = \begin{cases} 1 & i = 0 \\ b\sigma(b)\cdots\sigma^{i-1}(b) & 0 < i < n. \end{cases}$$

Then ϕ_a is the 2-coboundary defined by χ.
(7) ϕ induces a homomorphism of groups $A^G/NA \to \mathrm{H}^2(G,A)$.
(8) The homomorphisms of (4) and (7) are inverses of each other, hence $\mathrm{H}^2(G,A) \cong A^G/NA$.

EXERCISE 8.5.10. Let G be a group, H a normal subgroup of G, and A a left $\mathbb{Z}G$-module.
(1) If $n \geq 1$, show that $\mathrm{Res} \circ \mathrm{Inf} : \mathrm{H}^n(G/H, A^H) \to \mathrm{H}^n(H,A)$ is the zero map. (Hint: Use normalized cocycles and the descriptions of the maps given in Definition 8.5.12.)
(2) Show that the sequence

$$0 \to \mathrm{H}^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G,A) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(H,A)$$

is exact.

EXERCISE 8.5.11. In this exercise we construct an example of a $\mathbb{Z}/n$-module which is not free. Let $G = \langle \sigma \rangle$ be a finite cyclic group of order n and $M = \mathbb{Z}^{(n-1)}$ the free $\mathbb{Z}$-module of rank $n-1$ with standard basis $e_1,\dots,e_{n-1}$. Let C be the $(n-1)$-by-$(n-1)$ companion matrix of the cyclotomic polynomial $x^{n-1} + x^{n-2} + \cdots + x + 1$. Let $\sigma : M \to M$ be the homomorphism defined by C with respect to the standard basis. Show that this makes M into a left $\mathbb{Z}G$-module and

$$\mathrm{H}^r(G,M) = \begin{cases} 0 & \text{if } r \text{ is even,} \\ \mathbb{Z}/n & \text{if } r \text{ is odd.} \end{cases}$$

6. Theory of Faithfully Flat Descent

Generally, a faithfully flat descent theorem for modules refers to the following question. If S is a commutative faithfully flat R-algebra, and M is an S-module, then does there exist an R-module N such that M is isomorphic to $S \otimes_R N$? Faithfully flat descent tries to exhibit necessary and sufficient conditions on M such that the answer to this question is true. In addition to descent of modules, we also consider descent of elements in an S-algebra, the descent of homomorphisms of S-modules, and the descent of S-algebras.

The theory of faithfully flat descent was developed by A. Grothendieck in a series of Bourbaki seminars over the period 1959 – 1962. The typewritten lecture notes make up much of the book [**25**]. The lectures were later rewritten and published as [**26**, Exposeé VIII] (see also [**27**]). For the most part, our approach follows that of [**36**]. Most of the material in this section has been published in [**18**, Section 5.3]. Two applications of faithfully flat descent appear in Section 8.6.6.

6.1. The Amitsur Complex. Let $\theta : R \to S$ be a homomorphism of commutative rings. Let $\{M_i \mid i \in I\}$ be a family of R-modules. For any $n+1$-tuple $(i_0,\dots,i_n)$ in $I^{(n+1)}$, and for any j such that $0 \le j \le n+1$, there is an R-module homomorphism

$$\begin{aligned} M_{i_0} \otimes_R \cdots \otimes_R M_{i_n} &\xrightarrow{e_j} M_{i_0} \otimes_R \cdots \otimes_R M_{i_{j-1}} \otimes_R S \otimes_R M_{i_j} \otimes_R \cdots \otimes_R M_{i_n} \\ (x_0 \otimes \cdots \otimes x_n) &\mapsto x_0 \otimes \cdots \otimes x_{j-1} \otimes 1 \otimes x_j \otimes \cdots \otimes x_n. \end{aligned}$$

By $S^{\otimes r}$ we denote $S \otimes_R \cdots \otimes_R S$, the tensor product of r copies of S. The *Amitsur complex* for S/R is

$$0 \to R \xrightarrow{\theta} S \xrightarrow{d^0} S^{\otimes 2} \xrightarrow{d^1} S^{\otimes 3} \xrightarrow{d^2} \cdots$$

where the coboundary map $d^r : S^{\otimes(r+1)} \to S^{\otimes(r+2)}$ is defined to be $d^r = \sum_{i=0}^{r+1}(-1)^i e_i$. Denote this complex by $C^\bullet(S/R)$. The reader should verify that $e_j e_i = e_{i+1} e_j$ for all $j \le i$, and that this is a complex of R-modules.

Now we prove that the Amitsur complex is an exact sequence when S is a faithfully flat R-algebra. This fundamental result is the basis for the theory of faithfully flat descent.

PROPOSITION 8.6.1. *Let S be a commutative faithfully flat R algebra.*

(1) The Amitsur complex $C^\bullet(S/R)$ is an exact sequence.
(2) If M is any R-module, then the complex $M \otimes_R C^\bullet(S/R)$

$$0 \to M \xrightarrow{1 \otimes \theta} M \otimes_R S \xrightarrow{1 \otimes d^0} M \otimes S^{\otimes 2} \xrightarrow{1 \otimes d^1} M \otimes S^{\otimes 3} \xrightarrow{1 \otimes d^2} \cdots$$

is an exact sequence.

PROOF. (1): Step 1: Show that $C^\bullet(S/R)$ is exact if there exists an R-module homomorphism $\sigma : S \to R$ which is a splitting map for the structure homomorphism $\theta : R \to S$. This is true for example, if S is faithful and $R \cdot 1$ is an R-direct summand of S. Define a homotopy operator $k^r : S^{\otimes(r+2)} \to S^{\otimes(r+1)}$ by $k^r(x_0 \otimes \cdots \otimes x_{r+1}) = \sigma(x_0)x_1 \otimes \cdots \otimes x_{r+1}$. It follows from

$$\begin{aligned} k^r d^r(x_0 \otimes \cdots \otimes x_r) &= k^r \sum_{i=0}^{r} (-1)^r e_i(x_0 \otimes \cdots \otimes x_r) \\ &= x_0 \otimes \cdots \otimes x_r - \sigma(x_0) \otimes x_1 \otimes \cdots \otimes x_r + \sigma(x_0)x_1 \otimes 1 \otimes \cdots \otimes x_r + \cdots \end{aligned}$$

and

$$\begin{aligned} d^{r-1}k^{r-1}(x_0 \otimes \cdots \otimes x_r) &= d^{r-1}(\sigma(x_0)x_1 \otimes \cdots \otimes x_r) \\ &= 1 \otimes \sigma(x_0)x_1 \otimes \cdots \otimes x_r - \sigma(x_0)x_1 \otimes 1 \otimes \cdots \otimes x_r + \cdots \end{aligned}$$

that $k^r d^r + d^{r-1}k^{r-1}$ is the identity map on $S^{\otimes(r+1)}$. By Exercise 8.1.8, the complex is an exact sequence.

Step 2: If T is another commutative R-algebra, then $C^\bullet(S \otimes_R T/T)$, the Amitsur complex for $S \otimes_R T$ over T, is obtained by applying the functor $(\cdot) \otimes_R T$ to the complex $C^\bullet(S/R)$. This is because $S^{\otimes r} \otimes_R T \cong (S \otimes_R T)^{\otimes r}$.

Step 3: Let $\rho : S \to S \otimes_R S$ by $a \mapsto a \otimes 1$. Define $\mu : S \otimes_R S \to S$ by $\mu(a \otimes b) = ab$. Then μ is a splitting map for ρ and by Step 1 the Amitsur complex $C^\bullet(S \otimes_R S/S)$ for $\rho : S \to S \otimes_R S$ is exact. Since $C^\bullet(S \otimes_R S/S)$ is exact and S is faithfully flat, by Step 2 applied to S, it follows that $C^\bullet(S/R)$ is exact.

(2): As in (1), assume there is a section and construct a contracting homotopy. The rest is left to the reader. $\square$

6.2. The Descent of Elements. Example 8.6.2 considers the Amitsur complex defined by the faithfully flat R-algebra associated with a finite cover of $\operatorname{Spec} R$ by basic open sets.

EXAMPLE 8.6.2. Let R be a commutative ring and $\alpha_1,\dots,\alpha_n$ a set of n elements of R such that $R = R\alpha_1 + \cdots + R\alpha_n$. For the localization of R with respect to the multiplicative set $\{\alpha^n \mid n \geq 0\}$, write R_α instead of $R[\alpha^{-1}]$. By Lemma 3.3.3, $U(\alpha_1),\dots,U(\alpha_n)$ is an open cover for the Zariski topology on $\operatorname{Spec} R$. By Exercise 3.5.13, $S = \bigoplus_{i=1}^n R_{\alpha_i}$ is faithfully flat over R. Using Lemma 3.1.4, we identify $R_{\alpha_i} \otimes_R R_{\alpha_j}$ with $R_{\alpha_i\alpha_j}$. Then the Amitsur complex $C^\bullet(S/R)$ looks like

$$0 \to R \xrightarrow{\theta} \bigoplus_{i\in I_n} R_{\alpha_i} \xrightarrow{d^0} \bigoplus_{(i,j)\in I_n^2} R_{\alpha_i\alpha_j} \xrightarrow{d^1} \bigoplus_{(i,j,k)\in I_n^3} R_{\alpha_i\alpha_j\alpha_k} \xrightarrow{d^2} \cdots$$

where $I_n = \{1,\dots,n\}$. By Proposition 8.6.1, this sequence is exact, so we know that an element $y \in R$ is completely determined by a set of local data $x = (x_1,\dots,x_n) \in S$ such that $x_i = x_j$ in $R_{\alpha_i\alpha_j}$.

The element y can be constructed from the local data x and the elements α_i. For some $p \geq 0$ there exist $y_1,\dots,y_n$ in R such that $x_i = y_i\alpha_i^{-p}$. Assuming $d^0(x) = 0$, there exists $q \geq 0$ such that for all i,j pairs

$$(\alpha_i\alpha_j)^q(\alpha_j^p y_i - \alpha_i^p y_j) = 0.$$

Since $R = R\alpha_1^{q+p} + \cdots + R\alpha_n^{q+p}$, there exist $g_i \in R$ such that $1 = g_1\alpha_1^{q+p} + \cdots + g_n\alpha_n^{q+p}$. Set $y = g_1\alpha_1^q y_1 + \cdots + g_n\alpha_n^q y_n$. The reader should verify that $y = y_j\alpha_j^{-p} = x_j$ in R_{α_j}, hence $\theta(y) = x$.

In Example 8.6.3, the technique introduced in Example 8.6.2 is applied to define the characteristic polynomial of an endomorphism ϕ on a finitely generated projective R-module P. The important observation is that P is locally free of finite rank. Hence the characteristic polynomial of ϕ is locally defined. So the characteristic polynomial exists upon restriction to a faithfully flat R-algebra.

EXAMPLE 8.6.3. Let R be a commutative ring, P a finitely generated projective R-module, and $\phi \in \operatorname{Hom}_R(P,P)$. In this example, we show how to construct the *characteristic polynomial* of ϕ. Let $\alpha_1,\dots,\alpha_n$ be a set of n elements of R such that $R = R\alpha_1 + \cdots + R\alpha_n$ and $P_{\alpha_i} = P \otimes_R R_{\alpha_i}$ is free of finite rank over R_{α_i}. Let $S = \bigoplus_{i=1}^n R_{\alpha_i}$ and as in Example 8.6.2 identify $S^{\otimes 2} = \bigoplus_{(i,j)} R_{\alpha_i\alpha_j}$. Then $S[x] = S \otimes_R R[x] = \bigoplus_{i=1}^n R_{\alpha_i}[x]$ and $S^{\otimes 2}[x] = \bigoplus_{(i,j)} R_{\alpha_i\alpha_j}[x]$. The Amitsur complex $C^\bullet(S[x]/R[x])$ becomes

$$0 \to R[x] \xrightarrow{\theta} \bigoplus_{i\in I_n} R_{\alpha_i}[x] \xrightarrow{d^0} \bigoplus_{(i,j)\in I_n^2} R_{\alpha_i\alpha_j}[x] \xrightarrow{d^1} \cdots$$

which is an exact sequence, because $S[x]$ is faithfully flat over $R[x]$.

For each i, let $\phi_i = \phi \otimes 1 \in \operatorname{Hom}_{R_{\alpha_i}}(P_{\alpha_i},P_{\alpha_i})$. By Definition 1.7.6, the characteristic polynomial $p_i(x) = \operatorname{char.poly}_{R_{\alpha_i}}(\phi_i)$ can be computed as a determinant of $x - \phi_i$ and does not depend on the choice of a basis of P_{α_i}. The polynomial $p_i(x)$ is an element of $R_{\alpha_i}[x]$. We remark that the determinant operator commutes with change of base ring. In other words, if $\theta : A \to B$ is a homomorphism of commutative rings and M is a matrix in $M_n(A)$, then $\det(\theta(M)) = \theta(\det(M))$. This follows straight from the determinant formula Definition 1.7.4. Therefore, if $\phi_{ij} = \phi \otimes 1 \in \operatorname{Hom}_{R_{\alpha_i\alpha_j}}(P_{\alpha_i\alpha_j},P_{\alpha_i\alpha_j})$, then in $R_{\alpha_i\alpha_j}[x]$ we have the equalities $\operatorname{char.poly}_{R_{\alpha_i}}(\phi_i) = \operatorname{char.poly}_{R_{\alpha_i\alpha_j}}(\phi_{ij}) = \operatorname{char.poly}_{R_{\alpha_j}}(\phi_j)$. This says

$d^0(p_1(x),\dots,p_n(x)) = 0$. Therefore, the local data $(p_1(x),\dots,p_n(x))$ descend to a polynomial $p(x)$ in $R[x]$. The polynomial $p(x)$ is usually denoted by $\operatorname{char.poly}_R(\phi)$ and is called the characteristic polynomial of ϕ.

Now we show that the polynomial $\operatorname{char.poly}_R(\phi)$ just constructed does not depend on the open cover of $\operatorname{Spec} R$. Let $\beta_1,\dots,\beta_m$ be another set of elements in R that generated the unit ideal and such that P_{β_j} is free over R_{β_j} for each j. Let $T = \bigoplus_{j=1}^m R_{\beta_j}$ and by the above method, let $q(x)$ be the characteristic polynomial of ϕ constructed using the faithfully flat R-algebra T. We show that $q(x)$ is equal to the polynomial $p(x)$ which was constructed initially. Notice that $S\otimes_R T$ is a faithfully flat R-algebra and we can identify $S\otimes_R T = \bigoplus_{(i,j)} R_{\alpha_i\beta_j}$. The image of $p(x)$ in $R_{\alpha_i\beta_j}[x]$ is equal to the image of $q(x)$ in $R_{\alpha_i\beta_j}[x]$. Since the Amitsur complex $C^\bullet(S\otimes_R T[x]/R[x])$ is exact, this proves $p(x) = q(x)$.

Now we prove the Cayley-Hamilton theorem applies to $p(x) = \operatorname{char.poly}_R(\phi)$. Since S is faithfully flat over R, by Proposition 8.6.1, the sequence

$$0 \to \operatorname{Hom}_R(P,P) \xrightarrow{\theta} \operatorname{Hom}_R(P,P)\otimes_R S$$

is exact. We identify $\operatorname{Hom}_R(P,P)\otimes_R S$ with $\bigoplus_{i=1}^n \operatorname{Hom}_{R_{\alpha_i}}(P_{\alpha_i},P_{\alpha_i})$. The image of $p(\phi)$ under θ is $(p_1(\phi_1),\dots,p_n(\phi_n))$. By The Cayley-Hamilton Theorem, Theorem 1.7.7, this image is $(0,\dots,0)$, which means $p(\phi) = 0$.

If $\operatorname{Rank}_R(P) = n$ is defined, then the characteristic polynomial will have constant degree n. Let $\operatorname{char.poly}_R(\phi) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Following Exercise 1.7.1, we define the *determinant* of ϕ to be $\det(\phi) = (-1)^n a_0$ and the *trace* of ϕ to be $\operatorname{trace}(\phi) = -a_{n-1}$. The reader should verify that $\det(\phi\psi) = \det(\phi)\det(\psi)$.

6.3. Descent of Homomorphisms. Let S be a commutative R-algebra and M and N a pair of R-modules. The goal is to find sufficient conditions on a homomorphism $g \in \operatorname{Hom}_S(M\otimes_R S, N\otimes_R S)$ such that $g = f\otimes 1$ for some $f \in \operatorname{Hom}_R(M,N)$. The maps $e_i : S \to S\otimes_R S$ defined by $e_0(s) = 1\otimes s$ and $e_1(s) = s\otimes 1$ are both R-algebra homomorphisms. Therefore, $S\otimes_R S$ is an S-algebra in two different ways. Tensoring e_i with $(M\otimes_R S)\otimes_S ()$ we get the maps of Paragraph 8.6.1

$$e_i : M\otimes_R S \to (M\otimes_R S)\otimes_S (S\otimes_R S) \cong M\otimes_R S\otimes_R S$$

where $e_0(x\otimes s) = x\otimes 1\otimes s$ and $e_1(x\otimes s) = x\otimes s\otimes 1$. Assign the appellation $\mathfrak{F}_i$ to the functor "tensoring with the S-algebra $e_i : S \to S\otimes_R S$". There is a commutative square

$$\begin{tikzcd}
M\otimes_R S \arrow[r, "e_i"] \arrow[d, "g"'] & M\otimes_R S\otimes_R S \arrow[d, "\mathfrak{F}_i(g)"] \\
N\otimes_R S \arrow[r, "e_i"] & N\otimes_R S\otimes_R S
\end{tikzcd}$$

for $i = 0,1$ and $\mathfrak{F}_i(g)$ is an $S\otimes_R S$-module homomorphism.

PROPOSITION 8.6.4. *Let R be a commutative ring, S a faithfully flat commutative R-algebra, and M and N a pair of R-modules. The sequence*

$$0 \to \operatorname{Hom}_R(M,N) \xrightarrow{\mathfrak{F}} \operatorname{Hom}_S(M\otimes_R S, N\otimes_R S) \xrightarrow{\mathfrak{F}_0-\mathfrak{F}_1} \operatorname{Hom}_{S\otimes_R S}(M\otimes_R S\otimes_R S, N\otimes_R S\otimes_R S)$$

is exact, where $\mathfrak{F}(f) = f\otimes 1$ and $\mathfrak{F}_0$, $\mathfrak{F}_1$ are defined in the previous paragraph.

PROOF. Since each $\mathfrak{F}_i$ is an additive functor, $\mathfrak{F}_0 - \mathfrak{F}_1$ is a $\mathbb{Z}$-module homomorphism. If $f \in \operatorname{Hom}_R(M,N)$, then the diagram

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] \arrow[d, "f"] & M \otimes_R S \arrow[r, "d^0"] \arrow[d, "f\otimes 1"] & M \otimes_R S \otimes_R S \arrow[d, "f\otimes 1\otimes 1"] \\ 0 \arrow[r] & N \arrow[r] & N \otimes_R S \arrow[r, "d^0"] & N \otimes_R S \otimes_R S \end{tikzcd}$$

commutes and the rows are exact. Therefore, $\mathfrak{F}$ is one-to-one and $f \otimes 1 \otimes 1 = 0$. To complete the proof, we show $\ker(\mathfrak{F}_0 - \mathfrak{F}_1) \subseteq \operatorname{im}(\mathfrak{F})$. Let $g \in \operatorname{Hom}_S(M \otimes_R S, N \otimes_R S)$ and assume $\mathfrak{F}_0(g) = \mathfrak{F}_1(g)$. Given $m \in M$ we have $e_0(m \otimes 1) = e_1(m \otimes 1)$, so

$$e_0 g(m \otimes 1) = \mathfrak{F}_0(g) e_0(m \otimes 1) = \mathfrak{F}_0(g) e_1(m \otimes 1) = \mathfrak{F}_1(g) e_1(m \otimes 1) = e_1 g(m \otimes 1).$$

By Proposition 8.6.1, this proves that $g(m \otimes 1) \in N \otimes_R 1$. Define $f : M \to N$ by $f(m) = g(m \otimes 1)$. Then $g = \mathfrak{F}(f)$. $\square$

EXAMPLE 8.6.5. Let R be a commutative ring and P a finitely generated projective R-module. By Lemma 2.8.1, $\theta_R : P^* \otimes_R P \to \operatorname{Hom}_R(P,P)$ is an isomorphism of R-modules, where $\theta_R(f \otimes p)(x) = f(x)p$. Define $T : P^* \otimes_R P \to R$ by $T(f \otimes p) = f(p)$. By Exercise 5.6.6, this induces an R-module homomorphism $T : \operatorname{Hom}_R(P,P) \to R$ which is equal to the trace map of Exercise 1.7.2 and the trace map of Definition 5.6.6, when P is free. As in Example 8.6.2, let $R \to S$ be a faithfully flat R-algebra such that $P \otimes_R S$ is free. Upon change of base, $T \otimes 1 : \operatorname{Hom}_S(P \otimes_R S, P \otimes_R S) \to S$ is the trace map of Exercise 1.7.2. By Proposition 8.6.4, the map T is equal to the trace map of Definition 5.6.6. Assuming $\operatorname{Rank}_R(P)$ is defined, we also see that T is equal to the trace defined in Example 8.6.3 using the characteristic polynomial.

6.4. Descent of Modules. If S is a faithfully flat R-algebra, then Theorem 8.6.7, which is fundamental, gives sufficient conditions on an S-module M such that M descends to an R-module N. That is, such that M is isomorphic to $N \otimes_R S$ for some R-module N.

Let $\theta : R \to S$ be a homomorphism of commutative rings. Given S-modules A, B, C and D and an $S \otimes_R S$-module homomorphism $f : A \otimes_R B \to C \otimes_R D$, there are three $S \otimes_R S \otimes_R S$-module homomorphisms

$$\begin{aligned} f_1 &: S \otimes_R A \otimes_R B \to S \otimes_R C \otimes_R D \\ f_2 &: A \otimes_R S \otimes_R B \to C \otimes_R S \otimes_R D \\ f_3 &: A \otimes_R B \otimes_R S \to C \otimes_R D \otimes_R S \end{aligned}$$

where f_i is obtained by tensoring f with the identity map on S in position i. We employ this construction in the following setting. Start with any S-module M. Then $S \otimes_R M$ and $M \otimes_R S$ are two $S \otimes_R S$-modules. Then an $S \otimes_R S$-module homomorphism $g : S \otimes_R M \to M \otimes_R S$ gives rise to three $S \otimes_R S \otimes_R S$-module homomorphisms

$$\begin{aligned} g_1 &: S \otimes_R S \otimes_R M \to S \otimes_R M \otimes_R S \\ g_2 &: S \otimes_R S \otimes_R M \to M \otimes_R S \otimes_R S \\ g_3 &: S \otimes_R M \otimes_R S \to M \otimes_R S \otimes_R S. \end{aligned}$$

The ring homomorphism θ induces $\theta : M \to S \otimes_R M$, where $x \mapsto 1 \otimes x$. Let $\mu : M \otimes_R S \to M$ be the multiplication map, where $x \otimes s \mapsto sx$. The composition

$$S \otimes_R M \xrightarrow{g} M \otimes_R S \xrightarrow{\mu} M \xrightarrow{\theta} S \otimes_R M$$

upon restriction to $\operatorname{im}\theta$ induces an S-module homomorphism which will be denoted by $\bar{g} : 1 \otimes_R M \to 1 \otimes_R M$. Then $\bar{g}(1 \otimes m) = 1 \otimes \mu g(1 \otimes m)$.

PROPOSITION 8.6.6. *Let $\theta : R \to S$ be a homomorphism of commutative rings, M an S-module and $g : S \otimes_R M \to M \otimes_R S$ an $S \otimes_R S$-module homomorphism. The following are equivalent.*

(1) $\bar{g}$ is the identity map on $1 \otimes_R M$ and $g_2 = g_3 g_1$.
(2) g is an isomorphism of $S \otimes_R S$-modules and $g_2 = g_3 g_1$.

PROOF. (1) implies (2): Let $\tau : M \otimes_R S \to S \otimes_R M$ be the twist map defined by $x \otimes s \mapsto s \otimes x$. The reader should verify that $\tilde{g} = t^{-1} g \tau$ is an $S \otimes_R S$-module homomorphism. We show that $\tilde{g}$ is the inverse of g. Let $m \in M$. Then $1 \otimes m$ is a typical generator for the $S \otimes_R S$-module $S \otimes_R M$. If we write $g(1 \otimes m) = \sum_i m_i \otimes s_i$, then since $\bar{g}$ is the identity map,

$$1 \otimes m = \bar{g}(1 \otimes m) = 1 \otimes \sum_i m_i s_i.$$

Next write $g(1 \otimes m_i) = \sum_j m_{ij} \otimes t_{ij}$. We have

$$\begin{aligned}
\tilde{g}\big(g(1 \otimes m)\big) &= \tilde{g}\Big(\sum_i m_i \otimes s_i\Big) \\
&= \sum_i \tilde{g}(m_i \otimes s_i) \\
&= \sum_i (1 \otimes s_i)\tilde{g}(m_i \otimes 1) \\
&= \sum_i (1 \otimes s_i) \sum_j t_{ij} \otimes m_{ij} \\
&= \sum_i \sum_j t_{ij} \otimes s_i m_{ij}.
\end{aligned}$$

Let $\omega : M \otimes_R S \otimes_R S \to S \otimes_R M$ be the function $x \otimes a \otimes b \mapsto a \otimes xb$ which multiplies the two extreme factors. Since $g_2 = g_3 g_1$,

$$\omega\left(g_2(1 \otimes 1 \otimes m)\right) = \omega\Big(\sum_i m_i \otimes 1 \otimes s_i\Big) = 1 \otimes \sum_i m_i s_i = 1 \otimes m$$

is equal to

$$\omega g_3 g_1(1 \otimes 1 \otimes m) = \sum_i \omega g_3(1 \otimes m_i \otimes s_i) = \sum_i \sum_j \omega(m_{ij} \otimes t_{ij} \otimes s_i) = \sum_i \sum_j t_{ij} \otimes m_{ij} s_i$$

which is equal to $\tilde{g}g(1 \otimes m)$. This proves that $\tilde{g}g$ is the identity map on $S \otimes_R M$. The reader should verify that $g\tilde{g}$ is the identity map on $M \otimes_R S$.

(2) implies (1): We are given an isomorphism $g : S \otimes_R M \to M \otimes_R S$. Let $m \in M$ and write $g(1 \otimes m) = \sum_i m_i \otimes s_i$. Then

$$\bar{g}(1 \otimes m) = 1 \otimes \mu g(1 \otimes m) = 1 \otimes \sum_i m_i s_i.$$

Since g is one-to-one, it is enough to show $g(1 \otimes m) = g\big(1 \otimes \sum_i m_i s_i\big)$. Write $g(1 \otimes m_i) = \sum_j m_{ij} \otimes t_{ij}$. We have

$$g\big(1 \otimes \sum_i m_i s_i\big) = \sum_i g(1 \otimes m_i)(1 \otimes s_i) = \sum_i \sum_j m_{ij} \otimes t_{ij} s_i.$$

Let $\omega : M \otimes_R S \otimes_R S \to M \otimes_R S$ be the function $x \otimes a \otimes b \mapsto x \otimes ab$ which multiplies the last two factors. Since $g_2 = g_3 g_1$,

$$\omega g_2(1 \otimes 1 \otimes m) = \omega\Big(\sum_i m_i \otimes 1 \otimes s_i\Big) = \sum_i m_i \otimes s_i$$

is equal to

$$\omega g_3 g_1(1 \otimes 1 \otimes m) = \sum_i \omega g_3(1 \otimes m_i \otimes s_i) = \sum_i \sum_j \omega(m_{ij} \otimes t_{ij} \otimes s_i) = \sum_i \sum_j m_{ij} \otimes t_{ij} s_i.$$

It follows from these computations that $g(1 \otimes m) = g\big(1 \otimes \sum_i m_i s_i\big)$. □

If one of the equivalent properties of Proposition 8.6.6 is satisfied, then we say g is a *descent datum* for M over S.

THEOREM 8.6.7. *(The Theorem of Faithfully Flat Descent) Let S be a commutative faithfully flat R-algebra. Let M be an S-module and $g : S \otimes_R M \to M \otimes_R S$ a descent datum for M over S. Then there exists an R-module N and an isomorphism $\nu : N \otimes_R S \to M$ of S-modules such that the diagram of $S \otimes_R S$-modules*

(6.1)
$$\begin{tikzcd} S \otimes_R N \otimes_R S \arrow[r, "1\otimes\nu"] \arrow[d, "\tau"'] & S \otimes_R M \arrow[d, "g"] \\ N \otimes_R S \otimes_R S \arrow[r, "\nu\otimes 1"] & M \otimes_R S \end{tikzcd}$$

commutes, where $\tau(a \otimes b \otimes c) = b \otimes a \otimes c$. Up to isomorphism, these properties uniquely determine the module N and the isomorphism ν.

PROOF. (Existence.) Set $N = \{x \in M \mid x \otimes 1 = g(1 \otimes x)\}$ and let $\nu : N \otimes_R S \to M$ be the multiplication map $\nu(x \otimes s) = xs$. We show that N and ν have the desired properties. Notice that N is the kernel of the R-module homomorphism $ge_0 - e_1 : M \to M \otimes_R S$, hence the sequence

(6.2)
$$0 \to N \to M \xrightarrow{ge_0 - e_1} M \otimes_R S$$

is exact and N is an R-module. Over $S \otimes_R S$, the module $S \otimes_R N \otimes_R S$ is generated by elements of the form $1 \otimes x \otimes 1$, for $x \in N$. Diagram (6.1) commutes since

$$g\big((1 \otimes \nu)(1 \otimes x \otimes 1)\big) = g(1 \otimes x) = x \otimes 1 = (\nu \otimes 1)(x \otimes 1 \otimes 1) = (\nu \otimes 1)\big(\tau(1 \otimes x \otimes 1)\big).$$

The diagram of S-module homomorphisms

(6.3)
$$\begin{tikzcd} S \otimes_R M \arrow[r, "1\otimes e_1"] \arrow[d, "g"'] & S \otimes_R M \otimes_R S \arrow[d, "g_3 = g\otimes 1"] \\ M \otimes_R S \arrow[r, "1\otimes e_1 = e_2"'] & M \otimes_R S \otimes_R S \end{tikzcd}$$

commutes, since

$$g_3\big((1 \otimes e_1)(a \otimes x)\big) = g_3(a \otimes x \otimes 1) = g(a \otimes x) \otimes 1 = e_2\big(g(a \otimes x)\big).$$

Since $g_2 = g_3 g_1$, it follows that

$$g_3\big((1 \otimes ge_0)(a \otimes x)\big) = g_3\big(a \otimes g(1 \otimes x)\big) = g_3 g_1(a \otimes 1 \otimes x) = g_2(a \otimes 1 \otimes x) = e_1 g(a \otimes x).$$

Therefore, the diagram of S-module homomorphisms

$$\begin{tikzcd} S\otimes_R M \arrow[r, "1\otimes ge_0"] \arrow[d, "g"'] & S\otimes_R M\otimes_R S \arrow[d, "g_3=g\otimes 1"] \\ M\otimes_R S \arrow[r, "1\otimes e_0=e_1"'] & M\otimes_R S\otimes_R S \end{tikzcd} \tag{6.4}$$

commutes. Consider the diagram of S-module homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & S\otimes_R N \arrow[r] \arrow[d, dotted, "\phi"'] & S\otimes_R M \arrow[r, "1\otimes(ge_0-e_1)"] \arrow[d, "g"'] & S\otimes_R M\otimes_R S \arrow[d, "g_3"] \\ 0 \arrow[r] & M \arrow[r, "1\otimes\theta"'] & M\otimes_R S \arrow[r, "1\otimes(e_0-e_1)"'] & M\otimes_R S\otimes_R S \end{tikzcd} \tag{6.5}$$

The top row of (6.5) is exact, because it is obtained by applying the exact functor $S\otimes_R ()$ to the exact sequence (6.2). The bottom row of (6.5) is exact by Proposition 8.6.1. The diagram (6.5) commutes because it is constructed from the commutative diagrams (6.3) and (6.4). Since g and g_3 are isomorphisms, the S-module homomorphism ϕ exists and is an isomorphism, by Theorem 2.5.2. For $x\in N$, $\phi(1\otimes x)=x$, hence ϕ agrees with ν. This proves ν is an isomorphism.

(Uniqueness.) Suppose K is another R-module and $\kappa: K\otimes_R S\to M$ the corresponding S-module isomorphism. Consider the commutative diagram

$$\begin{tikzcd} S\otimes_R K\otimes_R S \arrow[r, "1\otimes\kappa"] \arrow[d, "\tau"'] & S\otimes_R M \arrow[d, "g"] & S\otimes_R N\otimes_R S \arrow[l, "1\otimes\nu"'] \arrow[d, "\tau"] \\ K\otimes_R S\otimes_R S \arrow[r, "\kappa\otimes 1"'] & M\otimes_R S & N\otimes_R S\otimes_R S \arrow[l, "\nu\otimes 1"] \end{tikzcd}$$

In the notation of Proposition 8.6.4, this says

$$\mathfrak{F}_0(\nu^{-1}\kappa)=\tau\Big(\big(1\otimes\nu^{-1}\kappa\big)\big(\tau^{-1}(x\otimes a\otimes b)\big)\Big)$$

is equal to

$$\mathfrak{F}_1(\nu^{-1}\kappa)=\big((\nu^{-1}\kappa)(x\otimes a)\big)\otimes b.$$

By Proposition 8.6.4, there exists $\lambda\in\operatorname{Hom}_R(K,N)$ such that $\nu^{-1}\kappa=\lambda\otimes 1$. Since S is faithfully flat over R and $\nu^{-1}\kappa$ is an isomorphism, $\lambda: K\to N$ is an R-module isomorphism. Lastly, $\kappa=\nu(\lambda\otimes 1)$. □

REMARK 8.6.8. Theorem 8.6.7 is sometimes stated from the opposite point of view. That is, the role of the descent datum is played by the function $h=g^{-1}$. Then $h: M\otimes_R S\to S\otimes_R M$ is an $S\otimes_R S$-module isomorphism which satisfies the 1-cocycle identity $h_1h_3=h_2$. Then $N=\{x\in M \mid h(x\otimes 1)=1\otimes x\}$, $\nu: N\otimes_R S\to M$ is the multiplication map $\nu(x\otimes s)=xs$, and $h=(1\otimes\nu)(\nu\otimes 1)^{-1}$.

EXAMPLE 8.6.9. Let R be a commutative ring and $\alpha_1,\dots,\alpha_n$ a set of n elements of R such that $R=R\alpha_1+\cdots+R\alpha_n$. For the localization of R with respect to the multiplicative set $\{\alpha^n \mid n\geq 0\}$, write R_α instead of $R[\alpha^{-1}]$. By Exercise 3.5.13, $S=\bigoplus_{i=1}^n R_{\alpha_i}$ is faithfully flat over R. Using Lemma 3.1.4, we identify $R_{\alpha_i}\otimes_R R_{\alpha_j}$ with $R_{\alpha_i\alpha_j}$. Then

$S \otimes_R S = \bigoplus_{(i,j)\in I_n^2} R_{\alpha_i\alpha_j}$, where $I_n = \{1,\dots,n\}$. Suppose for each i that M_i is an R_{α_i}-module. Then $M = \bigoplus_{i=1}^n M_i$ is an S-module. We have

$$S \otimes_R M = \bigoplus_{(i,j)\in I_n^2} R_{\alpha_i} \otimes_R M_j$$

and

$$M \otimes_R S = \bigoplus_{(i,j)\in I_n^2} M_i \otimes_R R_{\alpha_j}.$$

A descent datum $g : S \otimes_R M \to M \otimes_R S$ consists of a collection of $R_{\alpha_i\alpha_j}$-module isomorphisms

$$R_{\alpha_i} \otimes_R M_j \xrightarrow{g_{ij}} M_i \otimes_R R_{\alpha_j}$$

where $(i,j) \in I_n^2$. The identity $g_2 = g_3 g_1$ is equivalent to the statement that the diagram of $R_{\alpha_i\alpha_j\alpha_k}$-module homomorphisms

$$\begin{tikzcd}
R_{\alpha_i} \otimes_R R_{\alpha_j} \otimes_R M_k \arrow[rr, "g_{ik}\otimes 1"] \arrow[dr, "g_{jk}\otimes 1"'] & & M_i \otimes_R R_{\alpha_j} \otimes_R R_{\alpha_k} \\
& R_{\alpha_i} \otimes_R M_j \otimes_R R_{\alpha_k} \arrow[ur, "g_{ij}\otimes 1"'] &
\end{tikzcd}$$

commutes for all triples $(i,j,k) \in I_n^3$. If a descent datum exists, then by Theorem 8.6.7, there is an R-module N and for each i an isomorphism $M_i \cong N \otimes_R R_{\alpha_i}$ of R_{α_i}-modules.

6.5. Descent of Algebras. Let R be a commutative ring and S a faithfully flat commutative R-algebra. Let N be an R-module such that the S-module $N_S = N \otimes_R S$ has a multiplication operation which is defined by an S-module homomorphism $\mu : N_S \otimes_S N_S \to N_S$. If we identify $N_S \otimes_S N_S$ with $N \otimes_R N \otimes_R S$, then μ belongs to $\operatorname{Hom}_S(N \otimes_R N \otimes_R S, N \otimes_R S)$. By Proposition 8.6.4, the homomorphism μ descends to a unique R-module homomorphism $N \otimes_R N \to N$ if and only if $\mathfrak{F}_0(\mu)$ and $\mathfrak{F}_1(\mu)$ induce equal multiplication operations on $N \otimes_R S \otimes_R S$.

THEOREM 8.6.10. *Let S be a commutative faithfully flat R-algebra. Let B be an S-algebra and $g : S \otimes_R B \to B \otimes_R S$ a descent datum for B over S such that g is an isomorphism of $S \otimes_R S$-algebras. Then there exists an R-algebra A and an isomorphism $\nu : A \otimes_R S \to B$ of S-algebras.*

PROOF. The existence and uniqueness of the R-module A and the S-module isomorphism $\nu : A \otimes_R S \to B$ are guaranteed by Theorem 8.6.7. The diagram

$$\begin{tikzcd}
S \otimes_R A \otimes_R S \arrow[r, "1\otimes\nu"] \arrow[d, "\tau"'] & S \otimes_R B \arrow[d, "g"] \\
A \otimes_R S \otimes_R S \arrow[r, "\nu\otimes 1"] & B \otimes_R S
\end{tikzcd} \tag{6.6}$$

commutes, where $\tau(a \otimes b \otimes c) = b \otimes a \otimes c$. The counterpart of (6.6) for $A \otimes_R A \otimes_R S \cong B \otimes_S B$ is the commutative square

$$
\begin{tikzcd}
S \otimes_R (A \otimes_R A) \otimes_R S \arrow[r, "1\otimes(\nu\otimes_S\nu)"] \arrow[d, "\tau"'] & S \otimes_R (B \otimes_R B) \arrow[d, "g\otimes_S g"] \\
(A \otimes_R A) \otimes_R S \otimes_R S \arrow[r, "(\nu\otimes_S\nu)\otimes 1"] & (B \otimes_R B) \otimes_R S
\end{tikzcd}
\tag{6.7}
$$

Because g is an $S \otimes_R S$-algebra isomorphism, the diagram

$$
\begin{tikzcd}
S \otimes_R B \otimes_R B = (S \otimes_R B) \otimes_S (S \otimes_R B) \arrow[r] \arrow[d, "g\otimes_S g"'] & S \otimes_R B \arrow[d, "g"] \\
B \otimes_R B \otimes_R S = (B \otimes_R S) \otimes_S (B \otimes_R S) \arrow[r] & B \otimes_R S
\end{tikzcd}
\tag{6.8}
$$

commutes, where the horizontal arrows are the multiplication maps. The multiplication μ on $A_S = A \otimes_R S$ is defined by the multiplication operation on B and the S-algebra isomorphism ν. By definition of μ, the diagram

$$
\begin{tikzcd}
A \otimes_R A \otimes_R S = A_S \otimes_S A_S \arrow[r, "\mu"] \arrow[d, "\nu\otimes_S\nu"'] & A_S \arrow[d, "\nu"] \\
B \otimes_S B \arrow[r] & B
\end{tikzcd}
\tag{6.9}
$$

commutes, where the bottom arrow is multiplication in B. As was mentioned in the paragraph preceding the theorem, it suffices to show that $\mathfrak{F}_0(\mu)$ and $\mathfrak{F}_1(\mu)$ induce equal multiplication operations on $A \otimes_R S \otimes_R S$. Apply either functor $\mathfrak{F}_i$ to the commutative square (6.9) to get the commutative square

$$
\begin{tikzcd}
(A \otimes_R A) \otimes_R S \otimes_R S \arrow[r, "\mathfrak{F}_i(\mu)"] \arrow[d, "(\nu\otimes_S\nu)\otimes 1"'] & A \otimes_R S \otimes_R S \arrow[d, "\nu\otimes 1"] \\
B \otimes_S B \otimes_R S \arrow[r] & B \otimes_R S
\end{tikzcd}
\tag{6.10}
$$

Combine diagrams (6.6), (6.7), (6.8), and (6.10) to get the commutative diagram

$$
\begin{tikzcd}
(A \otimes_R A) \otimes_R S \otimes_R S \arrow[rrr, "\mathfrak{F}_i(\mu)"] \arrow[dr, "(1\otimes(\nu\otimes_S\nu))\tau^{-1}"] \arrow[ddr, "(\nu\otimes_S\nu)\otimes 1"'] & & & A \otimes_R S \otimes_R S \arrow[dl, "(1\otimes\nu))\tau^{-1}"'] \arrow[ddl, "\nu\otimes 1"] \\
& S \otimes_R B \otimes_R B \arrow[r] \arrow[d, "g\otimes_S g"] & S \otimes_R B \arrow[d, "g"'] & \\
& B \otimes_R B \otimes_R S \arrow[r] & B \otimes_R S &
\end{tikzcd}
$$

This diagram commutes with either $\mathfrak{F}_0(\mu)$ or $\mathfrak{F}_1(\mu)$ in the top row. Therefore the multiplication on A_S descends to a multiplication on A. The associative, commutative and distributive laws hold in A because they hold in A_S. $\square$

6.6. Applications. The results of Section 8.6 are applied to prove two important theorems. The first result gives a complete classification for involutions of quadratic extensions of a commutative ring. The second application is a criterion due to H. Bass for a module over a commutative ring to be a progenerator.

6.6.1. *Quadratic Extensions.* Let R be a commutative ring and A an R-algebra. An R-algebra *involution* of A is a function $\sigma : A \to A$ satisfying

$$\begin{aligned} \sigma(x+y) &= \sigma(x)+\sigma(y), \text{ if } x,y \in A \\ \sigma(xy) &= \sigma(y)\sigma(x), \text{ if } x,y \in A \\ \sigma(\sigma(x)) &= x, \text{ if } x \in A \\ \sigma(x) &= x, \text{ if } x \in R \end{aligned}$$

Associated to an involution σ are the *trace* $T_R^A : A \to A$ and the *norm* $N_R^A : A \to A$, defined by

$$\begin{aligned} T_R^A(x) &= x+\sigma(x) \\ N_R^A(x) &= x\sigma(x) \end{aligned}$$

Notice that

$$x^2 - xT_R^A(x) + N_R^A(x) = 0 \tag{6.11}$$

for all $x \in A$. We call σ a *standard involution* in case $T_R^S(x) \in R$ and $N_R^S(x) \in R$ for all $x \in S$. If σ is a standard involution, the reader should verify

$$N_R^S(x) = x\sigma(x) = \sigma(x)x$$

and

$$N_R^A(xy) = N_R^A(x)N_R^A(y)$$

for all $x,y \in A$.

Propositions 8.6.11 and 8.6.12 below are based on [**35**, (1.3.4) and (1.3.6)].

PROPOSITION 8.6.11. *If S is an R-algebra which as an R-module is a progenerator, then there exists at most one standard involution on S.*

PROOF. Suppose σ_1 and σ_2 are standard involutions of S. By Proposition 3.6.2, there exist $f_1,\dots,f_n$ in R such that S_{f_i} is a free R_{f_i} module of of finite rank and $\bigoplus_{i=1}^n S_{f_i}$ is a faithfully flat S-algebra. It suffices to show that $\sigma_1 = \sigma_2$ upon restriction to S_{f_i}, for each i. Therefore we assume from now on that S is free. By Proposition 3.5.6, $R\cdot 1$ is an R-module direct summand of S. Let $b_1,\dots,b_n$ be a free R-basis for S and assume $b_1 = 1$. Write T_i and N_i for the trace and norm associated to σ_i. Then $T_1(b_1) = T_2(b_1)$. By (6.11), $b_j^2 = b_jT_1(b_j) - N_1(b_j) = b_jT_2(b_j) - N_2(b_j)$, from which it follows that $T_1(b_j) = T_2(b_j)$ for $2 \le j \le n$. □

A *quadratic extension* of R is an R-algebra S which is an R-progenerator of rank two. By Exercise 3.6.3, a quadratic extension is commutative.

PROPOSITION 8.6.12. *A quadratic extension S/R has a unique standard involution.*

PROOF. Case 1: Assume S is a free R-module of rank two. As in the proof of Proposition 8.6.11, assume $S = R\cdot 1 + R\cdot\beta$. There exist $a,b \in R$ such that $\beta^2 = a + b\beta$. Define $\sigma : S \to S$ by $1 \mapsto 1$ and $\beta \mapsto b - \beta$. Then $\sigma(x+y\beta) = x + yb - y\beta$. The reader should verify that σ is a standard involution.

Case 2: S is locally free of rank two. As in the proof of Proposition 8.6.11, there exist $f_1,\dots,f_n$ in R such that S_{f_i} is a free R_{f_i} module of of finite rank, $\mathscr{R} = \bigoplus_{i=1}^n R_{f_i}$ is a faithfully flat R-algebra, and $\mathscr{S} = \bigoplus_{i=1}^{n} S_{f_i}$ is a faithfully flat S-algebra. By Case 1 there exist R_{f_i}-algebra involutions σ_i on S_{f_i} and $\sigma = \oplus\sigma_i$ is an $\mathscr{R}$-involution on $\mathscr{S}$. Let σ_{ij} denote the restriction of σ_i to $S_{f_if_j}$. By Proposition 8.6.11, $\sigma_{ij} = \sigma_{ji}$. By Example 8.6.2, the right-most square of the diagram

$$\begin{tikzcd}
0 \arrow[r] & S \arrow[r] \arrow[d, dotted, "\exists\sigma"] & \bigoplus_i S_{f_i} \arrow[r, "d^0"] \arrow[d, "\oplus\sigma_i"] & \bigoplus_{(i,j)} S_{f_if_j} \arrow[d, "\oplus\sigma_{ij}"] \\
0 \arrow[r] & S \arrow[r] & \bigoplus_i S_{f_i} \arrow[r, "d^0"] & \bigoplus_{(i,j)} S_{f_if_j}
\end{tikzcd}$$

commutes. The rows are exact, so σ defines an involution on S. The reader should verify that σ is a standard involution. □

6.6.2. *A Theorem of Bass.* In this short section we prove a theorem of Bass (Theorem 8.6.14) which was stated without proof in [**18**, Theorem 14.2.1]. The proof given in [**10**, Proposition (4.6), p. 476] is K-theoretic, whereas the proof given below is based on the method suggested in the paragraph immediately preceding [**42**, Theorem III.17] and utilizes only theorems proven in this book. The main idea for the proof is the following lemma.

LEMMA 8.6.13. *Let R be a ring and M a left R-module. For any $n > 0$, the assignment*

$$\operatorname{Hom}_R(M,M) \xrightarrow{\Delta} \operatorname{Hom}_R(M^{(n)},M^{(n)})$$

that maps a homomorphism φ in $\operatorname{Hom}_R(M,M)$ to the corresponding diagonal homomorphism $\Delta(\varphi) = \oplus_{i=1}^{n}\varphi$ in $\operatorname{Hom}_R(M^{(n)},M^{(n)})$ defines a monomorphism of rings. If R is commutative, Δ is an R-algebra homomorphism.

PROOF. The proof is left to the reader. □

THEOREM 8.6.14. *(H. Bass) Let R be a commutative ring and M an R-module. Then M is an R-progenerator if and only if there exists an R-module P such that $P \otimes_R M \cong R^{(s)}$ for some $s > 0$.*

PROOF. If there exists an R-module P such that $P \otimes_R M \cong R^{(s)}$, then by Proposition 2.3.25, both M and P are R-progenerators.

Assume M is an R-progenerator. First we show how to reduce to the case where M has constant rank. Assume M does not have constant rank. As in Corollary 3.4.7, let $e_1,\dots,e_t$ be the structure idempotents of M in R. Write R_i for Re_i and M_i for Me_i. Then $R = R_1 \oplus \cdots \oplus R_t$, $M = M_1 \oplus \cdots \oplus M_t$, and M_i is an R_i-progenerator of constant rank. For each i, assume there exists an integer $s_i > 0$ and an R_i-module P_i such that $M_i \otimes_{R_i} P_i \cong R_i^{(s_i)}$. Let s be the least common multiple of $\{s_1,\dots,s_t\}$. Then $M \otimes_R \left(P_1^{(s/s_1)} \oplus \cdots \oplus P_t^{(s/s_t)}\right) \cong R^{(s)}$.

Assume from now on that M has constant rank r. If M is free, then there is nothing to prove. Assume N is an R-progenerator such that $M \oplus N$ is free of rank rn and $n \geq 2$. By Exercises 3.6.4 and 3.5.13, there exists a commutative faithfully flat R-algebra S such that $M \otimes_R S$ and $N \otimes_R S$ are isomorphic to the free S-modules $S^{(r)}$ and $S^{(rn-r)}$, respectively. Then $(M \oplus N) \otimes_R S$ can be written as a direct sum $\oplus_{i=1}^{n} S^{(r)}$, which is isomorphic to the direct sum $(M \otimes_R S)^{(n)}$. Applying Lemma 8.6.13 to this direct sum decomposition defines the homomorphism $\Delta : \operatorname{Hom}_S(M \otimes_R S, M \otimes_R S) \to \operatorname{Hom}_S((M \oplus N) \otimes_R S, (M \oplus N) \otimes_R S)$. By Lemma 2.8.1 (1),

$$M^* \otimes_R M \xrightarrow{\theta_R} \operatorname{Hom}_R(M,M)$$

is an isomorphism of $\operatorname{Hom}_R(M,M)$-modules, hence is an isomorphism of R-modules. By Corollary 2.8.3 (6), M^* is an R-progenerator. By Proposition 2.3.24, $\operatorname{Hom}_R(M,M)$ is an R-progenerator module. By Proposition 3.5.6, $\operatorname{Hom}_R(M,M)$ is a faithfully flat R-algebra. Therefore, the natural map $\operatorname{Hom}_R(M,M) \to \operatorname{Hom}_R(M,M) \otimes_R S$ is one-to-one. By Proposition 3.5.8, $\operatorname{Hom}_R(M,M) \otimes_R S$ is isomorphic to $\operatorname{Hom}_S((M \oplus N) \otimes_R S, (M \oplus N) \otimes_R S)$. Similarly, the natural map $\operatorname{Hom}_R(M \oplus N, M \oplus N) \to \operatorname{Hom}_S((M \oplus N) \otimes_R S, (M \oplus N) \otimes_R S)$ is one-to-one. Consider the diagram

$$\begin{tikzcd}
\operatorname{Hom}_S(M \otimes_R S, M \otimes_R S) \arrow[r, "\Delta"] & \operatorname{Hom}_S((M \oplus N) \otimes_R S, (M \oplus N) \otimes_R S) \\
\operatorname{Hom}_R(M,M) \otimes_R S \arrow[u, "\cong"] & \operatorname{Hom}_R(M \oplus N, M \oplus N) \otimes_R S \arrow[u, "\cong"'] \\
\operatorname{Hom}_R(M,M) \arrow[u, "\subseteq"] \arrow[r, dashed, "\exists \delta"] & \operatorname{Hom}_R(M \oplus N, M \oplus N) \arrow[u, "\subseteq"']
\end{tikzcd} \tag{6.12}$$

of homomorphisms of R-algebras. Next we show that Δ restricts to a homomorphism $\delta : \operatorname{Hom}_R(M,M) \to \operatorname{Hom}_R(M \oplus N, M \oplus N)$. The proof is by faithfully flat descent. Start with a basis $\{b_1, \dots, b_r\}$ for the S-module $M \otimes_R S$ and extend it to a basis for $(M \oplus N) \otimes_R S$. With respect to these bases, interpret $\operatorname{Hom}_S(M \otimes_R S, M \otimes_R S)$ as r-by-r matrices over S (denoted $M_r(S)$) and $\operatorname{Hom}_S((M \oplus N) \otimes_R S, (M \oplus N) \otimes_R S)$ as rn-by-rn matrices over S (denoted $M_{rn}(S)$). We see that $\Delta : M_r(S) \to M_{rn}(S)$ sends a matrix A to the block diagonal matrix $A \oplus \cdots \oplus A$. Let $e_0 : S \to S \otimes_R S$ be defined by $s \mapsto 1 \otimes s$. Likewise, let $e_1 : S \to S \otimes_R S$ be defined by $s \mapsto s \otimes 1$. Then each e_i is an R-algebra homomorphism. Let $\mathfrak{F}_i$ be the functor from S-modules to $S \otimes_R S$-modules induced by tensoring with e_i. From the description of Δ above we see that $\mathfrak{F}_0(\Delta)$ is equal to $\mathfrak{F}_1(\Delta)$. By Proposition 8.6.4, there exists an R-algebra homomorphism δ such that diagram (6.12) commutes. By the homomorphism δ, we can view $\operatorname{Hom}_R(M,M)$ as a ring of endomorphisms of the R-module $M \oplus N$. By the Morita Theorem 2.8.2, there is an R-module P and a left $\operatorname{Hom}_R(M,M)$-module isomorphism $\sigma : P \otimes_R M \to M \oplus N$. Since $\operatorname{Hom}_R(M,M)$ is an R-algebra, σ is an R-module isomorphism. Since $M \oplus N$ is a free R-module of rank $s = rn$, we are finished. $\square$

7. Hochschild Cohomology

Hochschild cohomology groups first appeared in [**29**] and were applied to study separable algebras over a field. In Theorem 10.1.9 below we derive a criterion for separability based on Hochschild cohomology. A general reference for this section is [**14**, Chapter IX].

DEFINITION 8.7.1. Let R be a commutative ring, A an R-algebra, and $A^e = A \otimes_R A^o$ the enveloping algebra (Definition 5.1.1). If M is a two-sided A/R-module (Definition 5.1.4), then the *nth Hochschild cohomology group of A with coefficients in M* is defined to be

$$\mathrm{H}^n(A,M) = \operatorname{Ext}^n_{A^e}(A,M)$$

where we make M into a left A^e-module by $a \otimes b \cdot x = axb$

7.1. The Standard Complex. Let R be a commutative ring and A an R-algebra. We construct a chain complex $S_\bullet(A) \to A$ of A^e-modules. When A is a projective R-module, $S_\bullet(A)$ is a projective resolution of A as a left A^e-module, and is called the standard resolution. The standard resolution is applied to compute the Hochschild cohomology groups (Definition 8.7.1).

For $n \geq 0$, define left A^e-modules by

$$S_n(A) = \begin{cases} A^e = A \otimes_R A^o & \text{if } n = 0, \\ A \otimes_R (A^{\otimes n}) \otimes_R A & \text{if } n > 0. \end{cases} \tag{7.1}$$

Where $A^{\otimes n}$ denotes the tensor product of n copies of A, and $S_n(A)$ is a left A^e-module by $a \otimes b \cdot x = axb$. For notational convenience, we define $S_{-1}(A)$ to be A. For $n \geq 0$ and for $0 \leq i \leq n$, let $\mu_{n,i} : S_n \to S_{n-1}$ be define by

$$\mu_{n,i}(x_0 \otimes \cdots \otimes x_i \otimes \cdots \otimes x_{n+1}) = x_0 \otimes \cdots \otimes x_i x_{i+1} \otimes \cdots \otimes x_{n+1}.$$

Then $\mu_{n,i}$ is defined by tensoring the multiplication map $\mu : A^e \to A$ in the ith factor with the identity map elsewhere. Define boundary maps $d_n : S_n \to S_{n-1}$ by

$$d_n = \sum_{i=0}^{n} (-1)^n \mu_{n,i}.$$

Since μ is an A^e-module homomorphism, it follows that $\mu_{n,i}$ and d_n are A^e-module homomorphisms.

LEMMA 8.7.2. *In the above context,*

$$\cdots \to S_n(A) \xrightarrow{d_n} S_{n-1}(A) \to \cdots \to S_1 \xrightarrow{d_1} S_0 \xrightarrow{\mu} A \to 0$$

is an exact sequence. If A is projective as an R-module, then $S_\bullet(A) \to A$ is a projective resolution of A as a left A^e-module.

PROOF. By a slight variation of Theorem 2.3.23, we see that if A is a projective R-module, then $S_n(A)$ is a projective A^e-module. We must show that $d_{n-1}d_n = 0$, and that the homology of the complex is (0). For $n \geq -1$ define $k_n : S_n(A) \to S_{n+1}(A)$ by $k_n(x) = 1 \otimes x$. For all $n \geq 0$ and $x \in S_n(A)$, we see that

$$\begin{aligned} d_{n+1}k_n(x) &= d_{n+1}(1 \otimes x) \\ &= x + \sum_{i=1}^{n+1} (-1)^i \mu_{n+1,i}(1 \otimes x) \\ &= x - \sum_{i=0}^{n} (-1)^i 1 \otimes \mu_{n,i}(x) \end{aligned}$$

and

$$\begin{aligned} k_{n-1}d_n(x) &= k_{n+1} \sum_{i=0}^{n} (-1)^i \mu_{n,i}(x) \\ &= \sum_{i=0}^{n} (-1)^i 1 \otimes \mu_{n,i}(x). \end{aligned}$$

Therefore, the contracting homotopy relations

$$d_{n+1}k_n(x) + k_{n-1}d_n = 1$$

are satisfied. Now we show that $d_{n-1}d_n = 0$. For $n = 1$,

$$\mu d_1(x \otimes y \otimes z) = \mu(xy \otimes z - x \otimes yz) = (xy)z - x(yz) = 0$$

by the associative property for multiplication in A. By induction on n and the contracting homotopy relations, it follows that $d_{n-1}d_n = 0$ for all $n \geq 1$ (see the proof of Theorem 8.5.8). Applying Exercise 8.1.8 completes the proof. $\square$

7.2. Cocycle and Coboundary Groups in Low Degree. Let A be an R-algebra which is projective as an R-module. Let M be a left A^e-module. The Hochschild cohomology groups $\mathrm{H}^n(A,M)$ are defined to be $\mathrm{Ext}^n_{A^e}(A,M)$ (Definition 8.7.1). The projective resolution $S_\bullet(A) \to A$ of Lemma 8.7.2 is called the *standard complex of* A. From (7.1) we have

$$S_n(A) = A \otimes_R \left(A^{\otimes n}\right) \otimes_R A = A^e \otimes_R \left(A^{\otimes n}\right).$$

Then the Adjoint Isomorphism (Theorem 2.4.10 (1) implies

$$\begin{aligned}\mathrm{Hom}_{A^e}(S_n(A), M) &\cong \mathrm{Hom}_{A^e}\left(A^e \otimes_R \left(A^{\otimes n}\right), M\right) \\ &\cong \mathrm{Hom}_R\left(A^{\otimes n}, \mathrm{Hom}_{A^e}(A^e, M)\right) \\ &\cong \mathrm{Hom}_R(A^{\otimes n}, M).\end{aligned}$$

By Definition 8.3.8, the cohomology groups are the homology groups of the truncated complex $\mathrm{Hom}_{A^e}(S_\bullet(A), M)$. The terms of low degree are

$$\begin{aligned}(7.2)\quad 0 \to M \xrightarrow{\delta^0} \mathrm{Hom}_R(A,M) \xrightarrow{\delta^1} \mathrm{Hom}_R(A \otimes_R A, M) \\ \xrightarrow{\delta^2} \mathrm{Hom}_R(A \otimes_R A \otimes_R A, M) \xrightarrow{\delta^3} \mathrm{Hom}_R(A^{\otimes 4}, M) \to \cdots.\end{aligned}$$

A tedious computation involving (7.2), the boundary maps d_n of Lemma 8.7.2, the Adjoint Isomorphism, and the Hom functor results in a formula for the coboundary maps. Let $f \in \mathrm{Hom}_R(A^{\otimes n}, M)$ be an n-cochain. Then

$$\begin{aligned}(7.3)\quad (\delta^n f)(x_1 \otimes \cdots \otimes x_{n+1}) = x_1 f(x_2 \otimes \dots x_{n+1}) \\ + \sum_{i=1}^{n} (-1)^i f(x_1 \otimes \cdots \otimes x_i x_{i+1} \otimes \cdots \otimes x_{n+1}) \\ + (-1)^{n+1} f(x_1 \otimes \cdots \otimes x_n) x_{n+1}.\end{aligned}$$

8. Amitsur Cohomology

First we define the Amitsur cohomology groups in Section 8.8.1. Then we show in Section 8.8.2 that the twisted forms of an R-module are parametrized by a certain Amitsur cohomology group of degree one.

Amitsur cohomology was first used in [**1**]. It is the basis of the Čech cohomology which was introduced by Grothendieck and Cartier for schemes. The results presented here are taken from various sources, including [**30**], [**36**] and [**47**]. Most of the material in this section has been published in [**18**, Section 5.5].

8.1. The Definition and First Properties. Let S be a commutative R-algebra. By $S^{\otimes r}$ we denote $S \otimes_R \cdots \otimes_R S$, the tensor product of r copies of S. As in Section 8.6.1, for $0 \leq j \leq n+1$, there is an R-algebra homomorphism

$$\begin{aligned}S^{\otimes(n+1)} &\xrightarrow{e_j} S^{\otimes(n+2)} \\ (x_0 \otimes \cdots \otimes x_n) &\mapsto x_0 \otimes \cdots \otimes x_{j-1} \otimes 1 \otimes x_j \otimes \cdots \otimes x_n.\end{aligned}$$

Let $\mathfrak{F}$ be a covariant functor from the category of commutative R-algebras to the category of abelian groups. The *Amitsur complex* for S/R with coefficients in $\mathfrak{F}$ is

$$1 \to \mathfrak{F}(S) \xrightarrow{d^0} \mathfrak{F}(S^{\otimes 2}) \xrightarrow{d^1} \mathfrak{F}(S^{\otimes 3}) \xrightarrow{d^2} \cdots \tag{8.1}$$

where the coboundary map $d^r : \mathfrak{F}(S^{\otimes(r+1)}) \to \mathfrak{F}(S^{\otimes(r+2)})$ is defined to be

$$d^r = \prod_{i=0}^{r+1} \mathfrak{F}(e_i)^{(-1)^i}.$$

Denote this complex by $C^\bullet(S/R, \mathfrak{F})$. Since $e_j e_i = e_{i+1} e_j$ for all $j \le i$, the reader should verify that (8.1) is a complex of abelian groups.

DEFINITION 8.8.1. In the cochain complex (8.1), the kernel of d^n is the group of n-cocycles, $\mathrm{Z}^n(S/R, \mathfrak{F}) = \ker d^n$. The image of d^{n-1} is the group of n-coboundaries, $\mathrm{B}^n(S/R, \mathfrak{F}) = \operatorname{im} d^{n-1}$. The group of cocycles modulo the coboundaries is

$$\mathrm{H}^n(S/R, \mathfrak{F}) = \mathrm{Z}^n(S/R, \mathfrak{F}) / \mathrm{B}^n(S/R, \mathfrak{F})$$

which is called the *nth Amitsur cohomology group of S/R with coefficients in $\mathfrak{F}$*.

EXAMPLE 8.8.2. In degrees 0 and 1, we have

$$\begin{aligned} \mathrm{Z}^0(S/R, \mathfrak{F}) &= \mathrm{H}^0(S/R, \mathfrak{F}) \\ &= \{\alpha \in \mathfrak{F}(S) \mid \mathfrak{F}(e_0)(\alpha) = \mathfrak{F}(e_1)(\alpha)\} \\ \mathrm{B}^1(S/R, \mathfrak{F}) &= \{\mathfrak{F}(e_0)(\alpha)\mathfrak{F}(e_1)(\alpha^{-1}) \mid \alpha \in \mathfrak{F}(S)\} \\ \mathrm{Z}^1(S/R, \mathfrak{F}) &= \{\alpha \in \mathfrak{F}(S \otimes_R S) \mid \mathfrak{F}(e_2)(\alpha)\mathfrak{F}(e_0)(\alpha) = \mathfrak{F}(e_1)(\alpha)\}. \end{aligned} \tag{8.2}$$

EXAMPLE 8.8.3. For any commutative R-algebra S, let $\mathbb{G}_a(S)$ be the additive abelian group of S. If S is faithfully flat, then by Proposition 8.6.1,

$$\mathrm{H}^n(S/R, \mathbb{G}_a) = \begin{cases} \mathbb{G}_a(R) & \text{if } n = 0 \\ 0 & \text{if } n \ge 1. \end{cases}$$

DEFINITION 8.8.4. When $\mathfrak{F}$ is nonabelian, the cohomology is defined using the relations of (8.2). In this case, the result is not a group, but a pointed set. Let $\mathfrak{F}$ be a functor from the category of commutative R-algebras to the category of groups. We define

$$\mathrm{H}^0(S/R, \mathfrak{F}) = \{\alpha \in \mathfrak{F}(S) \mid \mathfrak{F}(e_0)(\alpha) = \mathfrak{F}(e_1)(\alpha)\}$$

with base point being the group identity of $\mathfrak{F}(S)$. We define

$$\mathrm{Z}^1(S/R, \mathfrak{F}) = \{\alpha \in \mathfrak{F}(S \otimes_R S) \mid \mathfrak{F}(e_2)(\alpha)\mathfrak{F}(e_0)(\alpha) = \mathfrak{F}(e_1)(\alpha)\}$$

with base point being the group identity of $\mathfrak{F}(S \otimes_R S)$. Define a relation on $\mathrm{Z}^1(S/R, \mathfrak{F})$ by $\alpha \sim \beta$ if there exists $\gamma \in \mathfrak{F}(S)$ such that

$$\alpha = \mathfrak{F}(e_1)(\gamma)\beta\mathfrak{F}(e_0)(\gamma^{-1}).$$

The reader should verify that $\sim$ is an equivalence relation. We define $\mathrm{H}^1(S/R, \mathfrak{F})$ to be the set of equivalence classes $\mathrm{Z}^1(S/R, \mathfrak{F})/\sim$, with base point being the equivalence class containing the group identity of $\mathfrak{F}(S \otimes_R S)$. When the functor $\mathfrak{F}$ takes its values in the category of abelian groups, it is clear that this definition agrees with Definition 8.8.1 for $n = 0, 1$.

THEOREM 8.8.5. *Suppose*

$$\begin{tikzcd} S \arrow[r, "f"] & S' \\ R \arrow[u, "\theta"] \arrow[r, "\phi"] & R' \arrow[u, "\theta'"'] \end{tikzcd}$$

is a commutative diagram of homomorphisms of commutative R-algebras. Let $\mathfrak{F}$ be a functor from the category of commutative R-algebras to the category of abelian groups. Then f induces homomorphisms

$$f^* : \mathrm{H}^n(S/R, \mathfrak{F}) \to \mathrm{H}^n(S'/R', \mathfrak{F})$$

for $n \geq 0$. Moreover, f^* is independent of f. That is, if $g : S \to S'$ is another such homomorphism, then $f^* = g^*$. If $\mathfrak{F}$ is a functor that takes its values in the category of nonabelian groups, then the above is true for $n = 0, 1$, where f^* is a morphism of pointed sets.

PROOF. Since $\mathfrak{F}$ is a functor, and the diagram of algebra homomorphisms commutes, f induces a morphism of cochain complexes $f : \mathfrak{F}(S^{\otimes n}) \to \mathfrak{F}((S')^{\otimes n})$. Consequently, there are homomorphisms $f^* : \mathrm{H}^n(S/R, \mathfrak{F}) \to \mathrm{H}^n(S'/R', \mathfrak{F})$.

Case 1: Assume $\mathfrak{F}$ is abelian and use additive notation in the groups $\mathfrak{F}(\cdot)$. By Theorem 8.2.6, it is enough to show that the two morphisms f and g between $\mathfrak{F}(S^{\otimes n})$ and $\mathfrak{F}((S')^{\otimes n})$ are homotopic. We define $k^n : \mathfrak{F}(S^{\otimes (n+1)}) \to \mathfrak{F}((S')^{\otimes n})$ and show that

$$(f^*)^n - (g^*)^n = d^{n-1}k^n + k^{n+1}d^n \tag{8.3}$$

for $n \geq 1$. For $0 \leq i < n$ define $k_i^n : S^{\otimes(n+1)} \to (S')^{\otimes n}$ by

$$k_i^n(s_0 \otimes \cdots \otimes s_n) = f(s_0) \otimes \cdots \otimes f(s_i)g(s_{i+1}) \otimes \cdots \otimes g(s_n). \tag{8.4}$$

Then each k_i^n is an R-algebra homomorphism (Exercises 2.3.10 and 2.3.18). The homotopy operator is defined by $k^n = \sum_{i=0}^{n-1} (-1)^i \mathfrak{F}(k_i^n)$. We define auxiliary R-algebra homomorphisms $h_i^n : S^{\otimes(n+1)} \to (S')^{\otimes(n+1)}$ by

$$h_i^n(s_0 \otimes \cdots \otimes s_n) = \begin{cases} g(s_0) \otimes \cdots \otimes g(s_n) & \text{if } i = 0 \\ f(s_0) \otimes \cdots \otimes f(s_{i-1}) \otimes g(s_i) \otimes \cdots \otimes g(s_n) & \text{if } 1 \leq i \leq n \\ f(s_0) \otimes \cdots \otimes f(s_n) & \text{if } i = n+1. \end{cases} \tag{8.5}$$

The reader should verify the relations

$$k_j^{n+1} e_i = \begin{cases} e_{i-1} k_j^n & \text{if } j < i-1 \\ h_i^n & \text{if } i-1 \leq j \leq i \\ e_i k_{j-1}^n & \text{if } i < j. \end{cases} \tag{8.6}$$

Starting with the right-most term in (8.3),

$$\begin{aligned} k^{n+1}d^n &= \sum_{j=0}^{n} \sum_{i=0}^{n+1} (-1)^j (-1)^i \mathfrak{F}(k_j^{n+1}) \mathfrak{F}(e_i) \\ &= \sum_{j=0}^{n} \sum_{i=0}^{n+1} (-1)^{j+i} \mathfrak{F}(k_j^{n+1} e_i) \end{aligned}$$

Using (8.6), we get

$$
\begin{aligned}
k^{n+1}d^n &= \sum_{i=2}^{n+1}\sum_{j=0}^{i-2}(-1)^{j+i}\mathfrak{F}(e_{i-1}k^n_j) \\
&\quad + \sum_{i=1}^{n+1}(-1)^{i-1+i}\mathfrak{F}(h_i) + \sum_{i=0}^{n}(-1)^{i+i}\mathfrak{F}(h_i) \\
&\quad + \sum_{i=0}^{n-1}\sum_{j=i+1}^{n}(-1)^{j+i}\mathfrak{F}(e_ik^n_{j-1})) \\
&= \sum_{i=2}^{n+1}\sum_{j=0}^{i-2}(-1)^{j+i}\mathfrak{F}(e_{i-1}k^n_j) \\
&\quad + \mathfrak{F}(h_0) - \mathfrak{F}(h_{n+1}) \\
&\quad + \sum_{i=0}^{n-1}\sum_{j=i+1}^{n}(-1)^{j+i}\mathfrak{F}(e_ik^n_{j-1})) \\
&= \sum_{j=0}^{n-1}(-1)^{j+n+1}\mathfrak{F}(e_nk^n_j) \\
&\quad + \sum_{i=1}^{n-1}\left(\sum_{j=0}^{i-1}(-1)^{j+i+1}\mathfrak{F}(e_ik^n_j)) + \sum_{j=i}^{n-1}(-1)^{j+i+1}\mathfrak{F}(e_ik^n_j))\right) \\
&\quad + \sum_{j=0}^{n-1}(-1)^{j}\mathfrak{F}(e_0k^n_j)) \\
&\quad + \mathfrak{F}(h_0) - \mathfrak{F}(h_{n+1}) \\
&= (g^*)^n - (f^*)^n - \sum_{i=0}^{n}\sum_{j=0}^{n-1}(-1)^{j+i}\mathfrak{F}(e_ik^n_j)) \\
&= (g^*)^n - (f^*)^n - d^{n-1}k^n
\end{aligned}
$$

Which proves the theorem when $\mathfrak{F}$ is abelian.

Case 2: Assume $\mathfrak{F}$ is non-abelian (written multiplicatively) and $n = 0$. Let $k^1_0 : S \otimes_R S \to S'$ be as in (8.4). Note that $k^1_0 e_0 = g$ and $k^1_0 e_1 = f$. If $\alpha \in \mathrm{Z}^0(S/R, \mathfrak{F})$, then $\mathfrak{F}(g)\alpha = \mathfrak{F}(k^1_0 e_0)\alpha = \mathfrak{F}(k^1_0)\mathfrak{F}(e_0)\alpha = \mathfrak{F}(k^1_0)\mathfrak{F}(e_1)\alpha = \mathfrak{F}(k^1_0 e_1)\alpha = \mathfrak{F}(f)\alpha$.

Case 3: Assume $\mathfrak{F}$ is non-abelian (written multiplicatively) and $n = 1$. Let k^2_0 and k^2_1 be the R-algebra homomorphisms defined in (8.4). If $\alpha \in \mathrm{Z}^1(S/R, \mathfrak{F})$, then on the one hand,

$$
\begin{aligned}
\mathfrak{F}(f \otimes g)(\alpha) &= \mathfrak{F}(h^1_1)(\alpha) \quad \text{(by (8.5))} \\
&= \mathfrak{F}(k^2_0 e_1)(\alpha) \quad \text{(by (8.6))} \\
&= \mathfrak{F}(k^2_0 e_2)(\alpha)\mathfrak{F}(k^2_0 e_0)(\alpha) \quad (\text{since } \alpha \in \mathrm{Z}^1(S/R, \mathfrak{F})) \\
&= \mathfrak{F}(e_1 k^1_0)(\alpha)\mathfrak{F}(h^1_0)(\alpha) \quad \text{(by (8.6))} \\
&= \mathfrak{F}(e_1 k^1_0)(\alpha)\mathfrak{F}(g \otimes g)(\alpha) \quad \text{(by (8.5))}.
\end{aligned} \tag{8.7}
$$

On the other hand,

$$
\begin{aligned}
\mathfrak{F}(f\otimes g)(\alpha) &= \mathfrak{F}(h_1^1)(\alpha) \quad \text{(by (8.5))}\\
&= \mathfrak{F}(k_1^2 e_1)(\alpha) \quad \text{(by (8.6))}\\
&= \mathfrak{F}(k_1^2 e_2)(\alpha)\mathfrak{F}(k_1^2 e_0)(\alpha) \quad (\text{since } \alpha\in \mathrm{Z}^1(S/R,\mathfrak{F}))\\
&= \mathfrak{F}(h_2^1)(\alpha)\mathfrak{F}(e_0 k_0^1)(\alpha) \quad \text{(by (8.6))}\\
&= \mathfrak{F}(f\otimes f)(\alpha)\mathfrak{F}(e_0 k_0^1)(\alpha) \quad \text{(by (8.5))}.
\end{aligned}
\tag{8.8}
$$

Set $\gamma=\mathfrak{F}(k_0^1)(\alpha)$. Combining (8.7) and (8.8),

$$\mathfrak{F}(f\otimes f)(\alpha)=\mathfrak{F}(e_1)(\gamma)\mathfrak{F}(g\otimes g)(\alpha)\mathfrak{F}(e_0)(\gamma^{-1})$$

which shows $\mathfrak{F}(f\otimes f)\sim\mathfrak{F}(g\otimes g)$. $\square$

8.2. Twisted Forms. Let R be a commutative ring and $\mathfrak{C}_{\mathrm{fl}}(R)$ the category of isomorphism classes of faithfully flat R-algebras. If A is an R-module (or R-algebra), let $\mathrm{Aut}(A)$ denote the functor from $\mathfrak{C}_{\mathrm{fl}}(R)$ to the category of groups defined by $S\mapsto \mathrm{Aut}_S(A\otimes_R S)$.

DEFINITION 8.8.6. Let R be a commutative ring and A a fixed R-module (or R-algebra). Given an R-module (or R-algebra) B and a faithfully flat R-algebra S, we say B is a *twisted form of A for the extension S/R* if there exists an isomorphism of S-algebras $B\otimes_R S\cong A\otimes_R S$.

PROPOSITION 8.8.7. *In the above context, the pointed set* $\mathrm{H}^1(S/R,\mathrm{Aut}(A))$ *classifies up to R-module (or R-algebra) isomorphism the twisted forms of A for the extension S/R.*

PROOF. Suppose B is a twisted form of A for the extension S/R, and $\beta: B\otimes_R S\to A\otimes_R S$ is an S-module isomorphism. In a switch from the notation of Proposition 8.6.4, we write β_i instead of $\mathfrak{F}_i(\beta)$. Define $\theta\in\mathrm{Aut}_{S\otimes_R S}(A\otimes_R S\otimes_R S)$ by $\theta=\beta_1\beta_0^{-1}$. So θ is the map that makes the diagram

$$
\begin{tikzcd}
& A\otimes_R S\otimes_R S \arrow[dd, "\theta"] \\
B\otimes_R S\otimes_R S \arrow[ur, "\beta_0"] \arrow[dr, "\beta_1"'] & \\
& A\otimes_R S\otimes_R S
\end{tikzcd}
$$

commute. The reader should verify the identities: $(\beta_0)_0=(\beta_0)_1$, $(\beta_0)_2=(\beta_1)_0$, $(\beta_1)_1=(\beta_1)_2$. Therefore, $\theta_2\theta_0=(\beta_1\beta_0^{-1})_2(\beta_1\beta_0^{-1})_0=(\beta_1)_2(\beta_0^{-1})_2(\beta_1)_0(\beta_0^{-1})_0=(\beta_1)_1(\beta_0^{-1})_1=(\beta_1\beta_0^{-1})_1=\theta_1$. So θ is a 1-cocycle. To show that the cohomology class of θ depends only on B, suppose $\alpha: B\otimes_R S\to A\otimes_R S$ is another S-module isomorphism, and $\phi=\alpha_1\alpha_0^{-1}$. Set $\gamma=\alpha\beta^{-1}$. Then γ is an S-module automorphism of $A\otimes_R S$. We have $\gamma_1\theta\gamma_0^{-1}=\gamma_1(\beta_1\beta_0^{-1})\gamma_0^{-1}=\alpha_1\beta_1^{-1}(\beta_1\beta_0^{-1})\beta_0\alpha_0^{-1}=\alpha_1\alpha_0^{-1}=\phi$. Therefore, ϕ is cohomologous to θ.

Let $\theta\in\mathrm{Aut}_{S\otimes_R S}(A\otimes_R S\otimes S)$. Assume θ is a 1-cocycle in $\mathrm{Z}^1(S/R,\mathrm{Aut}(A))$. In a switch from the notation of Section 8.8.1, write θ_i instead of $\mathfrak{F}(e_i)(\theta)$. Then $\theta_2\theta_0=\theta_1$. As in Section 8.6.3, for $i=0,1$ there are R-module homomorphisms $e_i: A\otimes_R S\to A\otimes_R S\otimes_R S$. Define

$$
\begin{aligned}
B&=\left\{\sum a_i\otimes s_i\in A\otimes_R S \mid \theta\left(\sum a_i\otimes 1\otimes s_i\right)=\sum a_i\otimes s_i\otimes 1\right\}\\
&=\ker\left\{\theta e_0-e_1: A\otimes_R S\to A\otimes_R S\otimes_R S\right\}.
\end{aligned}
$$

Then B is an R-module. Define $\beta : B \otimes_R S \to A \otimes_R S$ to be the multiplication map, $\beta((\sum a_i \otimes s_i) \otimes s) = \sum a_i \otimes s_i s$. As in the proof of Theorem 8.6.7, the reader should verify that β is an isomorphism of S-modules and $\theta = \beta_1 \beta_0^{-1}$. Therefore B is a twisted form of A for the extension S/R.

To see that B depends only on the cohomology class of θ, suppose ϕ is a 1-cocycle that is cohomologous to θ. Then there is $\gamma \in \operatorname{Aut}(A \otimes_R S)$ such that $\gamma_1 \theta \gamma_0^{-1} = \phi$. Since ϕ is a descent datum, there is an R-module C, and an isomorphism $\alpha : C \otimes_R S \to A \otimes_R S$ such that $\phi = \alpha_1 \alpha_0^{-1}$. It follows from

$$\begin{aligned} \phi &= \gamma_1 \theta \gamma_0^{-1} \\ \alpha_1 \alpha_0^{-1} &= \gamma_1 \beta_1 \beta_0^{-1} \gamma_0^{-1} \\ \alpha_0^{-1} \gamma_0 \beta_0 &= \alpha_1^{-1} \gamma_1 \beta_1 \end{aligned}$$

that $(\alpha^{-1}\gamma\beta)_0 = (\alpha^{-1}\gamma\beta)_1$. In the notation of Proposition 8.6.4, we see that $\mathfrak{F}_0(\alpha^{-1}\gamma\beta) = \mathfrak{F}_0(\alpha^{-1}\gamma\beta)$. This implies the isomorphism $\alpha^{-1}\gamma\beta : B \otimes_R S \to C \otimes_R S$ of S-modules comes from an isomorphism $B \cong C$ of R-modules. □

8.2.1. *Twisted Form of a Finitely Generated Free Module.* Let R be a commutative ring and denote by R^n the direct sum of n copies of R. Let S be a commutative faithfully flat R-algebra. A free module of rank n is a projective module of rank n. It follows from Lemma 3.5.12 that a twisted form of R^n for S/R is a projective module of rank n. The group $\operatorname{Aut}_S(R^n \otimes_R S) = \operatorname{Aut}_S(S^n)$ is isomorphic to the group of invertible matrices in $M_n(S)$. The group of invertible n-by-n matrices over S is also denoted $\mathrm{GL}_n(S)$ and is called the *general linear group*. We also denote by GL_n the functor from $\mathfrak{C}_{\mathrm{fl}}$ to the category of groups defined by $S \mapsto \mathrm{GL}_n(S)$.

COROLLARY 8.8.8. *Let S be a commutative faithfully flat R-algebra.*

(1) The twisted forms of the free R-module of rank n for S/R are classified up to isomorphism by the pointed set $\mathrm{H}^1(S/R, \mathrm{GL}_n)$.

(2) If R is a ring for which finitely generated projective modules are free, then $\mathrm{H}^1(S/R, \mathrm{GL}_n) = \{1\}$. *This is true, for instance, if R is a local ring (Proposition 3.4.2), or a PID (Example 2.1.6).*

For $n = 1$, the general linear group $\mathrm{GL}_1(S)$ is equal to $S^* = \mathbb{G}_m(S)$, the group of invertible elements of S. Since S is commutative, $\mathbb{G}_m(S)$ is an abelian group and the pointed set $\mathrm{H}^1(S/R, \mathrm{GL}_n)$ is a group. By Corollary 8.8.8, $\mathrm{H}^1(S/R, \mathbb{G}_m)$ classifies the group of rank one projective R-modules P such that $P \otimes_R S \cong S$. This and Proposition 3.6.8 proves

COROLLARY 8.8.9. *In the above context, the group* $\mathrm{H}^1(S/R, \mathbb{G}_m)$ *is isomorphic to the kernel of the natural homomorphism* $\operatorname{Pic} R \to \operatorname{Pic} S$.

8.2.2. *Twisted Form of a Finitely Generated Free Algebra.* Let $R^n = R \oplus \cdots \oplus R$ be the trivial commutative separable extension of R of rank n. Let S be a commutative faithfully flat R-algebra. It follows from Proposition 5.6.10 that if B is a twisted form of R^n for S/R, then B is a separable R-algebra which is an R-module progenerator of constant rank n.

8.2.3. *Twisted Form of Matrices.* If S is a commutative R-algebra, then the S-algebra $M_n(R) \otimes_R S$ is naturally isomorphic to $M_n(S)$. Let $\operatorname{Aut}(M_n)$ denote the functor from $\mathfrak{C}_{\mathrm{fl}}$, the category of faithfully flat R-algebras, to the category of groups, defined by $S \mapsto \operatorname{Aut}_S(M_n(S))$. Now let S be a commutative faithfully flat R-algebra. By Proposition 8.8.7, $\mathrm{H}^1(S/R, \operatorname{Aut}(M_n))$ classifies the twisted forms of $M_n(R)$ for S/R.

CHAPTER 9

Prime Ideals in Commutative Rings

This chapter consists of more results on the subject of Commutative Algebra. For the most part, the topics involve prime ideals in noetherian commutative rings. The notions of prime ideals, primary ideals, and more generally primary submodules of an R-module are closely tied to the notion of zero divisors, and in particular to the notion of nilpotency. In a commutative ring R, an ideal P is prime if if P is not the unit ideal and R/P has no zero divisors. The ideal P is primary if P is not the unit ideal and any zero divisor in R/P is nilpotent. If M is an R-module and $P \in \operatorname{Spec} R$, then P is an associated prime of M if there is a cyclic submodule of M isomorphic to R/P. A primary submodule of M is a submodule N such that M/N has a unique associated prime. An ideal P is a primary ideal in R if and only if P is a primary submodule of R. The main result on this subject is the Primary Decomposition Theorem, which says that every submodule N of a finitely generated module M over a noetherian ring R can be written as an intersection of primary submodules. This is proved in Theorem 9.3.8 below. A graded version of this theorem is proved in Theorem 9.5.6. Theorem 9.5.13 states sufficient conditions on a graded module for the existence of the Hilbert polynomial.

Zariski's Main Theorem can be summarized by saying a quasi-finite morphism factors into an open immersion followed by a finite morphism (see Corollary 9.4.16).

The Krull dimension of a commutative ring is defined in terms of the lengths of chains of prime ideals in $\operatorname{Spec} R$. We prove the fundamental properties of this dimension. The Krull dimension of a polynomial ring in n indeterminates over a field k is equal to n.

We end this chapter with a proof of the Krull-Akizuki Theorem, which shows that the integral closure of a noetherian integral domain with Krull dimension one in a finite algebraic extension of its quotient field is also a noetherian integral domain with Krull dimension one.

1. Primary Ideals in a Commutative ring

In this section, R is a commutative ring. An ideal I in R is a primary ideal if I is not the unit ideal, and any zero divisor in R/I is nilpotent. A prime ideal is a primary ideal. The nil radical of a primary ideal is a prime ideal. A general reference for this section is [**4**].

LEMMA 9.1.1. *Let R be a commutative ring and I an ideal of R. The following are equivalent.*

(1) $I \neq R$ and if $xy \in I$, then either $x \in I$ or $y^n \in I$ for some $n > 0$.
(2) $R/I \neq 0$ and any zero divisor in R/I is nilpotent.

PROOF. Is left to the reader. □

An ideal that satisfies one of the equivalent conditions in Lemma 9.1.1 is called a *primary ideal*. In Definition 9.3.2, the more general notion of primary submodule is introduced. By Definition 1.5.1, an ideal I in a commutative ring R is prime if and only if R/I

is an integral domain. Therefore, a prime ideal satisfies Lemma 9.1.1 (2) and we see that a prime ideal is a primary ideal.

By Proposition 9.1.2 (1), the nil radical of a primary ideal is a prime ideal. For a given prime ideal P, an ideal I is said to be *P-primary*, if I is a primary ideal and $\operatorname{Rad}(I) = P$.

PROPOSITION 9.1.2. *Let R be a commutative ring and I an ideal of R.*

(1) *If I is a primary ideal, then $P = \operatorname{Rad}(I)$ is a prime ideal. Hence I is P-primary.*
(2) *If $\mathfrak{m} = \operatorname{Rad}(I)$ is a maximal ideal, then I is $\mathfrak{m}$-primary.*
(3) *If $I = \mathfrak{m}^n$ where $\mathfrak{m}$ is a maximal ideal and $n > 0$, then I is $\mathfrak{m}$-primary.*

PROOF. (1): Assume $xy \in \operatorname{Rad}(I)$. For some $n > 0$, $(xy)^n = x^n y^n \in I$. If $x^n \notin I$, then y^{nm} is in I for some $m > 0$. Therefore, one of x or y is in $\operatorname{Rad}(I)$.

(2): By Lemma 3.3.7, there is only one prime ideal that contains I, namely $\mathfrak{m}$. Therefore, R/I is a local ring and the Jacobson radical is $\mathfrak{m}/I$, which is equal to the nil radical. Then every element of R/I is either a unit, or a nilpotent. Every zero divisor of R/I is nilpotent.

(3): This is Exercise 9.1.2. □

PROPOSITION 9.1.3. *Let R be a commutative noetherian ring.*

(1) *The nil radical $\operatorname{Rad}_R(0)$ is nilpotent.*
(2) *Let I be an ideal of R and let $N = \operatorname{Rad}(I)$. For some $n > 0$, $N^n \subseteq I$.*

PROOF. (1): Assume $N = \operatorname{Rad}_R(0)$ is generated by $x_1, \dots, x_m$. For each i, there exists $e_i > 0$ such that $x_i^{e_i} = 0$. Take $n = e_1 + \cdots + e_m$. Then N^n is generated by elements of the form $x_1^{d_1} \cdots x_m^{d_m}$ where $d_1 + \cdots + d_m = n$. For at least one i we have $d_i \geq e_i$, so $N^n = 0$.

(2): Apply (1) to the ring R/I. □

COROLLARY 9.1.4. *Let R be a commutative noetherian ring, $\mathfrak{m}$ a maximal ideal of R. For an ideal I of R, the following are equivalent.*

(1) *I is $\mathfrak{m}$-primary.*
(2) $\operatorname{Rad}(I) = \mathfrak{m}$.
(3) *For some $n > 0$, $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$.*

PROOF. (1) is equivalent to (2): Follows from Proposition 9.1.2.

(2) implies (3): Follows from Proposition 9.1.3.

(3) implies (2): Follows from Exercise 3.3.4. □

1.1. Exercises.

EXERCISE 9.1.1. Let $f : R \to S$ be a homomorphism of commutative rings. Show that if I is a primary ideal of S, then $f^{-1}(I)$ is a primary ideal of R.

EXERCISE 9.1.2. Show that if $\mathfrak{m}$ is a maximal ideal in the commutative ring R, then $\mathfrak{m}^n$ is $\mathfrak{m}$-primary, for any positive integer n.

EXERCISE 9.1.3. Let R be a commutative ring and $W \subseteq S$ a multiplicative set. Let P be a prime ideal in R and let I be a P-primary ideal. Prove:

(1) If $P \cap W \neq \emptyset$, then $W^{-1}I = W^{-1}R$.
(2) If $P \cap W = \emptyset$, then $(W^{-1}I) \cap R = I$.
(3) $\operatorname{Rad}(W^{-1}I) = W^{-1}\operatorname{Rad}(I)$.
(4) If $P \cap W = \emptyset$, then $W^{-1}I$ is $W^{-1}P$-primary.
(5) There is a one-to-one correspondence between primary ideals in $W^{-1}R$ and primary ideals I of R such that $I \subseteq R - W$.

EXERCISE 9.1.4. Let k be a field and $A = k[x,y]$ the polynomial ring in two variables over k. Let $I = (x,y^2)$. Show that every zero divisor in A/I is nilpotent. Conclude that I is $\mathfrak{m}$-primary, where $\mathfrak{m} = (x,y) = \operatorname{Rad}(I)$.

EXERCISE 9.1.5. Let k be a field and $A = k[x,y]$ the polynomial ring in two variables over k. Let R be the k-subalgebra of A generated by x^2, xy, y^2. In R, let $P = (x^2, xy)$.

(1) Prove that P is prime, $P^2 = (x^4, x^3y, x^2y^2)$, and $\operatorname{Rad}(P^2) = P$. Show that y^2 is a zero divisor in R/P^2 which is not nilpotent. Conclude that P^2 is not a primary ideal.
(2) In R, let $I = (x^2)$. Prove that I is P-primary. (Hint: show that R_P is a principal ideal domain and P^2R_P is a primary ideal. Show that $x^2 \in P^2R_P$.)

EXERCISE 9.1.6. Let k be a field and $A = k[x,y]$ the polynomial ring in two variables over k. Let R be the k-subalgebra of A generated by $x^2, xy, y^2, x^3, x^2y, xy^2, y^3$. In R, let $P = (x^2, xy, x^3, x^2y, xy^2)$ and $I = (x^3)$. Prove:

(1) P is prime. (Hint: $R/P \cong k[y^2, y^3]$.)
(2) $P = \operatorname{Rad}(I)$.
(3) In R/I the elements y^2 and y^3 are zero divisors, but not nilpotent. Conclude that I is not a primary ideal.

EXERCISE 9.1.7. Let R be a noetherian commutative ring. Let I be an ideal of R and $N = \operatorname{Rad}(I)$ the nil radical of I. Prove that the I-adic topology on R is equal to the N-adic topology on R and the I-adic completion of R is isomorphic to the N-adic completion of R. (Hint: Exercise 7.1.5 and Proposition 9.1.3.)

2. The Associated Primes of a Module

In this section R is a commutative noetherian ring. General references for the material in this section are [**12**] and [**41**].

LEMMA 9.2.1. *Let R be a commutative noetherian ring, M an R-module, and $P \in \operatorname{Spec} R$. The following are equivalent.*

(1) There exists an element $x \in M$ such that $\operatorname{annih}_R(x) = P$.
(2) M contains a submodule isomorphic to R/P.

PROOF. Is left to the reader. □

If $P \in \operatorname{Spec} R$ satisfies one of the conditions of Lemma 9.2.1, then P is called an *associated prime* of M. The set of all associated primes of M in $\operatorname{Spec} R$ is denoted $\operatorname{Assoc}_R(M)$, or simply $\operatorname{Assoc}(M)$. If $r \in R$ and $\ell_r : M \to M$ is "left multiplication by r", then we say r is a *zero divisor* for M in case ℓ_r is not one-to-one. If r is not a zero divisor for M, then we say r is *M-regular*.

PROPOSITION 9.2.2. *Let R be a commutative noetherian ring and M an R-module.*

(1) If P is a maximal member of the set of ideals $\mathscr{C} = \{\operatorname{annih}_R(x) \mid x \in M - (0)\}$, then P is an associated prime of M.
(2) $M = 0$ if and only if $\operatorname{Assoc}(M) = \emptyset$.
(3) The set of zero divisors of M is equal to the union of the associated primes of M.
(4) If P is a prime ideal of R, then $\operatorname{Assoc}_R(R/P) = \{P\}$.
(5) If N is a submodule of M, then

$$\operatorname{Assoc}(N) \subseteq \operatorname{Assoc}(M) \subseteq \operatorname{Assoc}(N) \cup \operatorname{Assoc}(M/N).$$

(6) *Suppose I is an index set and $\{M_\alpha \mid \alpha \in I\}$ is a family of submodules of M such that $M = \bigcup_\alpha M_\alpha$. Then*

$$\operatorname{Assoc}_R(M) = \bigcup_{\alpha \in I} \operatorname{Assoc}_R(M_\alpha).$$

PROOF. (1): Suppose $P = \operatorname{annih}(x)$ is a maximal member of $\mathscr{C}$. Assume $a, b \in R$, $ab \in P$, and $b \notin P$. Then $bx \neq 0$ and $abx = 0$. But $P = \operatorname{annih}(x) \subseteq \operatorname{annih}(bx)$. By maximality of P, we conclude $a \in P$.

(2): If $M = 0$, then clearly $\operatorname{Assoc}(M) = \emptyset$. If M is nonzero, then in Part (1) we see that $\mathscr{C}$ is nonempty. Because R is noetherian, $\mathscr{C}$ contains a maximal member which is an associated prime of M.

(3): If $r \in R$, $x \in M - (0)$ and $rx = 0$, then $r \in \operatorname{annih}(x)$. By Parts (1) and (2), there exists a prime ideal P which contains r and which is an associated prime of M. Conversely, if P is an associated prime, every element of P is a zero divisor of M.

(4): If $x + P \neq P$, then in the integral domain R/P, the principal ideal $Rx + P$ is a free R/P-module.

(5): The inclusion $\operatorname{Assoc}(N) \subseteq \operatorname{Assoc}(M)$ follows straight from Lemma 9.2.1. Let $P \in \operatorname{Assoc}(M)$ and let $S \subseteq M$ be a submodule that is isomorphic to R/P. If $S \cap N = (0)$, then S is isomorphic to a submodule of M/N, so $P \in \operatorname{Assoc}(M/N)$. If $x \in S \cap N$, $x \neq 0$, then by Part (4) the cyclic submodule Rx is isomorphic to R/P. In this case, $P \in \operatorname{Assoc}(N)$.

(6): Is left to the reader. $\square$

COROLLARY 9.2.3. *Let R be a commutative noetherian ring and $\{M_\alpha \mid \alpha \in I\}$ a family of R-modules, where I is an index set. If $M = \bigoplus_{\alpha \in I} M_\alpha$ is the direct sum, then* $\operatorname{Assoc}_R(M) = \bigcup_{\alpha \in I} \operatorname{Assoc}_R(M_\alpha)$.

PROOF. If I is a singleton set, then there is nothing to prove.

Step 1: Assume $I = \{\alpha, \beta\}$ has cardinality two. Since the sequence $0 \to M_\alpha \to M \to M_\beta \to 0$ is split exact, Proposition 9.2.2 (5) applied twice gives $M_\alpha \cup M_\beta \subseteq M \subseteq M_\alpha \cup M_\beta$.

Step 2: Assume $n \geq 2$ and I is a finite set of cardinality n. Then by Mathematical Induction and Step 1, $\operatorname{Assoc}_R(M) = \bigcup_{\alpha \in I} \operatorname{Assoc}_R(M_\alpha)$.

Step 3: Assume I is infinite. Let $F = \{S \subseteq I \mid S \text{ is a finite subset of } I \text{ and } |S| \geq 1\}$. By Proposition 9.2.2 (6) and Step 2,

$$\begin{aligned}
\operatorname{Assoc}_R(M) &= \bigcup_{S \in F} \operatorname{Assoc}_R\left(\bigoplus_{\alpha \in S} M_\alpha\right) \\
&= \bigcup_{S \in F} \bigcup_{\alpha \in S} \operatorname{Assoc}_R(M_\alpha) \\
&= \bigcup_{\alpha \in I} \operatorname{Assoc}_R(M_\alpha).
\end{aligned}$$

$\square$

PROPOSITION 9.2.4. *Let R be a commutative noetherian ring, M an R-module, and Φ a subset of* $\operatorname{Assoc}(M)$. *Then there exists a submodule N of M such that* $\operatorname{Assoc}(N) = \operatorname{Assoc}(M) - \Phi$ *and* $\operatorname{Assoc}(M/N) = \Phi$.

PROOF. Let $\mathfrak{S}$ be the set of all submodules S of M such that $\operatorname{Assoc}(S) \subseteq \operatorname{Assoc}(M) - \Phi$. Since $(0) \in \mathfrak{S}$, $\mathfrak{S} \neq \emptyset$. We partially order $\mathfrak{S}$ by set inclusion. If $\{S_\alpha\}$ is a chain in $\mathfrak{S}$, then by Proposition 9.2.2 (6), the union $\bigcup S_\alpha$ is also in $\mathfrak{S}$. By Zorn's Lemma, there exists a maximal element, say N, in $\mathfrak{S}$. By Proposition 9.2.2 (5), to finish the proof it suffices to show $\operatorname{Assoc}(M/N) \subseteq \Phi$. Let $\mathfrak{p} \in \operatorname{Assoc}(M/N)$. Then there is a submodule F/N of M/N such that F/N is isomorphic to $R/\mathfrak{p}$. By Proposition 9.2.2 (2), we know $N \subsetneq F$. By Proposition 9.2.2 (4) and (5), $\operatorname{Assoc}(F) \subseteq \operatorname{Assoc}(N) \cup \operatorname{Assoc}(F/N) \subseteq \operatorname{Assoc}(N) \cup \{\mathfrak{p}\}$. Since N is a maximal member of $\mathfrak{S}$, we know $\operatorname{Assoc}(F) \not\subseteq \operatorname{Assoc}(N)$. Therefore, $\mathfrak{p} \in \Phi$. $\square$

See Corollary 9.3.11 for a generalization of Lemma 9.2.5.

LEMMA 9.2.5. *Let R be a commutative noetherian ring and M an R-module. Let $W \subseteq R$ be a multiplicative set and $\theta : R \to W^{-1}R$ the localization. Let $\Phi = \{P \in \operatorname{Spec} R \mid P \cap W = \emptyset\}$. Then*

$$\begin{aligned}\theta^\sharp(\operatorname{Assoc}_{W^{-1}R}(W^{-1}M)) &= \operatorname{Assoc}_R(M) \cap \Phi \\ &= \operatorname{Assoc}_R(W^{-1}M).\end{aligned}$$

PROOF. By Exercise 3.3.9, the continuous map $\theta^\sharp : \operatorname{Spec}(W^{-1}R) \to \operatorname{Spec} R$ is one-to-one and has image equal to Φ.

Step 1: Suppose $P \in \operatorname{Assoc}_R(M) \cap \Phi$. By Lemma 9.2.1, there exists $x \in M$ such that $P = \operatorname{annih}_R(x)$. The diagram

$$\begin{tikzcd} 0 \arrow[r] & P \arrow[r] \arrow[d] & R \arrow[r, "1\mapsto x"] \arrow[d, "\theta"'] & Rx \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & W^{-1}P \arrow[r] & W^{-1}R \arrow[r, "1\mapsto x/1"] & (W^{-1}R)(x/1) \arrow[r] & 0 \end{tikzcd}$$

commutes and has exact rows. This proves $W^{-1}P$ is equal to $\operatorname{annih}_{W^{-1}R}(x/1)$. Since $P = \theta^\sharp(W^{-1}P)$, we have

$$\operatorname{Assoc}_R(M) \cap \Phi \subseteq \theta^\sharp(\operatorname{Assoc}_{W^{-1}R}(W^{-1}M)).$$

Step 2: Suppose $P \in \Phi$ and $W^{-1}P$ is an associated prime of $W^{-1}M$. Then $W^{-1}P = \operatorname{annih}_{W^{-1}R}(x/t)$ for some $x \in M$, $t \in W$. Then $\operatorname{annih}_R(x/t) = W^{-1}P \cap R = P$, so $P \in \operatorname{Assoc}_R(W^{-1}M)$. That is,

$$\theta^\sharp(\operatorname{Assoc}_{W^{-1}R}(W^{-1}M)) \subseteq \operatorname{Assoc}_R(W^{-1}M).$$

Since R is noetherian, P is finitely generated. Write $P = Ra_1 + \cdots + Ra_n$ for some elements $a_i \in P$. For each a_i we have $(a_i/1)(x/t) = 0$. That is, there exists $w_i \in W$ such that $w_i a_i x = 0$. Let $w = w_1 w_2 \cdots w_n$. Given any $y = \sum_i r_i a_i \in P$, it follows that $ywx = \sum_i r_i w a_i x = 0$. This proves $P \subseteq \operatorname{annih}_R(wx)$. For the reverse inclusion, suppose $u \in R$ and $uwx = 0$. Then $(u/1)(x/t) = 0$ so $u/1$ is in $\operatorname{annih}_{W^{-1}R}(x/t) = W^{-1}P$. This proves $P = \operatorname{annih}_R(wx)$ is an associated prime of M, so

$$\theta^\sharp(\operatorname{Assoc}_{W^{-1}R}(W^{-1}M)) \subseteq \operatorname{Assoc}_R(M) \cap \Phi.$$

Step 3: Suppose $P \in \operatorname{Assoc}_R(W^{-1}M)$. Then $P = \operatorname{annih}_R(x/t)$ for some $x \in M$, $t \in W$. If $w \in P \cap W$, then $w(x/t) = 0$ implies $x/t = 0$. Therefore, $P \in \Phi$. The diagram

$$\begin{tikzcd} 0 \arrow[r] & P \arrow[r] \arrow[d] & R \arrow[r, "1\mapsto x/t"] \arrow[d, "\theta"'] & R(x/t) \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & W^{-1}P \arrow[r] & W^{-1}R \arrow[r, "1\mapsto x/t"] & (W^{-1}R)(x/t) \arrow[r] & 0 \end{tikzcd}$$

commutes and the rows are exact. Therefore, $W^{-1}P = \operatorname{annih}_{W^{-1}R}(x/t)$. It follows that $W^{-1}P \in \operatorname{Assoc}_{W^{-1}R}(W^{-1}M)$. Since $\theta^\sharp(W^{-1}P) = P$, this proves

$$\operatorname{Assoc}_R(W^{-1}M) \subseteq \theta^\sharp(\operatorname{Assoc}_{W^{-1}R}(W^{-1}M)),$$

which completes the proof. □

PROPOSITION 9.2.6. *Let R be a noetherian commutative ring and M an R-module. Let $W \subseteq R$ be a multiplicative set. Let $\Psi = \{\mathfrak{p} \in \operatorname{Assoc}_R(M) \mid \mathfrak{p} \cap W = \emptyset\}$. If K is the kernel of the localization homomorphism $\theta : M \to W^{-1}M$, then K is the unique submodule of M such that* $\operatorname{Assoc}_R(K) = \operatorname{Assoc}_R(M) - \Psi$ *and* $\operatorname{Assoc}_R(M/K) = \Psi$.

PROOF. Let N be any submodule of M such that $\operatorname{Assoc}_R(N) = \operatorname{Assoc}_R(M) - \Psi$ and $\operatorname{Assoc}_R(M/N) = \Psi$. There exists at least one such N, by Proposition 9.2.4. The proof consists in showing $N = \ker\theta$. Let $\pi : M \to M/N$ be the natural projection. The sequence

$$0 \to W^{-1}N \to W^{-1}M \xrightarrow{1\otimes\pi} W^{-1}(M/N) \to 0$$

is exact because $W^{-1}R$ is a flat R-module (Lemma 3.1.7). If $\mathfrak{p} \in \operatorname{Assoc}_R(N)$, then $\mathfrak{p} \cap W \neq \emptyset$. By Lemma 9.2.5, $\operatorname{Assoc}_R(W^{-1}N) = \emptyset$. By Proposition 9.2.2 (2), $W^{-1}N = (0)$, hence $1\otimes\pi$ is one-to-one. Now consider the localization map $\beta : M/N \to W^{-1}(M/N)$. We have $\operatorname{Assoc}_R(\ker\beta) \subseteq \operatorname{Assoc}_R(M/N) \subseteq \Psi$. For contradiction's sake, suppose $\mathfrak{p} \in \operatorname{Assoc}_R(\ker\beta)$. Then there is some $x \in \ker\beta$ and $\mathfrak{p} = \operatorname{annih}_R(x)$. Since $\beta(x) = 0$, $\mathfrak{p} \cap W = \operatorname{annih}_R(x) \cap W \neq \emptyset$. In other words, $\mathfrak{p} \notin \Psi$. This contradiction implies $\operatorname{Assoc}_R(\ker\beta) = \emptyset$, and therefore $\ker\beta = (0)$. In the commutative diagram

$$\begin{tikzcd}
M \arrow[r, "\pi"] \arrow[d, "\theta"'] & M/N \arrow[d, "\beta"] \\
W^{-1}M \arrow[r, "1\otimes\pi"] & W^{-1}(M/N)
\end{tikzcd}$$

the maps β and $1\otimes\pi$ are one-to-one. Therefore, $K = \ker\theta = \ker\pi = N$. □

Let M be a module over the commutative ring R. If $P \in \operatorname{Spec} R$, then the *stalk* of M at P is the localization M_P of M with respect to the multiplicative set $R - P$. The *support* of M is the set of all points in $\operatorname{Spec} R$ for which the stalk of M is nontrivial,

$$\operatorname{Supp}_R(M) = \{P \in \operatorname{Spec} R \mid M_P \neq 0\}.$$

If R is understood, we write simply $\operatorname{Supp}(M)$.

THEOREM 9.2.7. *Let R be a noetherian commutative ring and M an R-module.*

(1) $\operatorname{Assoc}(M) \subseteq \operatorname{Supp}(M)$.
(2) If $P \in \operatorname{Supp}(M)$, then P contains a member of $\operatorname{Assoc}(M)$. *If P is a minimal member of* $\operatorname{Supp}(M)$, *then $P \in \operatorname{Assoc}(M)$.*
(3) The sets $\operatorname{Assoc}(M)$ *and* $\operatorname{Supp}(M)$ *have the same minimal elements.*
(4) If I is an ideal in R, then the minimal associated primes of the R-module R/I are precisely the minimal prime over-ideals of I.

PROOF. (1): Let $P \in \operatorname{Assoc}(M)$ and set $W = R - P$. By Lemma 9.2.5, $W^{-1}P$ is an associated prime of $W^{-1}M = M_P$. By Proposition 9.2.2, it follows that $M_P \neq 0$.

(2): Let $P \in \operatorname{Supp}(M)$. Then $M_P \neq 0$. By Proposition 9.2.2, M_P has an associated prime in R_P. By Lemma 9.2.5, elements of $\operatorname{Assoc}_{R_P}(M_P)$ correspond bijectively to elements of $\operatorname{Assoc}_R(M)$ that are contained in P. This proves that P contains an element of

$\mathrm{Assoc}_R(M)$. If P is a minimal member of $\mathrm{Supp}(M)$, then $\mathrm{Supp}(M_P)$ contains only one prime, namely PR_P. In this case, it follows that P is a minimal element in $\mathrm{Assoc}(M)$.

(3): Follows from the arguments in (1) and (2).

(4): By Exercise 9.2.1, the support of the module R/I is $V(I)$. □

PROPOSITION 9.2.8. *Let R be a noetherian commutative ring. Then the following are true.*

(1) The set of zero divisors of R is equal to the union of the associated primes of R.
(2) If $P_1,\dots,P_n$ are the minimal prime over-ideals of (0), then $\{P_1,\dots,P_n\}$ is a subset of $\mathrm{Assoc}(R)$.
(3) The nil radical of R, $\mathrm{Rad}_R(0)$, is equal to the intersection of the associated primes of R.
(4) If R is an integral domain, then $\mathrm{Assoc}(R) = \{(0)\}$.
(5) If R is a commutative artinian ring, then $\mathrm{Assoc}(R) = \mathrm{Spec}\, R$.

PROOF. Part (1) follows from Proposition 9.2.2 (3). Part (2) follows from Theorem 9.2.7 (4). Part (3) follows from (2) and Lemma 3.3.7. Part (4) is immediate from (1). Part (5) follows from Theorem 4.5.6 and (1). □

DEFINITION 9.2.9. Let R be a noetherian commutative ring and M an R-module. If $P \in \mathrm{Assoc}(M)$ and P is not a minimal member of $\mathrm{Assoc}(M)$, then we say *P is an embedded prime of M*.

THEOREM 9.2.10. *Let R be a noetherian commutative ring and M a nonzero finitely generated R-module.*

(1) There exists a filtration $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$ of M and a set of prime ideals $P_i \in \mathrm{Spec}\, R$ such that $M_i/M_{i-1} \cong R/P_i$ for $i = 1,\dots,n$.
(2) If $P_1,\dots,P_n$ are the primes mentioned in Part (1), then $\mathrm{Assoc}(M) \subseteq \{P_1,\dots,P_n\} \subseteq \mathrm{Supp}(M)$.
(3) $\mathrm{Assoc}(M)$ is a finite set.

PROOF. (1): Assume $M \neq (0)$. By Proposition 9.2.2, $\mathrm{Assoc}(M) \neq \emptyset$, so there exists a submodule S of M isomorphic to R/P for some prime P. Define $\mathscr{C}$ to be the set of all submodules $S \subseteq M$ such that S has the kind of filtration specified in Part (1). Since $\mathscr{C}$ is nonempty and R is noetherian, $\mathscr{C}$ has a maximal member, say N. If $N \neq M$, then by Proposition 9.2.2, $\mathrm{Assoc}(M/N) \neq \emptyset$. By Lemma 9.2.1 applied to M/N there is a submodule S of M such that $N \subsetneq S \subseteq M$ and $S/N \cong R/P$ for some prime P. Therefore, $S \in \mathscr{C}$ which is a contradiction. This proves Part (1).

(2): By Proposition 9.2.2 (4), $\mathrm{Assoc}(M_i/M_{i-1}) = \{P_i\}$. Proposition 9.2.2 (5), applied $n-1$ times, yields

$$\begin{aligned}\mathrm{Assoc}(M) &\subseteq \mathrm{Assoc}(M_1) \cup \mathrm{Assoc}(M_2/M_1) \cup \cdots \cup \mathrm{Assoc}(M_n/M_{n-1}) \\ &\subseteq \{P_1,\dots,P_n\}.\end{aligned}$$

By Exercise 9.2.1, the support of the R-module R/P_i is $V(P_i)$, which contains P_i. By Exercise 9.2.2, $P_i \in \mathrm{Supp}(M_i) \subseteq \mathrm{Supp}(M)$. This proves Part (2).

(3): This follows straight from Part (2). □

EXAMPLE 9.2.11. Let $R = \mathbb{Z}/36$, a principal ideal ring of order 36. Then R is isomorphic to the direct sum $\mathbb{Z}/4 \oplus \mathbb{Z}/9$ and R has exactly two prime ideals, namely $P = 2R$ and $Q = 3R$. So R/P is a field of order 2 and R/Q is a field of order 3. Note that P is the annihilator of the coset containing 18, and Q is the annihilator of the coset containing 12. Since

R is artinian, Proposition 9.2.8 (4) implies $\operatorname{Assoc}(R) = \operatorname{Spec} R = \operatorname{Supp}(R) = \{P, Q\}$. We illustrate the conclusion of Theorem 9.2.10, where we take M to be R, the free R-module of rank one. Set $M_0 = (0)$, $M_1 = 18R$, $M_2 = 9R$, $M_3 = 3R$, $M_4 = R$. Now we determine the sequence of primes P_i, $1 \le i \le 4$. We have $M_1 \cong R/P$, so $P_1 = P$. Likewise, $M_2/M_1 \cong R/P$, so $P_2 = P$, $M_3/M_2 \cong R/Q$, so $P_3 = Q$, and $M_4/M_3 \cong R/Q$, so $P_4 = Q$.

2.1. Exercises.

EXERCISE 9.2.1. Let R be a commutative ring and I an ideal in R. Let $P \in \operatorname{Spec} R$. Prove that $(R/I)_P \neq 0$ if and only if $I \subseteq P$. Conclude that $\operatorname{Supp}(R/I)$ is equal to $V(I)$. In particular, $\operatorname{Supp}(R) = \operatorname{Spec} R$.

EXERCISE 9.2.2. Let R be a commutative ring, M an R-module and N a submodule. Show that

$$\operatorname{Supp}(M) = \operatorname{Supp}(N) \cup \operatorname{Supp}(M/N).$$

(Hint: Localize the exact sequence $0 \to N \to M \to M/N \to 0$.)

EXERCISE 9.2.3. Let R be a commutative ring, M an R-module and $\{M_\alpha \mid \alpha \in I\}$ a collection of submodules such that $\sum_{\alpha \in I} M_\alpha = M$. Show that

$$\operatorname{Supp}(M) = \bigcup_{\alpha \in I} \operatorname{Supp}(M_\alpha).$$

(Hint: Use Exercise 9.2.2 and the exact sequence $\bigoplus_{\alpha \in I} M_\alpha \to M \to 0$.)

EXERCISE 9.2.4. Let R be a commutative ring, M an R-module and $\{x_\alpha \mid \alpha \in I\}$ a set of generators for M. Show that

$$\begin{aligned} \operatorname{Supp}(M) &= \bigcup_{\alpha \in I} \operatorname{Supp}(Rx_\alpha) \\ &= \bigcup_{\alpha \in I} V\big(\operatorname{annih}(x_\alpha)\big). \end{aligned}$$

(Hint: Use Exercise 9.2.1, Exercise 9.2.3, and the isomorphism $Rx_\alpha \cong R/\operatorname{annih}(x_\alpha)$.)

EXERCISE 9.2.5. Let R be a commutative ring and $I_1, \dots, I_n$ some ideals in R. Show that

$$V(I_1 \cap \cdots \cap I_n) = V(I_1 \cdots I_n) = V(I_1) \cup \cdots \cup V(I_n).$$

(Hint: Use Lemma 6.3.3 and Lemma 3.3.3.)

EXERCISE 9.2.6. Let R be a commutative ring and M a finitely generated R-module. Show that $\operatorname{Supp}(M) = V\big(\operatorname{annih}(M)\big)$. Conclude that $\operatorname{Supp}(M)$ is a closed subset of $\operatorname{Spec} R$. (Hint: $\operatorname{annih}(M) = \bigcap_{i=1}^n \operatorname{annih}(x_i)$ where $x_1, \dots, x_n$ is a generating set for M. Use Exercise 9.2.4 and Exercise 9.2.5.)

EXERCISE 9.2.7. Let R be a noetherian commutative ring, M a finitely generated R-module and I an ideal of R such that $\operatorname{Supp}(M) \subseteq V(I)$. Show that there exists $n > 0$ such that $I^n M = 0$. (Hint: Show that $\operatorname{Rad}(I) \subseteq \operatorname{Rad}(\operatorname{annih}(M))$. Use Proposition 9.1.3.)

EXERCISE 9.2.8. Let R be a commutative ring and M a finitely generated R-module. Show that the minimal associated primes of M are precisely the minimal prime over-ideals of $\operatorname{annih}(M)$.

EXERCISE 9.2.9. Let R be a commutative noetherian ring and $P_1, \dots, P_n$ the complete list of distinct minimal primes of the zero ideal. Prove that the kernel of the natural map

$$R \xrightarrow{\phi} \bigoplus_{i=1}^{n} R/P_i$$

is equal to the nil radical of R.

EXERCISE 9.2.10. Let A and R be as in Exercise 9.1.6. In R, let $I = (x^3)$ and $\mathfrak{m} = (x^2, xy, y^2, x^3, x^2y, xy^2, y^3)$. Prove:

(1) $\mathfrak{m}$ is a maximal ideal.
(2) $x^4\mathfrak{m} \subseteq I$.
(3) $\mathfrak{m} \in \operatorname{Assoc}_R(R/I)$.

EXERCISE 9.2.11. Let R be a noetherian commutative ring, M a finitely generated R-module and N an arbitrary R-module. Prove:

(1) $\operatorname{Supp}(\operatorname{Hom}_R(M,N)) \subseteq \operatorname{Supp}(M)$.
(2) For any $n \geq 1$, $\operatorname{Assoc}_R(N) = \operatorname{Assoc}_R(\bigoplus_{i=1}^{n} N)$.
(3) If $R^n \to M \to 0$ is an exact sequence, then $0 \to \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(R^n,N)$ is an exact sequence.
(4) If $\mathfrak{p} \in \operatorname{Assoc}_R(\operatorname{Hom}_R(M,N))$, then $\mathfrak{p} \in \operatorname{Assoc}_R(N) \cap \operatorname{Supp}(M)$.

EXERCISE 9.2.12. Let R be a noetherian commutative ring, M a finitely generated R-module, and N an arbitrary R-module. Let $\mathfrak{p} \in \operatorname{Assoc}_R(N) \cap \operatorname{Supp}(M)$. Follow the steps below to prove that $\mathfrak{p} \in \operatorname{Assoc}_R(\operatorname{Hom}_R(M,N))$.

(1) $M \otimes_R k(\mathfrak{p}) \neq 0$, where $k(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is the residue field.
(2) The natural map $\operatorname{Hom}_{k(\mathfrak{p})}(M \otimes_R k(\mathfrak{p}), k(\mathfrak{p})) \to \operatorname{Hom}_{R_\mathfrak{p}}(M \otimes_R k(\mathfrak{p}), k(\mathfrak{p}))$ is one-to-one, hence both modules are nonzero.
(3) The natural map $\operatorname{Hom}_{R_\mathfrak{p}}(M \otimes_R k(\mathfrak{p}), k(\mathfrak{p})) \to \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, k(\mathfrak{p}))$ is one-to-one, hence both modules are nonzero.
(4) $\operatorname{Hom}_R(M, R/\mathfrak{p})$ is nonzero.
(5) $\mathfrak{p}$ is an associated prime of $\operatorname{Hom}_R(M, R/\mathfrak{p})$.
(6) $\mathfrak{p}$ is an associated prime of $\operatorname{Hom}_R(M,N)$.

EXERCISE 9.2.13. Let R be a noetherian integral domain and M a finitely generated nonzero R-module. Prove that the following are equivalent.

(1) M is torsion free (see Definition 1.7.13).
(2) $\operatorname{Assoc}_R(M) = \{(0)\}$.
(3) $\operatorname{Hom}_R(M,M)$ is torsion free.

(Hint: Exercises 9.2.11, and 9.2.12.)

EXERCISE 9.2.14. Let R be a noetherian commutative local ring with maximal ideal $\mathfrak{m}$. Let C be a finitely generated nonzero R-module and assume $\operatorname{Assoc}_R(C) = \{\mathfrak{m}\}$. Prove that if M is a finitely generated nonzero R-module, then $\operatorname{Hom}_R(M,C)$ is nonzero. (Hint: Exercise 9.2.12.)

EXERCISE 9.2.15. Let R be an integral domain and M and N two R-modules. Prove that if N is torsion free (Definition 1.7.13), then $\operatorname{Hom}_R(M,N)$ is torsion free. (Hint: Prove this directly, it does not require any theorem from this chapter.)

EXERCISE 9.2.16. Let R be a commutative noetherian ring which decomposes into an internal direct sum $R = Re_1 \oplus \cdots \oplus Re_n$, where $\{e_1, \dots, e_n\}$ is a set of orthogonal idempotents. For each i, let $P_i = \operatorname{annih}_R(e_i)$. Assume each ring Re_i is an integral domain. Prove:

(1) $\operatorname{Assoc}(R) = \{P_1, \dots, P_n\}$.
(2) The chain of ideals $(0) \subsetneq Re_1 \subsetneq Re_1 \oplus Re_2 \subsetneq \cdots \subsetneq Re_1 \oplus Re_2 \oplus \cdots \oplus Re_n$ is a filtration of R such that together with the primes $\{P_1, \dots, P_n\}$, the conclusion of Theorem 9.2.10 is satisfied.

3. Primary Decomposition Theorem

Throughout this section R is a commutative noetherian ring. We prove in Theorem 9.3.8 below that if M is a finitely generated module over R, then any submodule N has a primary decomposition. For instance, if I is a proper ideal in R, then Theorem 9.3.8 states that I has a unique representation as an intersection of primary ideals in R. Generally, an ideal I does not have a factorization as a product of prime ideals, or even a product of primary ideals. We will see in Section 12.3 below that if R is an integrally closed noetherian integral domain such that every nonzero prime ideal in R is maximal, then I has a unique factorization into a product of prime ideals (Theorem 12.3.2). General references for the material in this section are [**12**] and [**41**].

3.1. Primary Submodules.

PROPOSITION 9.3.1. *If R is a noetherian commutative ring and M is an R-module, then (1) and (2) are equivalent.*

(1) $\operatorname{Assoc}(M) = \{P\}$. *In words, M has exactly one associated prime.*
(2) *(a)* $M \neq 0$, *and*
(b) if $r \in R$ is a zero divisor for M, then for every $x \in M$ there exists $n > 0$ such that $r^n x = 0$.

PROOF. (1) implies (2): Suppose r is a zero divisor for M. By Proposition 9.2.2 (3), $r \in P$. Given any $x \in M - (0)$, $Rx \neq 0$. Therefore $\emptyset \neq \operatorname{Assoc}(Rx) \subseteq \operatorname{Assoc}(M) = \{P\}$, which implies $\operatorname{Assoc}(Rx) = \{P\}$. By Theorem 9.2.7 (3), P is the unique minimal member of $\operatorname{Supp}(Rx)$. By Exercise 9.2.6, P is the unique minimal member of $V(\operatorname{annih}(Rx))$. Therefore, $P = \operatorname{Rad}(\operatorname{annih}(Rx)))$. There exists $n > 0$ such that $r^n \in \operatorname{annih}(Rx)$.

(2) implies (1): Let P be the set of all zero divisors in R for M. By (2), if $r \in P$ and $x \in M$, then there exists $n > 0$ such that $r^n x = 0$. The reader should verify that P is an ideal in R. Let $Q \in \operatorname{Assoc}(M)$. There exists $x \in M$ such that $Q = \operatorname{annih}(x)$. Every element of Q is a zero divisor, so $Q \subseteq P$. Given $r \in P$, there exists $n > 0$ such that $r^n \in \operatorname{annih}(x) = Q$. Since Q is prime, this implies $r \in Q$. So $P \subseteq Q$. $\square$

DEFINITION 9.3.2. Let R be a noetherian commutative ring and M an R-module. Suppose N is a submodule of M and M/N satisfies the equivalent conditions of Proposition 9.3.1. That is, assume $\operatorname{Assoc}(M/N) = \{P\}$. Then we say N is a *P-primary submodule of M*. Suppose I is an ideal of R. Comparing Lemma 9.1.1 and Proposition 9.3.1 we see that I is a primary submodule of R if and only if I is a primary ideal of R and in this case, $\operatorname{Assoc}_R(R/I) = \operatorname{Rad}(I)$.

LEMMA 9.3.3. *Let R be a noetherian commutative ring, M an R-module, and P a prime ideal of R. If S, T are P-primary submodules of M, then $S \cap T$ is a P-primary submodule of M.*

PROOF. The sequence

$$0 \to M/(S \cap T) \to M/S \oplus M/T$$

is exact. By Proposition 9.2.2 (5), $\operatorname{Assoc}(M/(S \cap T)) \subseteq \operatorname{Assoc}(M/S) \cup \operatorname{Assoc}(M/T) = \{P\}$. Since $M/(S \cap T) \neq 0$, it follows that P is the only associated prime of $M/(S \cap T)$. $\square$

3.2. Primary Decomposition.

DEFINITION 9.3.4. Let R be a noetherian commutative ring, M an R-module, and N a submodule of M. A *primary decomposition* of N is a representation of the form $N = Y_1 \cap Y_2 \cap \cdots \cap Y_n$ where each Y_i is a primary submodule of M. Let P_i denote the associated prime of M/Y_i. The primary decomposition $N = Y_1 \cap Y_2 \cap \cdots \cap Y_n$ is called *reduced* in case

(1) $P_1, \dots, P_n$ are distinct prime ideals and
(2) for $j = 1, 2, \dots, n$ we have $Y_j \not\supseteq \bigcap_{i \neq j} Y_i$.

A primary decomposition can always be simplified to a reduced one. In fact, any submodule Y_j for which (2) fails is redundant hence can be removed. Furthermore, Lemma 9.3.3 says that we can merge by intersection all of the Y_i that have the same associated prime.

LEMMA 9.3.5. *Let R be a noetherian commutative ring, M an R-module, and N a submodule of M. Suppose $N = Y_1 \cap Y_2 \cap \cdots \cap Y_n$ is a reduced primary decomposition. For each i, let P_i be the associated prime ideal of M/Y_i. Then*

(1) $\operatorname{Assoc}(M/N) = \{P_1, \dots, P_n\}$.
(2) In a reduced primary decomposition of N, the set of associated prime ideals is uniquely determined by N.

PROOF. This proof uses Proposition 9.2.2, Parts (2) and (5). The sequence

$$0 \to N \to M \to \bigoplus_{i=1}^{n} M/Y_i$$

is exact. Therefore $\operatorname{Assoc}(M/N) \subseteq \operatorname{Assoc}(M/Y_1) \cup \cdots \cup \operatorname{Assoc}(M/Y_n) = \{P_1, \dots, P_n\}$. Fix j and let $N_j = \bigcap_{i \neq j} Y_i$. Then $N_j \cap Y_j = N$, so the sequence

$$0 \to N \to N_j \to M/Y_j$$

is exact. Therefore $\operatorname{Assoc}(N_j/N) \subseteq \operatorname{Assoc}(M/Y_j) = \{P_j\}$. Since the decomposition of N is reduced, $N_j/N \neq 0$, and $\operatorname{Assoc}(N_j/N) \neq \emptyset$. Thus $P_j \in \operatorname{Assoc}(N_j/N)$. Because

$$0 \to N \to N_j \to M/N$$

is exact, we conclude that $P_j \in \operatorname{Assoc}(N_j/N) \subseteq \operatorname{Assoc}(M/N)$. □

PROPOSITION 9.3.6. *Let R be a noetherian commutative ring, $P, Q \in \operatorname{Spec} R$, M an R-module and N a P-primary submodule of M. Let $\theta : M \to M_Q$ be the localization.*

(1) If $P \not\subseteq Q$, then $N_Q = M_Q$.
(2) If $P \subseteq Q$, then $N = M \cap N_Q$. That is, $N = \theta^{-1}(N_Q)$.

PROOF. (1): By assumption, $\operatorname{Assoc}_R(M/N) = \{P\}$. Let $\Phi = \{x \in \operatorname{Spec} R \mid x \subseteq Q\}$. Then $\operatorname{Assoc}_R(M/N) \cap \Phi = \emptyset$. By Lemma 9.2.5, $\operatorname{Assoc}_R\big((M/N)_Q\big) = \emptyset$. But Proposition 9.2.2 (2) implies $M_Q/N_Q = (M/N)_Q = 0$.

(2): By Proposition 9.3.1, the set of all zero divisors for M/N is equal to P, which is contained in Q. The set $R - Q$ does not contain any zero divisors for M/N, so the localization map $M/N \to (M/N)_Q = M_Q/N_Q$ is one-to-one. □

COROLLARY 9.3.7. *Let R be a noetherian commutative ring, M an R-module and N a submodule of M which possesses a reduced primary decomposition, $N = Y_1 \cap \cdots \cap Y_n$. Let P_i denote the associated prime of M/Y_i.*

(1) If P_i is a minimal member of $\operatorname{Assoc}(M/N)$*, then $Y_i = M \cap N_{P_i}$.*
(2) In a reduced primary decomposition of N, a primary component belonging to a minimal associated prime is uniquely determined by N and the prime.

PROOF. (1): If $i \neq j$, then by Proposition 9.3.6 applied with $N = Y_j$, $P = P_j$, $Q = P_i$, it follows that $(Y_j)_{P_i} = M_{P_i}$. On the other hand, $M \cap (Y_i)_{P_i} = Y_i$. Together with Exercise 3.1.1, we get

$$\begin{aligned} M \cap N_{P_i} &= M \cap (Y_1 \cap \cdots \cap Y_n)_{P_i} \\ &= M \cap \left((Y_1)_{P_i} \cap \cdots \cap (Y_n)_{P_i} \right) \\ &= M \cap (Y_i)_{P_i} \\ &= Y_i \end{aligned}$$

(2): Follows from (1). $\square$

THEOREM 9.3.8. *Let R be a noetherian commutative ring and M an R-module.*

(1) *For each $P \in \operatorname{Assoc}(M)$ there exists a P-primary submodule Y_P of M such that $(0) = \bigcap_{P \in \operatorname{Assoc}(M)} Y_P$.*
(2) *If M is finitely generated and N is a submodule of M, then there exists a primary decomposition $N = \bigcap_{P \in \operatorname{Assoc}(M/N)} Y_P$, where Y_P is a P-primary submodule of M.*

PROOF. (1): Fix $P \in \operatorname{Assoc}(M)$. Let $\mathscr{C}$ be the set of all submodules S of M such that P is not an associated prime of S. Because $(0) \in \mathscr{C}$, this is a nonempty set. Given a linearly ordered subset $\{S_i \mid i \in I\} \subseteq \mathscr{C}$, let $S = \bigcup_{i \in I} S_i$. Then S is a submodule of M and $P \notin \operatorname{Assoc}(S)$. Therefore, $S \in \mathscr{C}$. By Zorn's Lemma, Proposition 1.2.4, there exists a maximal member, say Y, in $\mathscr{C}$. Because $P \in \operatorname{Assoc}(M)$ and $P \notin \operatorname{Assoc}(Y)$, Proposition 9.2.2 (5) implies $P \in \operatorname{Assoc}(M/Y)$. To show that Y is P-primary, suppose $P' \in \operatorname{Assoc}(M/Y)$ and $P' \neq P$. Then there exists a submodule $Y \subsetneq Y' \subseteq M$ such that $Y'/Y \cong R/P'$. Therefore $\operatorname{Assoc}(Y'/Y) = \{P'\}$ and by Proposition 9.2.2 (5), $P \notin \operatorname{Assoc}(Y') \subseteq \operatorname{Assoc}(Y) \cup \{P'\}$. Then $Y' \in \mathscr{C}$ which contradicts the maximal choice of Y. We have shown that $Y_P = Y$ is P-primary. Since

$$\operatorname{Assoc}\left(\bigcap_{P \in \operatorname{Assoc}(M)} Y_P \right) \subseteq \bigcap_{P \in \operatorname{Assoc}(M)} \operatorname{Assoc}(Y_P) = \emptyset,$$

it follows from Proposition 9.2.2 (2) that $\bigcap_{P \in \operatorname{Assoc}(M)} Y_P = (0)$. This proves (1).

(2): Apply Part (1) to the module M/N. The set $\operatorname{Assoc}(M/N)$ is finite, by Theorem 9.2.10. $\square$

3.3. Exercise.

EXERCISE 9.3.1. Let R be a commutative noetherian ring, $P \in \operatorname{Spec} R$, and $n \geq 1$. Prove:

(1) P is the unique minimal associated prime of P^n.
(2) The P-primary component of P^n is uniquely determined by P and n. The P-primary component of P^n is denoted $P^{(n)}$ and is called the nth *symbolic power* of P.
(3) $P^{(n)} = P^n R_P \cap R$.

3.4. Flat Algebras and Associated Primes. Throughout this section R and S will be commutative rings. Usually R and S will be noetherian. Let $f : R \to S$ be a homomorphism of rings, and $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 3.3.3. Let $P \in \operatorname{Spec} R$. The residue field at P is $k(P) = R_P / PR_P$. The fiber over P of the map $f^\sharp$ is $\operatorname{Spec}(S \otimes_R k(P))$, which is homeomorphic to $(f^\sharp)^{-1}(P)$, by Exercise 3.4.3. By Exercise 3.4.2, if Q is a prime ideal of S lying over P, then the corresponding prime ideal of $S \otimes_R k(P)$ is $Q \otimes_R k(P)$ and the local ring is $S_Q \otimes_R k(P) = S_Q/PS_Q$.

PROPOSITION 9.3.9. *Let $f : R \to S$ be a homomorphism of commutative noetherian rings, and M an S-module. Then*

$$f^\sharp(\operatorname{Assoc}_S(M)) = \operatorname{Assoc}_R(M).$$

PROOF. Step 1: Show $f^\sharp(\operatorname{Assoc}_S(M)) \subseteq \operatorname{Assoc}_R(M)$. Suppose $Q \in \operatorname{Assoc}_S(M)$. By Lemma 9.2.1, there exists $x \in M$ such that $Q = \operatorname{annih}_S(x)$. Now $\operatorname{annih}_R(x) = \operatorname{annih}_S(x) \cap R = Q \cap R = f^\sharp(Q)$, which proves Step 1.

Step 2: We show that $f^\sharp(\operatorname{Assoc}_S(M)) \supseteq \operatorname{Assoc}_R(M)$. Suppose $P \in \operatorname{Assoc}_R(M)$. By Lemma 9.2.1, there exists $x \in M$ such that $P = \operatorname{annih}_R(x)$. Set $N = \operatorname{annih}_S(x)$. By Theorem 9.3.8 there exists a reduced primary decomposition $N = Y_1 \cap Y_2 \cap \cdots \cap Y_n$. For each i, Y_i is a primary ideal in S. By Proposition 9.1.2, let $Q_i = \operatorname{Rad}_S(Y_i)$ be the associated prime ideal of S/Y_i. Then $\operatorname{Assoc}_S(S/N) = \{Q_1, \dots, Q_n\}$, by Lemma 9.3.5. The cyclic submodule Sx of M is isomorphic to S/N. By Proposition 9.2.2, each Q_i is in $\operatorname{Assoc}_S(M)$. The proof will be complete if we show $P = Q_i \cap R = f^\sharp(Q_i)$ for some i. For contradiction's sake, assume $P \neq Q_i \cap R$ for each i. We have $P = \operatorname{annih}_R(x) = \operatorname{annih}_S(x) \cap R = N \cap R \subseteq Y_i \cap R \subseteq Q_i \cap R$. So for each i there exists $y_i \in Q_i \cap R - P$. Since $Q_i = \operatorname{Rad}_S(Y_i)$, there exists $\alpha_i > 0$ such that $y_i^{\alpha_i} \in Y_i \cap R$. Then $y = y_1^{\alpha_1} \cdots y_n^{\alpha_n} \in Y_1 \cdots Y_n \cap R \subseteq Y_1 \cap \cdots \cap Y_n \cap R = N \cap R = P$. Since P is a prime ideal, $y_i \in P$ for some i. This is a contradiction. $\square$

THEOREM 9.3.10. *Let $f : R \to S$ be a homomorphism of commutative noetherian rings, B an S-module that is flat as an R-module. Then the following are true.*

(1) For each $P \in \operatorname{Spec} R$,

$$\begin{aligned} f^\sharp(\operatorname{Assoc}_S(B/PB)) &= \operatorname{Assoc}_R(B/PB) \\ &= \begin{cases} \{P\} & \text{if } B/PB \neq (0) \\ \emptyset & \text{if } B/PB = (0). \end{cases} \end{aligned}$$

(2) If A is any R-module, then

$$\operatorname{Assoc}_S(A \otimes_R B) = \bigcup_{P \in \operatorname{Assoc}_R(A)} \operatorname{Assoc}_S(B/PB).$$

PROOF. (1): By Proposition 9.2.2 (2)) we can assume $B/PB \neq (0)$, otherwise all of the sets are empty. By Theorem 2.3.23, $B/PB = B \otimes_R R/P$ is a flat R/P-module. Since R/P is an integral domain, B/PB is a torsion free R/P-module, by Exercise 3.7.3. Applying Proposition 9.3.9 twice,

$$\begin{aligned} f^\sharp(\operatorname{Assoc}_S(B/PB)) &= \operatorname{Assoc}_R(B/PB) \\ &= \eta^\sharp\left(\operatorname{Assoc}_{R/P}(B/PB)\right) \\ &= \eta^\sharp(\{(0)\}) \\ &= \{P\} \end{aligned}$$

where $\eta : R \to R/P$ is the natural homomorphism.

(2): First we show the right hand side is contained in the left. We remark that this part of the proof does not require R to be noetherian. Let $P \in \operatorname{Assoc}_R(A)$. There exists $x \in A$ and R/P is isomorphic to the cyclic submodule $Rx \subseteq A$. Tensoring with B which is a flat R-module, we see that $R/P \otimes_R B = B/PB$ is isomorphic to the S-submodule $Rx \otimes_R B$ of $A \otimes_R B$. By Proposition 9.2.2 (5), $\operatorname{Assoc}_S(A \otimes_R B) \supseteq \operatorname{Assoc}_S(B/PB)$.

Now we show the left hand side is contained in the right. This part of the proof is split into three cases.

Case 1: We show that the result is true if A is a finitely generated R-module and $\operatorname{Assoc}_R(A) = \{P\}$ is a singleton set. Let $x_1, \dots, x_m$ be a generating set for A over R. For any $r \in P$, there is $n > 0$ such that $r^n x_i = 0$ for all i (Proposition 9.3.1). For any $a \in A$, $r^n a = 0$. Let $Q \in \operatorname{Assoc}_S(A \otimes_R B)$. Then there is $z = \sum_{i=1}^t a_i \otimes b_i \in A \otimes_R B$ such that $Q = \operatorname{annih}_S(z)$. Since $r^n a_i = 0$ for each i, $r^n \in Q$. Since Q is a prime ideal, $r \in Q$. This shows $Q \cap R \supseteq P$. Given $r \in R - P$, r is not a zero divisor for M. That is, $\ell_r : A \to A$ is one-to-one. Since B is R-flat, $\ell_r \otimes 1 : A \otimes_R B \to A \otimes_R B$ is one-to-one. Therefore, r is not in Q. Hence $Q \cap R \subseteq P$. We have shown that $f^\sharp(\operatorname{Assoc}_S(A \otimes_R B)) = \operatorname{Assoc}_R(A) = \{P\}$.

Now apply Theorem 9.2.10 to get a filtration $0 = A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n = A$ of A and a set of prime ideals $P_i \in \operatorname{Spec} R$ such that $A_i/A_{i-1} \cong R/P_i$ for $i = 1, \dots, n$. Since B is R-flat, $0 = A_0 \otimes_R B \subsetneq A_1 \otimes_R B \subsetneq A_2 \otimes_R B \subsetneq \cdots \subsetneq A_n \otimes_R B = A \otimes_R B$ is a filtration of $A \otimes_R B$ and $A_i \otimes_R B / A_{i-1} \otimes_R B \cong R/P_i \otimes_R B = B/P_i B$ for $i = 1, \dots, n$. Proposition 9.2.2 (5), applied $n-1$ times, yields

$$\operatorname{Assoc}_S(A \otimes_R B) \subseteq \bigcup_{i=1}^{n} \operatorname{Assoc}_S(B/P_i B).$$

By Part (1), if $Q \in \operatorname{Assoc}_S(B/P_i B)$, then $Q \cap R = P_i$. By what we proved in the first paragraph of Case 1, if $P_i \neq P$, then $Q \notin \operatorname{Assoc}_S(A \otimes_R B)$. This proves $\operatorname{Assoc}_S(A \otimes_R B) \subseteq \operatorname{Assoc}_S(B/PB)$.

Case 2: We prove (2) is true if A is a finitely generated R-module. By Theorem 9.3.8, for each $P \in \operatorname{Assoc}_R(M)$ there is a P-primary submodule $Y(P)$ of A such that $(0) = \bigcap_{P \in \operatorname{Assoc}_R(A)} Y(P)$. Then the sequence of R-modules

$$0 \to A \to \bigoplus_{P \in \operatorname{Assoc}_R(A)} A/Y(P)$$

is exact. Since B is R-flat,

$$0 \to A \otimes_R B \to \bigoplus_{P \in \operatorname{Assoc}_R(A)} A/Y(P) \otimes_R B$$

is an exact sequence of S-modules. By Case 1, $\operatorname{Assoc}_S(A/Y(P) \otimes_R B) = \operatorname{Assoc}_S(B/PB)$. Applying Proposition 9.2.2 (5),

$$\begin{aligned}
\operatorname{Assoc}_S(A \otimes_R B) &\subseteq \bigcup_{P \in \operatorname{Assoc}_R(A)} \operatorname{Assoc}_S(A/Y(P) \otimes_R B) \\
&\subseteq \bigcup_{P \in \operatorname{Assoc}_R(A)} \operatorname{Assoc}_S(B/PB)
\end{aligned}$$

which proves (2) in this case.

Case 3: Let A be an R-module. Given any $Q \in \operatorname{Assoc}_S(A \otimes_R B)$, there is $z \in A \otimes_R B$ such that $Q = \operatorname{annih}_S(z)$. Write $z = \sum_{i=1}^n a_i \otimes b_i$ for some elements $a_i \in A$ and $b_i \in B$. Let $Z = \sum_{i=1}^n R a_i$ be the R-submodule of A generated by $a_1, \dots, a_n$. Since z is in the S-submodule $Z \otimes_R B$ of $A \otimes_R B$, it follows that $Q \in \operatorname{Assoc}_S(Z \otimes_R B)$. By Case 2, there is $P \in \operatorname{Assoc}_R(Z)$ such that $Q \in \operatorname{Assoc}_S(B/PB)$. Since $\operatorname{Assoc}_R(Z) \subseteq \operatorname{Assoc}_R(A)$, this completes the proof. $\square$

The following corollary of Theorem 9.3.10 is a generalization of Lemma 9.2.5.

COROLLARY 9.3.11. *Let $f : R \to S$ be a homomorphism of commutative noetherian rings and assume S is flat as an R-module. Then the following are true.*

(1) $\operatorname{Assoc}_S(S) = \bigcup_{P \in \operatorname{Assoc}_R(R)} \operatorname{Assoc}_S(S/PS)$
(2) $f^\sharp(\operatorname{Assoc}_S(S)) = \{P \in \operatorname{Assoc}_R(R) \mid S \neq PS\}$.
(3) If S is faithfully flat over R, then $f^\sharp(\operatorname{Assoc}_S(S)) = \operatorname{Assoc}_R(R)$.

4. Zariski's Main Theorem

Throughout this section all rings are commutative. Let B be a finitely generated commutative A-algebra with structure homomorphism $f : A \to B$. If $p \in \operatorname{Spec} A$ and $k_p = A_p/pA_p$ is the residue field at p, then the fiber over p of f is $B \otimes_A k_p$. If $B \otimes_A k_p$ is finite dimensional over k_p for all $p \in \operatorname{Spec} A$, then we say B is quasi-finite over A (see Definition 9.4.4). As we see in Proposition 9.4.3 below, this is equivalent to the property that for every $p \in \operatorname{Spec} A$, the fiber $\operatorname{Spec}(B \otimes_A k_p)$ is a discrete set. While the thrust of Zariski's Main Theorem itself can be somewhat difficult for one to grasp on first encounter, there is one important application that can be readily stated here. In Corollary 9.4.16 we show that if B is a quasi-finite A-algebra, then there is an A-subalgebra R of B such that R is finitely generated as an A-module and $\operatorname{Spec} B \to \operatorname{Spec} R$ is an open immersion (see Exercise 3.5.18). In other words, this says that a quasi-finite morphism $f^\sharp : \operatorname{Spec} B \to \operatorname{Spec} A$ factors into an open immersion $\operatorname{Spec} B \to \operatorname{Spec} R$ followed by a finite morphism $\operatorname{Spec} R \to \operatorname{Spec} A$. The proof we give is from [**48**, Chapter IV].

4.1. Quasi-finite Algebras.

PROPOSITION 9.4.1. *Let k be a field, B a finitely generated commutative k-algebra, and $q \in \operatorname{Spec} B$. The following are equivalent.*

(1) q is an isolated point in $\operatorname{Spec} B$*.*
(2) B_q is a finite dimensional k-algebra.

PROOF. (1) implies (2): If the point q is isolated in the Zariski topology, then it is an open set. There exists $f \in B$ such that $q = \operatorname{Spec} B - V(f) = \operatorname{Spec} B_f$. Since B_f is noetherian and has only one prime ideal, B_f is artinian by Proposition 4.5.4. Since B_f has only one prime ideal, B_f is local with maximal ideal qB_f. By Exercise 6.2.5, B_f is finite dimensional over k. Since B_f is local, $B_f = (B_f)_q = B_q$, which shows B_q is finite dimensional over k.

(2) implies (1): Suppose B_q is finite dimensional over k. Let K and C be the kernel and cokernel of the localization map $B \to B_q$. Consider the sequence of B-modules

$$0 \to K \to B \to B_q \to C \to 0.$$

Then $K_q = C_q = 0$. Since B is noetherian, K is finitely generated over B. Since B_q is finite dimensional over k, C is finite dimensional over k hence finitely generated over B. By Lemma 3.1.10, there exists $f \in B - q$ such that $K_f = C_f = 0$. Therefore $B_f = B_q$. But B_q is local and finite dimensional over k, hence is artinian. So $\operatorname{Spec} B_q = q = \operatorname{Spec} B_f$. So q is isolated. □

PROPOSITION 9.4.2. *Let B be a finitely generated commutative A-algebra, $q \in \operatorname{Spec} B$, and $p = q \cap A$. The following are equivalent.*

(1) q is an isolated point in the fiber $\operatorname{Spec}(B \otimes_A k_p) = \operatorname{Spec}(B \otimes_A (A_p/pA_p))$.
(2) B_q/pB_q is finite dimensional over k_p.

PROOF. By k_p we denote the residue field of A at the prime p. That is, $k_p = A_p/pA_p$. Then $B \otimes_A k_p = B \otimes_A A_p \otimes_{A_p} k_p = B_p \otimes_{A_p} k_p$. Also, $B_q = (B_p)_q$, from which we get $B_q/pB_q = (B_p)_q/p(B_p)_q$. It is enough to prove the proposition when A is a local ring with maximal ideal p. In this case, $B/pB = B \otimes_A k_p$ is a finitely generated algebra over the field $A/p = k_p$ and $(B/pB)_q = B_q/pB_q$. Apply Proposition 9.4.1 to the algebra B/pB over k_p. $\square$

If A and B are as in Proposition 9.4.2 and either (1) or (2) is satisfied, then we say B is *quasi-finite* over A at q.

PROPOSITION 9.4.3. *Let B be a finitely generated commutative A-algebra. The following are equivalent.*

(1) B is quasi-finite over A for all $q \in \operatorname{Spec} B$.
(2) For all $p \in \operatorname{Spec} A$, $B \otimes_A k_p$ is a finite dimensional k_p-algebra.

PROOF. It is enough to prove the proposition when $A = k$ is a field. Assume that B is a finitely generated k-algebra.

(2) implies (1): Assume B is a finite dimensional k-algebra. Therefore, B is artinian (Exercise 4.1.13) and semilocal (Proposition 4.5.3). By Theorem 4.5.6, the natural homomorphism $B \to \bigoplus B_q$ is an isomorphism, where q runs through the finite set $\operatorname{Spec} B$. Each B_q is finite dimensional over k. By Proposition 9.4.1, each q is isolated in $\operatorname{Spec} B$.

(1) implies (2): For each $q \in \operatorname{Spec} B$, q is isolated. So $\operatorname{Spec} B$ is a disjoint union $\cup_{q \in \operatorname{Spec} B} \operatorname{Spec} B_{f(q)}$, where $\operatorname{Spec} B_{f(q)} = q$. Only finitely many of the $f(q)$ are required to generate the unit ideal, so the union is finite. Therefore B is a finite direct sum of the local rings $B_{f(q)} = B_q$. Each B_q is finite dimensional over k, by Proposition 9.4.1. Therefore B is finite dimensional over k. $\square$

DEFINITION 9.4.4. Let B be a commutative finitely generated A-algebra. If either Part (1) or (2) of Proposition 9.4.3 is satisfied, then we say B is *quasi-finite* over A.

LEMMA 9.4.5. *Let $A \subseteq C \subseteq B$ be three rings. Assume B is finitely generated over A and $q \in \operatorname{Spec} B$. If B is quasi-finite over A at q, then B is quasi-finite over C at q.*

PROOF. Let $p = q \cap A$ and $r = q \cap C$. The fiber over r is a subset of the fiber over p. If q is isolated in the fiber over p, then q is isolated in the fiber over r. $\square$

EXAMPLE 9.4.6. (1) If B is a commutative A-algebra that is finitely generated as an A-module, then B is quasi-finite over A (Exercise 9.4.4).

(2) Let A be a commutative ring, $f \in A$, and $B = A_f$. If $q \in \operatorname{Spec} B$, and $p = q \cap A$, then $B_q = A_p$. Therefore, A_f is quasi-finite over A.

4.2. Zariski's Main Theorem.

LEMMA 9.4.7. *Let $A \subseteq B$ be commutative rings, $q \in \operatorname{Spec} B$ and $p = q \cap A$. Assume*

(1) A is integrally closed in B,
(2) $B = A[x]$ is generated by one element as an A-algebra, and
(3) B is quasi-finite over A at q.

Then $B_p = A_p$.

PROOF. The first step is to reduce to the case where A is a local ring with maximal ideal p. Clearly $B_p = A[x] \otimes_A A_p$ is finitely generated over A_p and B_p is quasi-finite over A_p. Let us check that A_p is integrally closed in B_p. Let $b \in B$ and $f \in A - p$ and assume b/f is integral over A_p. Then

$$\frac{b^n}{f^n} + \frac{a_{n-1}}{y_{n-1}} \frac{b^{n-1}}{f^{n-1}} + \cdots + \frac{a_0}{y_0} = 0$$

for some $a_i \in A$ and $y_i \in A - p$. Multiply both sides by f^n to get

$$b^n + \frac{fa_{n-1}}{y_{n-1}} b^{n-1} + \cdots + \frac{f^n a_0}{y_0}.$$

Let $y = y_0 \cdots y_{n-1}$ and multiply both sides by y^n to get

$$y^n b^n + \frac{fya_{n-1}}{y_{n-1}} y^{n-1} b^{n-1} + \cdots + \frac{f^n y^n a_0}{y_0} = 0$$
$$(yb)^n + \alpha_{n-1}(yb)^{n-1} + \cdots + \alpha_0 = 0$$

for some $\alpha_i \in A$. So yb is integral over A, hence $b \in A_p$.

From now on we assume

(1) A is integrally closed in B,
(2) $B = A[x]$,
(3) A is local with maximal ideal p, and if $q \in \operatorname{Spec} B$ lies over p, then B is quasi-finite over A at q.

Out goal is to prove that $A = B$. It is enough to show that x is integral over A. Let $k = A/p$. Since B is quasi-finite over A at q, $B/pB = A[x] \otimes_A k = k[\bar{x}]$ is the fiber over p and q is isolated in $\operatorname{Spec} k[\bar{x}]$. Throughout the rest of the proof, if $b \in B$, then the image of b in B/pB will be denoted by $\bar{b}$. By Exercise 9.4.3, $\bar{x}$ is algebraic over k. There exists a monic polynomial $f(t) \in A[t]$ of degree greater than or equal to one, such that $\bar{f}(\bar{x}) = 0$ in $k[\bar{x}]$. That is, $f(x) \in pB$. Let $y = 1 + f(x)$. We have the inclusion relations $A \subseteq A[y] \subseteq A[x]$ and because x is integral over $A[y]$, the map $\operatorname{Spec} k[x] \to \operatorname{Spec} k[y]$ is onto by Theorem 6.3.6. Let $\bar{y}$ denote the image of y in $k[y] \otimes_A k = k[\bar{y}]$. Under the map $k[\bar{y}] \to k[\bar{x}]$, the image of $\bar{y}$ is 1. Because $\bar{y}$ generates the unit ideal of $k[\bar{x}]$, we see that $\bar{y}$ does not belong to any prime ideal of $k[\bar{y}]$. Therefore, $\bar{y}$ is a unit of $k[\bar{y}]$. Since $\operatorname{Spec} k[\bar{x}]$ is finite, it follows that $\operatorname{Spec} k[\bar{y}]$ is finite. That is to say, $k[\bar{y}]$ is finite dimensional over k.

Now we show that $y \in A$. Since $\bar{y}$ is algebraic over k, there exist $a_i \in A$ such that

$$\bar{y}^n + \bar{a}_{n-1}\bar{y}^{n-1} + \cdots + \bar{a}_0 = 0$$

where $n \geq 1$ and $\bar{a}_0 \neq 0$. Therefore

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 \in pA[y],$$

which says there exist $b_i \in p$ such that

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = b_m y^m + \cdots + b_1 y + b_0.$$

After adding some zero terms we can suppose $m = n$. Subtracting,

$$(a_m - b_m)y^m + \cdots + (a_1 - b_1)y + (a_0 - b_0) = 0.$$

But A is local and a_0 is not in p, so $a_0 - b_0$ is a unit. There exist $c_i \in A$ such that

$$1 + (c_0 + c_1 y + \cdots + c_{m-1}y^{m-1})y = 0$$

which shows y is invertible in $A[y]$. The last equation yields

$$y^{-1} + c_0 + (c_1 + \cdots + c_{m-1}y^{m-2})y = 0$$

and

$$y^{-2} + c_0 y^{-1} + c_1(c_2 + \cdots + c_{m-1}y^{m-3})y = 0.$$

Iterating we get

$$y^{-m} + c_0 y^{1-m} + \cdots + c_{m-2}y^{-1} + c_{m-1} = 0$$

which shows that y^{-1} is integral over A. Since A is integrally closed in B, $y^{-1} \in A$. Since y^{-1} is invertible in B, y^{-1} is not in q. Therefore, y^{-1} is not in $p = q \cap A$. Thus y^{-1} is invertible in A and y is in A. We have $A = A[y] \subseteq A[x] = B$ and x is integral over A. So $A = B$. $\square$

LEMMA 9.4.8. *Assume B is an integral domain which is an integral extension of the polynomial ring $A[T]$. Let q be a prime ideal of B. Then B is not quasi-finite over A at q.*

PROOF. Let $p = q \cap A$ and $k_p = A_p/pA_p$ the residue field. Choose q to be maximal among all primes lying over p. We will show q is not minimal, which will prove that q is not isolated in the fiber $B \otimes_A k_p$, hence B is not quasi-finite over A at q.

Assume A is integrally closed in its quotient field. Let $r = q \cap A[T]$. Since B is integral over $A[T]$, Theorem 6.3.6 (3) says that r is maximal among the set of prime ideals of $A[T]$ lying over p. That is, $r \otimes_A k_p$ is a maximal ideal of $A[T] \otimes_A k_p = k_p[T]$. This says r properly contains the prime ideal $pA[T]$. By Theorem 6.3.6 (5), there is a prime ideal $q_1 \in \operatorname{Spec} B$ such that $q_1 \subsetneq q$ and $q_1 \cap A[T] = pA[T]$. This proves q is not a minimal prime lying over p.

For the general case, let $\tilde{A}$ be the integral closure of A in its field of quotients and $\tilde{B}$ the integral closure of B in its field of quotients. Then $\tilde{B}$ is integral over $\tilde{A}[T]$. Let $\tilde{q}$ be a prime ideal of $\tilde{B}$ lying over q. Let $\tilde{p} = \tilde{q} \cap \tilde{A}$. By Theorem 6.3.6 (2), $\tilde{q}$ is maximal among primes lying over $\tilde{p}$. By the previous paragraph, there is $\tilde{q}_1$ in $\operatorname{Spec} \tilde{B}$ such that $\tilde{q}_1 \subsetneq \tilde{q}$ and $\tilde{q}_1$ lies over $\tilde{p}$. By Theorem 6.3.6 (2), $\tilde{q}_1 \cap B \subsetneq q$ so q is not a minimal prime lying over p. $\square$

LEMMA 9.4.9. *Let $A \subseteq A[x] \subseteq B$ be three rings such that*

(1) B is integral over $A[x]$,
(2) A is integrally closed in B, and
(3) there exists a monic polynomial $F(T) \in A[T]$ such that $F(x)B \subseteq A[x]$. That is, $F(x)$ is in the conductor from B to $A[x]$ (see Exercise 1.1.8).

Then $A[x] = B$.

PROOF. Let $b \in B$. Our goal is to show $b \in A[x]$. We are given that $F(x)b \in A[x]$, so $F(x)b = G(x)$ for some $G(T) \in A[T]$. Since F is monic, we can divide F into G. There exist $Q(T), R(T) \in A[T]$ such that $G(T) = F(T)Q(T) + R(T)$ and $0 \le \deg R < \deg F$. Note that $G(x) = F(x)b = Q(x)F(x) + R(x)$, hence $(b - Q(x))F(x) = R(x)$. Set $y = b - Q(x)$. It is enough to show that $y \in A[x]$.

Let $\theta : B \to B[y^{-1}]$ be the localization of B. Let $\bar{A}$, $\bar{y}$, $\bar{x}$, etc. denote the images of A, y, x, etc. under θ. Then $yF(x) = R(x)$ implies that $\bar{F}(\bar{x}) = y^{-1}\bar{R}(\bar{x})$ in $B[y^{-1}]$. Since $\deg R < \deg F$, this implies that $\bar{x}$ is integral over $\bar{A}[y^{-1}]$. But $y \in B$, so y is integral over $A[x]$. Hence $\bar{y}$ is integral over $\bar{A}[\bar{x}]$. Since integral over integral is integral, $\bar{y}$ is integral over $\bar{A}[y^{-1}]$. There exists $P(T) \in \bar{A}[y^{-1}][T]$ such that $(\bar{y})^n + P(\bar{y}) = 0$ and $\deg P(T) < n$. By clearing denominators, we see that for some $m > 0$, $(\bar{y})^{n+m} + (\bar{y})^m P(\bar{y}) = 0$ is a monic polynomial equation in $\bar{y}$ over $\bar{A}$. Therefore, $\bar{y}$ is integral over $\bar{A}$ and there exists a monic polynomial $\bar{H}(T) \in \bar{A}[T]$ such that $\bar{H}(\bar{y}) = 0$. Let $H \in A[T]$ be a monic polynomial such that $\theta(H(T)) = \bar{H}(T)$. Since $\theta(H(y)) = 0$ in $B[y^{-1}]$, there exists $u > 0$ such that $y^u H(y) = 0$ in B. This shows that y is integral over A, hence $y \in A$. $\square$

LEMMA 9.4.10. *Let $A \subseteq R \subseteq B$ be three rings and $p \in \operatorname{Spec} A$. Assume*

(1) B is a finitely generated R-module,
(2) c is the conductor from B to R, and
(3) c' is the conductor from B_p to R_p.

Then $c' = c_p$.

PROOF. Let $\alpha/\beta \in c_p$, where $\alpha \in c$, $\beta \in A - p$. Then

$$(\alpha/\beta)B_p \subseteq (\alpha B)_p \subseteq R_p$$

shows that $\alpha/\beta \in c'$.

Let $\alpha/\beta \in c'$ where $\alpha \in R$ and $\beta \in A - p$. If $b \in B$ and $z \in A - p$, then

$$(\alpha/1)(b/z) = (\alpha/\beta)((\beta b)/z) \in R_p$$

So $\alpha/1 \in c'$. Let $b_1, \dots, b_n$ be a generating set for B over R. Then $(\alpha/1)(b_i/1) \in R_p$ so there exists $x_i \in A - p$ such that $\alpha b_i x_i \in R$. Therefore $\alpha x_1 \cdots x_n \in c$ and since $\beta x_1 \cdots x_n \in A - p$ it follows that $\alpha/\beta \in c_p$. $\square$

LEMMA 9.4.11. *Let $A \subseteq A[x] \subseteq B$ be three rings, $q \in \operatorname{Spec} B$ and $p = q \cap A$. Assume*

(1) B is finitely generated as a module over $A[x]$,
(2) A is integrally closed in B, and
(3) B is quasi-finite over A at q.

Then $A_p = B_p$.

PROOF. Let

$$c = \{\alpha \in A[x] \mid \alpha B \subseteq A[x]\}$$

be the conductor from B to $A[x]$.

Case 1: $c \not\subseteq q$. Let $r = q \cap A[x]$. There exists $\alpha \in c - r$, hence $A[x]_r = B \otimes_{A[x]} A[x]_r = B_r$. It follows that B_r is a local ring and $B_r = B_q$. Since $r \cap A = q \cap A = p$, and B is quasi-finite over A at q, we have

$$B_q/pB_q = A[x]_r/pA[x]_r$$

is finite dimensional over k_p. This says $A[x]$ is quasi-finite over A at r. Apply Lemma 9.4.7 to get $A[x]_p = A_p$. But B is finitely generated as a module over $A[x]$, so B_p is finitely generated over $A_p = A[x]_p$. Since A is integrally closed in B, A_p is integrally closed in B_p and $A_p = B_p$.

Case 2: $c \subseteq q$. Let n be a minimal element of the set $\{z \in \operatorname{Spec} B \mid c \subseteq z \subseteq q\}$ and let $m = n \cap A$. First we show that the image of x in the residue field $k_n = B_n/nB_n$ is transcendental over the subfield $k_m = A_m/mA_m$. To prove this, it is enough to assume A is local with maximal ideal m. Lemma 9.4.10 says the conductor c is preserved under this localization step. Suppose that image of x in k_n is algebraic over $k_m = A/m$. Then $n \cap A[x]$ is a prime ideal, so the integral domain $A[x]/(n \cap A[x])$ is a finite integral extension of the field $k_m = A/m$. Therefore, $A[x]/(n \cap A[x])$ is a field so $n \cap A[x]$ is a maximal ideal. Since B is integral over $A[x]$, by Theorem 6.3.6, it follows that n is a maximal ideal of B and $B/n = k_n$. By assumption, there exists a monic polynomial $F(T) \in A[T]$ such that $F(x) \in n$. But n is minimal with respect to prime ideals of B containing c. In B_n, nB_n is the only prime ideal containing c_n and the radical of c_n is equal to nB_n. Let $\bar{F}(\bar{x})$ denote the image of $F(x)$ in B_n. There exists $\nu > 0$ such that $(\bar{F}(\bar{x}))^\nu \in c_n$. There exists $y \in B - n$ such that $y(F(x))^\nu \in c$. This implies $y(F(x))^\nu B \subseteq A[x]$. Let $B' = A[x][yB]$. Clearly $F(x)^\nu$ is in the conductor from B' to $A[x]$. Apply Lemma 9.4.9 to $A \subseteq A[x] \subseteq B'$ with the monic polynomial F^ν. Then $A[x] = B'$ which implies $yB \subseteq A[x]$. This says $y \in c \subseteq n$, which contradicts the choice of y.

For the rest of the proof, let $\bar{B} = B/n$ and $\bar{A} = A/m$ and assume the image $\bar{x}$ of x in $\bar{B}$ is transcendental over $\bar{A}$. We have $\bar{A} \subseteq \bar{A}[\bar{x}] \subseteq \bar{B}$. Let $\bar{q}$ denote the image of q in $\bar{B}$. Since B is quasi-finite over A at q, it follows that $\bar{B}$ is quasi-finite over $\bar{A}$ at $\bar{q}$. This contradicts Lemma 9.4.8, so Case 2 cannot occur. $\square$

PROPOSITION 9.4.12. *Let $A \subseteq C \subseteq B$ be three commutative rings, $q \in \operatorname{Spec} B$ and $p = q \cap A$. Assume*

(1) C is finitely generated as an A-algebra,
(2) B is finitely generated as a C-module,
(3) A is integrally closed in B, and
(4) B is quasi-finite over A at q.

Then $B_p = A_p$.

PROOF. Proceed by induction on the number n of generators for the A-algebra C. If $n = 0$, then B is integral over A and by assumption, $A = B$.

Assume $n > 0$ and suppose the proposition is true when C is generated by $n-1$ elements over A. Let $C = A[x_1,\dots,x_n]$. Let $\tilde{A}$ be the integral closure of $R = A[x_1,\dots,x_{n-1}]$ in B. Then B is finitely generated as a module over $\tilde{A}[x_n]$ and $\tilde{A} \subseteq \tilde{A}[x_n] \subseteq B$. Since B is quasi-finite over A at q, by Lemma 9.4.5, B is quasi-finite over $\tilde{A}$ at q. We are in the setting of Lemma 9.4.11, so if $\tilde{p} = q \cap \tilde{A}$, then $\tilde{A}_{\tilde{p}} = B_{\tilde{p}}$.

Since $\tilde{A}$ is integral over $R = A[x_1,\dots,x_{n-1}]$, $\tilde{A}$ is the direct limit $\tilde{A} = \varinjlim_\alpha A_\alpha$ over all subalgebras A_α where $R \subseteq A_\alpha \subseteq \tilde{A}$ and A_α is finitely generated as a module over R. For any such A_α, let $p_\alpha = q \cap A_\alpha = \tilde{p} \cap A_\alpha$.

Let $r = q \cap R$. Since B is finitely generated as an R-algebra, $B_{\tilde{p}} = \tilde{A}_{\tilde{p}}$ is finitely generated as an R_r-algebra. Pick a generating set $z_1/y_1,\dots,z_m/y_m$ for the R_r-algebra $\tilde{A}_{\tilde{p}}$ where $z_i \in \tilde{A}$ and $y_i \in \tilde{A} - \tilde{p}$. Since $\tilde{A}$ is integral over R, it follows that $A_1 = R[z_1,\dots,z_m,y_1,\dots,y_m]$ is finitely generated as a module over R. Let $p_1 = q \cap A_1$. For each i, we have $z_i/y_i \in (A_1)_{p_1}$ so the natural map $(A_1)_{p_1} \to \tilde{A}_{\tilde{p}} = B_{\tilde{p}}$ is an isomorphism. Therefore, $(A_1)_{p_1} \cong \tilde{A}_{\tilde{p}} = B_{\tilde{p}} = B_q$. By the induction hypothesis applied to $A \subseteq R \subseteq A_1$, we have $A_p = (A_1)_p = (A_1)_{p_1}$. This shows $A_p = B_p$. $\square$

THEOREM 9.4.13. *(Zariski's Main Theorem) Let B be a finitely generated commutative A-algebra, $\tilde{A}$ the integral closure of A in B and $q \in \operatorname{Spec} B$. If B is quasi-finite over A at q, then there exists $f \in \tilde{A}$ such that $f \notin q$ and $\tilde{A}_f = B_f$.*

PROOF. By Lemma 9.4.5, B is quasi-finite over $\tilde{A}$ at q. Let $\tilde{p} = q \cap \tilde{A}$. By Proposition 9.4.12, $\tilde{A}_{\tilde{p}} = B_{\tilde{p}}$. Let $b_1,\dots,b_n$ be a generating set for the $\tilde{A}$-algebra B. For each i there exists $a_i/x_i \in \tilde{A}_{\tilde{p}}$ such that $a_i/x_i = b_i/1$ in $B_{\tilde{p}}$. Let $f = x_1 \cdots x_n$. Then $f \in \tilde{A} - \tilde{p}$. The inclusion $\tilde{A}_f \subseteq B_f$ is an equality. $\square$

COROLLARY 9.4.14. *Let A be a ring, B a finitely generated commutative A-algebra. The set of all q in $\operatorname{Spec} B$ such that B is quasi-finite over A at q is an open subset of $\operatorname{Spec} B$.*

PROOF. Let $q \in \operatorname{Spec} B$ and assume B is quasi-finite over A at q. Let $\tilde{A}$ be the integral closure of A in B. By Theorem 9.4.13 (Zariski's Main Theorem), there exists $f \in \tilde{A} - q$ such that $\tilde{A}_f = B_f$. Since $\tilde{A}$ is integral over A, we can write $\tilde{A}$ as the direct limit of all subalgebras A_α such that $f \in A_\alpha$ and A_α is finitely generated as a module over A. Therefore

$$\tilde{A} = \varinjlim A_\alpha$$

which implies

$$B_f = \tilde{A}_f = \left(\varinjlim A_\alpha\right)_f = \varinjlim (A_\alpha)_f.$$

But B is finitely generated as an A-algebra, hence B_f is too. Let $a_1/f^\nu,\dots,a_m/f^\nu$ be a set of generators of $\tilde{A}_f$ over A. For some α, $\{a_1,\dots,a_m\} \subseteq A_\alpha$. It follows that $B_f = (A_\alpha)_f$ for this α. By Example 9.4.6, $(A_\alpha)_f$ is quasi-finite over A. The open set $V = \operatorname{Spec} B_f$ is a neighborhood of q. $\square$

EXAMPLE 9.4.15. Let $A \to B \to C$ be homomorphisms of rings. Assume B is finitely generated as an A-module, C is finitely generated as a B-algebra and $\operatorname{Spec} C \to \operatorname{Spec} B$ is an open immersion (Exercise 3.5.18). Then C is quasi-finite over A. The next corollary says every quasi-finite homomorphism factors in this way.

COROLLARY 9.4.16. *Let B be a commutative A-algebra which is finitely generated as an A-algebra and which is quasi-finite over A. If $\tilde{A}$ is the integral closure of A in B, then*

(1) $\operatorname{Spec} B \to \operatorname{Spec} \tilde{A}$ *is an open immersion and*
(2) there exists an A-subalgebra R of $\tilde{A}$ such that R is finitely generated as an A-module and $\operatorname{Spec} B \to \operatorname{Spec} R$ *is an open immersion.*

PROOF. By Corollary 9.4.14 there are a finite number of $f_i \in \tilde{A}$ such that $B_{f_i} \cong \tilde{A}_{f_i}$ and $\{f_i\}$ generate the unit ideal of B. The open sets $U_i = \operatorname{Spec} B_{f_i}$ are an open cover of $\operatorname{Spec} B$, so $\operatorname{Spec} B \to \operatorname{Spec} \tilde{A}$ is an open immersion. By the argument of Corollary 9.4.14, the finite set $\{f_i\}$ of elements in $\tilde{A}$ belongs to a subalgebra $R \subseteq \tilde{A}$ such that R is finitely generated as a module over A and $R_{f_i} \cong B_{f_i}$ for each i. Therefore $\operatorname{Spec} B \to \operatorname{Spec} R$ is an open immersion. $\square$

4.3. Exercises.

EXERCISE 9.4.1. (Quasi-finite over quasi-finite is quasi-finite) If B is quasi-finite over A, and C is quasi-finite over B, then C is quasi-finite over A.

EXERCISE 9.4.2. If S is a commutative finitely generated separable R-algebra, then S is quasi-finite over R.

EXERCISE 9.4.3. Show that if k is a field and x an indeterminate, then $\operatorname{Spec} k[x]$ has no isolated point. (Hint: Show that $\operatorname{Spec} k[x]$ is infinite and that a proper closed subset is finite.)

EXERCISE 9.4.4. Let B be a commutative A-algebra. Prove that if B is finitely generated as an A-module, then B is quasi-finite over A.

5. Graded Rings and Modules

Throughout this section all rings are commutative. We refer the reader to Section 7.2 for the definitions of graded rings and modules. A graded version of the Primary Decomposition Theorem is proved in Theorem 9.5.6. Numerical polynomials are defined and their fundamental properties are derived in Section 9.5.2. Theorem 9.5.13 states sufficient conditions on a graded module for the existence of the Hilbert polynomial. General references for this section are [**28**, Section I.7] and [**41**, § 10].

5.1. Associated Prime Ideals of a Graded Module.

LEMMA 9.5.1. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a graded ring and $M = \oplus_{n \in \mathbb{Z}} M_n$ a graded R-module. If N is an R-submodule of M, then the following are equivalent.*

(1) $N = \bigoplus_{n \in \mathbb{Z}} (N \cap M_n)$
(2) N is generated by homogeneous elements.
(3) if $x = x_p + x_{p+1} + \cdots + x_{p+m}$ is in N where each x_i is in M_i, then each x_i is in N.

PROOF. Is left to the reader. $\square$

If N satisfies the equivalent properties of Lemma 9.5.1, then we say N is a *graded submodule* of M. A *homogeneous ideal* of R is an ideal which is a graded submodule of the free R-module R.

LEMMA 9.5.2. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a graded ring and I a homogeneous ideal in R.*

(1) *I is a prime ideal if and only if for all homogeneous $a, b \in R^h$, if $ab \in I$, then $a \in I$, or $b \in I$.*
(2) *$\operatorname{Rad}(I)$ is a homogeneous ideal.*
(3) *If $\{I_j \mid j \in J\}$ is a family of homogeneous ideals in R, then $\sum_{j \in J} I_j$ and $\bigcap_{j \in J} I_j$ are homogeneous ideals.*
(4) *If $\mathfrak{p}$ is a prime ideal in R and $\mathfrak{q}$ is the ideal generated by the homogeneous elements in $\mathfrak{p}$, then $\mathfrak{q}$ is a prime ideal.*

PROOF. (1): Suppose $x = \sum_{i=0}^{p} x_i$ and $y = \sum_{j=0}^{q} y_j$ are in R and $xy \in I$ and $y \notin I$. Prove that $x \in I$. Suppose $y_m \notin I$ and that $y_j \in I$ for all $j > m$. The homogeneous component of xy in degree $p+m$ is $z_{p+m} = x_p y_m + \sum_{i=1}^{p} x_{p-i} y_{m+i}$. Therefore, $x_p y_m = z_{p+m} - \sum_{i=1}^{p} x_{p-i} y_{m+i} \in I$ and by hypothesis we get $x_p \in I$. Subtract to get $(x - x_p)y \in I$. Descending induction on p shows $x_i \in I$ for each $i \geq 0$.

(2): Suppose $x = \sum_{i=0}^{p} x_i \in \operatorname{Rad}(I)$. For some $n > 0$, $x^n \in I$. The homogeneous component of x^n of degree np is x_p^n, which is in I because I is homogeneous. This implies $x_p \in \operatorname{Rad}(I)$. Subtract to get $x - x_p \in \operatorname{Rad}(I)$. Descending induction on p shows $x_i \in \operatorname{Rad}(I)$ for each $i \geq 0$.

(3) and (4): Are left to the reader. $\square$

LEMMA 9.5.3. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a noetherian graded ring and $M = \oplus_{n \in \mathbb{Z}} M_n$ a graded R-module.*

(1) *$\operatorname{annih}_R(M)$ is a homogeneous ideal.*
(2) *If P is a maximal member of the set of ideals $\mathscr{C} = \{\operatorname{annih}_R(x) \mid x \in M^h - (0)\}$, then P is an associated prime of M.*
(3) *If P is an associated prime of M, then*
   (a) *P is a homogeneous ideal,*
   (b) *there exists a homogeneous element $x \in M$ of degree n such that $P = \operatorname{annih}_R(x)$, and*
   (c) *the cyclic submodule Rx is isomorphic to $(R/P)(-n)$.*
(4) *If I is a homogeneous ideal of R and P is a minimal prime over-ideal of I, then P is homogeneous.*

PROOF. (1): Is left to the reader.

(2): Is left to the reader. Mimic the proof of Proposition 9.2.2 (1).

(3): There exists $x = x_p + \cdots + x_{p+q}$ in M such that $P = \operatorname{annih}_R(x)$ and each x_i is homogeneous of degree i. Let f be an arbitrary element of P and write f in terms of its homogeneous components, $f = f_0 + \cdots + f_r$. The idea is to show each f_i is in P and apply Lemma 9.5.1 (3). Start with

$$\begin{aligned} 0 = fx &= \sum_{i=0}^{r} \sum_{j=0}^{q} f_i x_{p+j} \\ &= \sum_{k=0}^{r+q} \sum_{i+j=k} f_i x_{p+j} \end{aligned}$$

Comparing homogeneous components we get $\sum_{i+j=k} f_i x_{p+j} = 0$ for each $k = 0, \dots, r+q$. For $k = r+q$, this means $f_r x_{p+q} = 0$. For $k = r+q-1$, it means

$$\begin{aligned}
0 &= f_r x_{p+q-1} + f_{r-1} x_{p+q} \\
&= f_r^2 x_{p+q-1} + f_{r-1} f_r x_{p+q} \\
&= f_r^2 x_{p+q-1}.
\end{aligned}$$

Inductively, we see that $0 = f_r x_{p+q} = f_r^2 x_{p+q-1} = \cdots = f_r^j x_{p+q-j+1}$ for any $j \geq 1$. Therefore $f_r^{q+1} x = 0$, which implies $f_r \in P$. By descending induction on r, we see that $f_i \in P$ for each i. This proves P satisfies Lemma 9.5.1 (3), so P is homogeneous.

For (b), suppose we are given a homogeneous element $h \in P^h$, since $0 = hx = hx_p + \cdots + hx_{p+q}$, it follows that $hx_j = 0$ for each x_j. Since P is generated by homogeneous elements, this proves that $P \subseteq \operatorname{annih}(x_j)$ for each j. We have

$$P \subseteq \bigcap_{j=p}^{p+q} \operatorname{annih}(x_j) \subseteq \operatorname{annih}(x) = P.$$

Because P is prime, Lemma 6.3.3 says $P = \operatorname{annih}(x_j)$ for some j.

(c): Assume $x \in M_n$ and $P = \operatorname{annih}(x)$. Then $1 \mapsto x$ defines a function $(R/P)(-n) \to Rx$ which is an isomorphism of graded R-modules.

(4): By Theorem 9.2.7 (4), a minimal prime over-ideal P of an ideal I is an associated prime of R/I. Part (3) (a) says P is homogeneous. $\square$

The next result is the graded counterpart of Theorem 9.2.10.

THEOREM 9.5.4. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a noetherian graded ring and $M = \oplus_{n \in \mathbb{Z}} M_n$ a finitely generated graded R-module.*

(1) There exists a filtration $0 = S_0 \subsetneq S_1 \subsetneq S_2 \subsetneq \cdots \subsetneq S_r = M$ of M by graded submodules, a set of homogeneous prime ideals $P_i \in \operatorname{Spec} R$, and integers n_i such that $S_i/S_{i-1} \cong (R/P_i)(-n_i)$ for $i = 1, \dots, r$.

(2) The filtration in (1) is not unique, but for any such filtration we do have:

(a) If P is a homogeneous prime ideal of R, then

$$P \supseteq \operatorname{annih}_R(M) \Leftrightarrow P \supseteq P_i$$

for some i. In particular, the minimal elements of the set $\{P_1, \dots, P_r\}$ are the minimal prime over-ideals of $\operatorname{annih}_R M$.

(b) For each minimal prime over-ideal P of $\operatorname{annih}_R M$, the number of times which P occurs in the set $\{P_1, \dots, P_r\}$ is equal to the length of M_P over the local ring R_P, hence is independent of the filtration.

PROOF. Assume $M \neq (0)$. By Proposition 9.2.2, $\operatorname{Assoc}(M) \neq \emptyset$. By Lemma 9.5.3 there exists a graded submodule S of M isomorphic to $(R/P)(-n)$ for some homogeneous prime P and some integer n. Define $\mathscr{C}$ to be the set of all graded submodules $S \subseteq M$ such that S has the kind of filtration specified in Part (1). Since $\mathscr{C}$ is nonempty and M is a finitely generated module over the noetherian ring R, $\mathscr{C}$ has a maximal member, say N. If $N \neq M$, then by Proposition 9.2.2, $\operatorname{Assoc}(M/N) \neq \emptyset$. By Lemma 9.5.3 applied to M/N there is a graded submodule S of M such that $N \subsetneq S \subseteq M$ and $S/N \cong (R/P)(-n)$ for some homogeneous prime P and integer n. Therefore, $S \in \mathscr{C}$. But N is maximal in $\mathscr{C}$, which is a contradiction. This proves Part (1).

(2) We have $\operatorname{annih}\big(S_i/S_{i-1}\big) = \operatorname{annih}\big((R/P_i)(-n_i)\big) = P_i$. Because $S_0 = (0)$, $x \in \prod_{i=1}^{r} P_i$ implies $x \in \operatorname{annih}(M)$. Thus $\prod_{i=1}^{r} P_i \subseteq \operatorname{annih}(M)$. If $x \in \operatorname{annih}(M)$, then $x \in$

$\bigcap_{i=1}^r P_i$. Therefore $\operatorname{annih}(M) \subseteq \bigcap_{i=1}^r \mathfrak{p}_i$. Let P be a homogeneous prime ideal in R. If $P \supseteq \operatorname{annih}(M)$, then we have $P \supseteq \prod_{i=1}^r P_i$. By Proposition 1.5.4, we have $P \supseteq P_i$ for some i. Conversely, if $P \supseteq P_i$ for some i, then $P \supseteq \bigcap_{i=1}^r P_i \supseteq \operatorname{annih}(M)$. This proves (a).

For (b), localize at P. Consider

$$(5.1) \qquad \left(S_i/S_{i-1}\right)_P = \left((R/P_i)(-n_i)\right)_P.$$

If $P = P_i$, then the right-hand side of (5.1) is $(R/P)_P = R_P/PR_P$ which has length one as an R_P-module, since PR_P is the maximal ideal of R_P. Since P is a minimal prime over-ideal of $\operatorname{annih}(M)$, if $P \neq P_i$, then there exists some $x \in P_i$ which is not in P. In this case, the right-hand side of (5.1) is (0). That is, $(S_{i-1})_P = (S_i)_P$. We have shown that M_P has a filtration of length equal to the number of times P occurs in $\{P_1, \dots, P_r\}$. □

DEFINITION 9.5.5. If R is a noetherian graded ring, M is a finitely generated graded R-module, and P is a minimal prime over-ideal of $\operatorname{annih}_R(M)$, then the length of M_P over the local ring R_P is called the *multiplicity* of M at P and is denoted $\mu_P(M)$. In Algebraic Geometry, it plays an important role in the definition of intersection multiplicity of two hypersurfaces along a subvariety.

The next result is the counterpart of Theorem 9.3.8 for a graded ring and module.

THEOREM 9.5.6. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a noetherian graded ring and $M = \oplus_{n\in\mathbb{Z}} M_n$ a graded R-module.*

(1) For each $P \in \operatorname{Assoc}(M)$ there exists a P-primary graded submodule Y_P of M such that $(0) = \bigcap_{P\in\operatorname{Assoc}(M)} Y_P$.
(2) If M is finitely generated and N is a graded submodule of M, then there exists a primary decomposition $N = \bigcap_{P\in\operatorname{Assoc}(M/N)} Y_P$, where Y_P is a P-primary graded submodule of M.

PROOF. Is left to the reader. (Mimic the proof of Theorem 9.3.8, substituting graded submodules.) □

5.2. Numerical Polynomials.

DEFINITION 9.5.7. A *numerical polynomial* is a polynomial $p(x) \in \mathbb{Q}[x]$ with the property that there exists $N > 0$ such that $p(n) \in \mathbb{Z}$ for all integers n greater than N. If r is a nonnegative integer, the *binomial coefficient function* is defined to be

$$\binom{x}{r} = \frac{1}{r!}x(x-1)\cdots(x-r+1)$$

which is clearly a polynomial of degree r in $\mathbb{Q}[x]$. For any polynomial $p \in \mathbb{Q}[x]$, define the *difference polynomial* to be

$$\Delta p(x) = p(x+1) - p(x).$$

LEMMA 9.5.8. *In the context of Definition 9.5.7,*

(1) For any integer x, $\binom{x}{r}$ is an integer.
(2) The binomial coefficient function is a numerical polynomial of degree r.
(3) The set $\{\binom{x}{i} \mid i = 0, \dots, r\}$ is linearly independent over $\mathbb{Q}$.
(4) The set $\{\binom{x}{i} \mid i = 0, \dots, r\}$ is a $\mathbb{Q}$-basis for $\{f \in \mathbb{Q}[x] \mid \deg f \le r\}$.
(5) $\binom{z+1}{r} - \binom{z}{r} = \binom{z}{r-1}$
(6) For all integers $d > 0$, $\binom{z+d}{r} - \binom{z}{r} = \binom{z+d-1}{r-1} + \cdots + \binom{z}{r-1}$.

(7) $\Delta\binom{z}{r} = \binom{z}{r-1}$.

PROOF. Is left to the reader. $\square$

PROPOSITION 9.5.9. *In the context of Definition 9.5.7,*

(1) If $p(x) \in \mathbb{Q}[x]$ is a numerical polynomial, then there exist integers c_i such that

$$p(x) = c_0\binom{x}{r} + c_1\binom{x}{r-1} + \cdots + c_r.$$

In particular, $p(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

(2) If $f : \mathbb{Z} \to \mathbb{Z}$ is any function, and if there exists a numerical polynomial $q(x) \in \mathbb{Q}[x]$ such that the difference function $\Delta f = f(n+1) - f(n)$ is equal to $q(n)$ for all sufficiently large integers n, then there exists a numerical polynomial $p(x)$ such that $f(n) = p(n)$ for all sufficiently large integers n.

PROOF. (1): The proof is by induction on $r = \deg p$. If $r = 0$, then (1) is obvious. Assume $r > 0$ and assume (1) is true for all numerical polynomials of degree less than r. By Lemma 9.5.8 (4), write p as a linear combination of the binomial coefficient functions

$$p(x) = c_0\binom{x}{r} + c_1\binom{x}{r-1} + \cdots + c_r$$

where $c_i \in \mathbb{Q}$. Using Lemma 9.5.8 (5),

$$\Delta p(x) = c_0\binom{x}{r-1} + c_1\binom{x}{r-2} + \cdots + c_{r-1}$$

is a numerical polynomial of degree $r-1$. By the induction hypothesis, and Lemma 9.5.8 (3), it follows that $c_0, \dots, c_{r-1}$ are integers. Since $p(n) \in \mathbb{Z}$ for all sufficiently large integers n, it follows that c_r is an integer.

(2): Applying Part (1) to q,

$$q(x) = c_0\binom{x}{r} + c_1\binom{x}{r-1} + \cdots + c_r$$

for integers c_i. Setting

$$p(x) = c_0\binom{x}{r+1} + c_1\binom{x}{r} + \cdots + c_r\binom{x}{1},$$

we see that $\Delta p = q$. Therefore $\Delta(f - q)(n) = 0$ for all sufficiently large integers n. Hence $(f - p)(n) = c$ is constant for all sufficiently large integers n. Then $f(n) = p(n) + c$ for all sufficiently large n. The desired polynomial is $p(x) + c$. $\square$

5.3. The Hilbert Polynomial.

EXAMPLE 9.5.10. Let A be a commutative artinian ring. By Proposition 4.5.4, A is an A-module of finite length, say $\ell(A)$. If $S = A[x_0, \dots, x_r]$, then S is a graded ring, where $S_0 = A$ and each indeterminate x_i is homogeneous of degree 1. The homogeneous component S_d is a free A-module of rank $\rho(d)$, where $\rho(d)$ is equal to the number of monomials of degree d in the variables $x_0, \dots, x_r$. The reader should verify that $\operatorname{Rank}_A(S_d) = \rho(d) =$

$\binom{r+d}{d} = \binom{r+d}{r}$. By Exercise 4.5.2, the length of the A-module S_d is equal to

$$\begin{aligned}\ell(S_d) &= \rho(d)\ell(A)\\ &= \binom{r+d}{d}\ell(A)\\ &= \frac{(r+d)!}{r!d!}\ell(A)\\ &= \frac{\ell(A)}{r!}(d+r)\cdots(d+1)\end{aligned}$$

which is a numerical polynomial in $\mathbb{Q}[d]$ of degree r and with leading coefficient $\ell(A)/r!$.

EXAMPLE 9.5.11. Let A be a commutative artinian ring and $S = A[x_0, \dots, x_r]$. Let $M = \oplus_{j=0}^{\infty} M_j$ be a finitely generated graded S-module. Then M is generated over S by a finite set of homogeneous elements. Let $\{\xi_1, \dots, \xi_m\} \subseteq M^h$ be a generating set for M and suppose $d_i = \deg(\xi_i)$. Let $S(-d_i)$ be the twisted S-module. The map $\phi_i : S(-d_i) \to M$ defined by $1 \mapsto \xi_i$ is a graded homomorphism of graded S-modules. Let $\phi : \oplus_{i=1}^{m} S(-d_i) \to M$ be the sum map. So ϕ is a graded homomorphism of graded S-modules, and ϕ is onto because the image of ϕ contains a generating set for M. For all $d \geq 0$, there is an exact sequence

$$\bigoplus_{i=1}^{m} S(-d_i)_d \to M_d \to 0.$$

By Proposition 4.1.22, $\ell(M_d) \leq \sum_{i=1}^{m} \ell(S_{d-d_i})$. By Example 9.5.10, it follows that $\ell(M_d)$ is finite.

DEFINITION 9.5.12. Let A be a commutative artinian ring and $S = A[x_0, \dots, x_r]$. Let $M = \oplus_{j=0}^{\infty} M_j$ be a finitely generated graded S-module. The *Hilbert function* of M is defined to be $\varphi_M(d) = \ell(M_d)$. By Example 9.5.11, $\varphi_M(d) \in \mathbb{Z}$ for all d.

THEOREM 9.5.13. *(Hilbert-Serre) Let A be a commutative artinian ring and $S = A[x_0, \dots, x_r]$. Let $M = \oplus_{j=0}^{\infty} M_j$ be a finitely generated graded S-module. There exists a unique numerical polynomial $P_M(z) \in \mathbb{Q}[z]$ such that $\varphi_M(d) = P_M(d)$ for all sufficiently large integers d. The polynomial P_M is called the* Hilbert polynomial *of M.*

PROOF. A polynomial in $\mathbb{Q}[z]$ is determined by its values on a finite set, so $P_M(z)$ is clearly unique, if it exists. Since A is noetherian, so is S.

Step 1: If $S = S_0 = A$, is concentrated in degree 0, then since M is finitely generated it follows that $M_d = 0$ for all sufficiently large d. The polynomial is $P_M(z) = 0$. Proceed by induction on the number $r+1$ of generators for S over $S_0 = A$. Assume $r \geq 0$.

Step 2: For any short exact sequence of graded S-modules

$$0 \to J \to K \to L \to 0$$

Proposition 4.1.22 implies $\varphi_K = \varphi_J + \varphi_L$. If the Theorem is true for the S-modules J and L, then it is true for K. By Theorem 9.5.4 there is a filtration of M by graded submodules such that the consecutive factors are isomorphic to graded S modules of the form $(S/P)(-d)$, where P is a homogeneous prime ideal of S, and d is an integer. The twist corresponds to a change of variables $z \mapsto z - d$ on the Hilbert polynomials, so it suffices to prove the Theorem for S-modules of the form $M = S/P$. Assume that $M = S/P$, where P is a homogeneous prime ideal in the graded ring $S = A[x_0, \dots, x_r]$.

Step 3: Assume P contains the exceptional ideal $(x_0, \dots, x_r)$. Then $M = S/P$ is concentrated in degree 0, so $\varphi_M(d) = \ell(M_d) = 0$ for all $d > 0$. The desired polynomial is $P_M(z) = 0$.

Step 4: Assume P does not contain the exceptional ideal $(x_0, \dots, x_r)$. Without loss of generality, assume $x_0 \notin P$. Consider the S-module map $\lambda : S/P \to S/P$ which is defined by $1 \mapsto x_0$. Then λ is "left multiplication by x_0". Since P is a prime ideal and $x_0 \in S - P$, x_0 is not a zero divisor. The sequence

$$0 \to M \xrightarrow{\lambda} M \to M' \to 0$$

is exact, where $M' = S/(P + (x_0))$. Since $\deg(x_0) = 1$, there is an exact sequence

$$0 \to M_{d-1} \xrightarrow{\lambda} M_d \to M'_d \to 0$$

for each $d > 0$. Proposition 4.1.22 implies $\varphi_M(d) = \varphi_M(d-1) + \varphi_{M'}(d)$. In the notation of Proposition 9.5.9, we have $\varphi_{M'}(d) = (\Delta\varphi_M)(d-1)$. Since M' is a graded $S/(x_0)$-module and $S/(x_0) = A[x_1, \dots, x_r]$ is generated over A by r elements, our induction hypothesis applies to M'. By Proposition 9.5.9, $P_M(z)$ exists. □

6. Krull Dimension of a Commutative Noetherian Ring

The Krull dimension of a commutative ring is defined as the supremum of the lengths of all chains of prime ideals. The fundamental properties of this dimension are derived in this section. General references for this section are [**41**, § 12 and § 13] and [**4**, Chapter 11].

6.1. Definitions. Let R be a commutative ring. Suppose

$$P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$$

is a chain of $n+1$ distinct prime ideals in $\operatorname{Spec} R$. We say this is a *prime chain* of *length n*. If $P \in \operatorname{Spec} R$, the *height* of P, denoted $\operatorname{ht}(P)$, is the supremum of the lengths of all prime chains with $P = P_0$. Let I be a proper ideal of R. The *height* of I, denoted $\operatorname{ht}(I)$, is defined to be the infimum of the heights of all prime ideals containing I, $\operatorname{ht}(I) = \inf\{\operatorname{ht}(P) \mid P \in \operatorname{Spec} R, P \supseteq I\}$. The *Krull dimension*, or simply *dimension* of R is the supremum of the heights of all prime ideals in R, $\dim(R) = \sup\{\operatorname{ht}(P) \mid P \in \operatorname{Spec} R\}$.

EXAMPLE 9.6.1. Let R be a commutative ring.

(1) If R is artinian, then by Proposition 4.5.3, every prime ideal is maximal, so $\dim(R) = 0$.
(2) If R is a PID, then by Theorem 1.5.8, $\dim(R) \le 1$. If R is not a field, $\dim(R) = 1$.
(3) If P is a minimal prime over-ideal of (0), then $\operatorname{ht}(P) = 0$.
(4) If R is a UFD with Krull dimension one, then by Theorem 1.5.8, R is a PID.

LEMMA 9.6.2. *Let R be a commutative ring.*

(1) If $P \in \operatorname{Spec} R$, then $\operatorname{ht}(P) = \dim(R_P)$.
(2) If I is not the unit ideal, then $\dim(R/I) + \operatorname{ht}(I) \le \dim(R)$.
(3) Let R be an integral domain of finite Krull dimension and P a prime ideal in R. If $\dim(R/P)$ *and* $\dim(R)$ *are equal, then* $P = (0)$.
(4) If $W \subseteq R$ is a multiplicative set, then $\dim(W^{-1}R) \le \dim(R)$.

PROOF. Is left to the reader. □

DEFINITION 9.6.3. Let R be a commutative ring and M an R-module. The *Krull dimension* of M is defined by

$$\dim_R(M) = \begin{cases} \dim(R/\operatorname{annih}_R(M)) & \text{if } M \neq (0) \\ -1 & \text{otherwise.} \end{cases}$$

If the ring R is unambiguous, then we write $\dim(M)$ instead of $\dim_R(M)$.

LEMMA 9.6.4. *Let R be a commutative noetherian ring and M a finitely generated nonzero R-module. The following are equivalent.*

(1) *The length of the R-module M is finite, $\ell(M) < \infty$.*
(2) *The ring $R/\operatorname{annih}_R(M)$ is artinian.*
(3) *The Krull dimension of M is zero, $\dim(M) = 0$.*

PROOF. (2) is equivalent to (3): Follows from Proposition 4.5.4.

(2) implies (1): Follows from Proposition 4.1.21 and Exercise 4.1.2.

(1) implies (3): Prove the contrapositive. Replace R with $R/\operatorname{annih}(M)$ and assume $\operatorname{annih}(M) = (0)$. Assume $\dim(R) > 0$. Let P be a minimal prime over-ideal of 0 such that P is not maximal. Since $\operatorname{annih}(M) = 0$ and M is finitely generated, Lemma 3.1.10 says $M_P \neq (0)$. Therefore $P \in \operatorname{Supp}(M)$ and because P is minimal, Theorem 9.2.7 says $P \in \operatorname{Assoc}(M)$. By Lemma 9.2.1, M contains a submodule isomorphic to R/P. The integral domain R/P contains a nonzero prime ideal, so by Proposition 4.5.4, the R-module R/P has infinite length. Therefore $\ell(M) = \infty$. □

6.2. The Krull Dimension of a Noetherian Semilocal Ring.

DEFINITION 9.6.5. Let R be a commutative noetherian semilocal ring with Jacobson radical $J = \mathrm{J}(R)$. Let I be an ideal which is contained in J. By Exercise 4.5.6, R/I is artinian if and only if there exists $\nu > 0$ such that $J^\nu \subseteq I \subseteq J$. If this is true, we call I an *ideal of definition* for R.

EXAMPLE 9.6.6. Let R be a commutative noetherian local ring and $I \subseteq \mathfrak{m}$ an ideal contained in the maximal ideal of R. By Corollary 9.1.4, I is an ideal of definition for R if and only if I is $\mathfrak{m}$-primary.

PROPOSITION 9.6.7. *Let R be a commutative noetherian semilocal ring, M a finitely generated R-module and I an ideal of definition for R.*

(1) *For $d \geq 0$, M/I^dM is an R/I-module of finite length.*
(2) *For all sufficiently large d, $\ell(M/I^dM)$ is a numerical polynomial. This polynomial, denoted $\chi_{M,I}(x)$, is called the* Hilbert polynomial of M with respect to I.
(3) *If $\mathrm{d}(M)$ denotes the degree of the Hilbert polynomial $\chi_{M,I}$, then $\mathrm{d}(M)$ is independent of the choice of I.*
(4) *$\mathrm{d}(M)$ is bounded above by the number of elements in a generating set for I.*

PROOF. As in Example 7.2.3, the associated graded ring for the I-adic filtration of R is $R^* = \operatorname{gr}_I(R) = \bigoplus_{n \geq 0} I^n/I^{n+1}$. As in Example 7.2.5, the associated graded R^*-module for the I-adic filtration of M is $M^* = \operatorname{gr}_I(M) = \bigoplus_{n \geq 0} I^nM/I^{n+1}M$. By Proposition 7.2.9, M^* is a finitely generated R^*-module. Because I is finitely generated, we can write $I = Ru_0 + \cdots + Ru_m$. Let $S = (R/I)[x_0, \ldots, x_m]$. The assignments $x_i \mapsto u_i$ define a graded homomorphism of graded R/I-algebras $S \to R^*$ which is onto. In degree d the length of the modules satisfy $\ell(I^d/I^{d+1}) \leq \ell(S_d)$. As computed in Example 9.5.10, the Hilbert polynomial of S, $P_S(x)$, has degree m. Therefore, the Hilbert polynomial of R^*, $P_{R^*}(x)$, has degree less than or equal to m. In Example 9.5.11 we computed $P_{M^*}(d) = \ell(I^d M/I^{d+1}M) \leq \sum P_{R^*}(d)$ where the sum is finite. It follows that the Hilbert polynomial $P_{M^*}(x)$ has degree less than or equal to m. From the filtration $I^d M \subseteq I^{d-1}M \subseteq \cdots \subseteq IM \subseteq M$, we compute

$$\ell(M/I^d M) = \sum_{j=0}^{d-1} \ell(I^j M/I^{j+1}M)$$

is finite, and is a polynomial of degree less than or equal to m for all sufficiently large d. This proves Parts (1), (2) and (4).

(3): Suppose J is another ideal of definition for R. There exists $\nu > 0$ such that $J^\nu \subseteq I$. For all $d \geq 0$ we have $\ell(M/I^d M) \leq \ell(M/J^{\nu d}M)$. That is, $\chi_{M,I}(x) \leq \chi_{M,J}(\nu x)$ for all sufficiently large x. Since ν is constant, we conclude that $\deg(\chi_{M,I}(x)) \leq \deg(\chi_{M,J}(x))$. By symmetry, we see that $\mathrm{d}(M)$ is independent of the choice of I. $\square$

PROPOSITION 9.6.8. *Let R be a commutative noetherian semilocal ring and I an ideal of definition for R. Let*

$$0 \to A \to B \to C \to 0$$

be an exact sequence of finitely generated R-modules. Then

(1) $\mathrm{d}(B)$ *is equal to the maximum of* $\mathrm{d}(A)$ *and* $\mathrm{d}(C)$.
(2) *The degree of the polynomial* $\chi_{B,I} - \chi_{A,I} - \chi_{C,I}$ *is less than* $\mathrm{d}(B)$.

PROOF. Since $C/I^n C = B/(A + I^n B)$, we have

$$\ell(C/I^n C) = \ell(B/(A + I^n B)) \leq \ell(B/I^n B)$$

hence $\mathrm{d}(C) \leq \mathrm{d}(B)$. From the exact sequence

$$0 \to (A + I^n B)/I^n B \to B/I^n B \to B/(A + I^n B) \to 0$$

and $(A + I^n B)/I^n B = A/(A \cap I^n B)$, we have

$$\begin{aligned}
\chi_{B,I}(n) - \chi_{C,I}(n) &= \ell(B/I^n B) - \ell(B/(A + I^n B)) \\
&= \ell((A + I^n B)/I^n B) \\
&= \ell(A/(A \cap I^n B)).
\end{aligned}$$

By Artin-Rees, Corollary 7.2.14, there exists an integer n_0 such that $I^{n+n_0}A \subseteq A \cap (I^n B) \subseteq I^{n-n_0}A$ for all $n > n_0$. This implies

$$\ell(A/I^{n+n_0}A) \geq \ell(A/(A + I^n B)) \geq \ell(A/I^{n-n_0}A)$$

for $n > n_0$. Taken together, this says the polynomials $\chi_{B,I} - \chi_{C,I}$ and $\chi_{A,I}$ have the same degree and the same leading coefficient. $\square$

PROPOSITION 9.6.9. *Let R be commutative noetherian ring.*

(1) *If R is a semilocal ring, then the Krull dimension of R is finite.*
(2) *If R is a semilocal ring, then* $\dim(R) \leq \mathrm{d}(R)$.
(3) *If $P \in \operatorname{Spec} R$, then* $\mathrm{ht}(P)$ *is finite.*
(4) *R satisfies the DCC on prime ideals.*

PROOF. (2): Let $J = \mathrm{J}(R)$. The proof is by induction on $\mathrm{d}(R)$. If $\mathrm{d}(R) = 0$, then there exists $N > 0$, such that $\ell(R/J^d)$ is constant for all $d \geq N$. By Corollary 7.3.6, this implies $J^N = (0)$. By Proposition 4.5.2, R is artinian and as we have seen in Example 9.6.1, $\dim(R) = 0$.

Inductively suppose $\mathrm{d}(R) > 0$ and that the result is true for any semilocal ring S such that $\mathrm{d}(S) < \mathrm{d}(R)$. If $\dim(R) = 0$, then the result is trivially true. Assume R has a prime chain

$P_0 \supsetneq \cdots \supsetneq P_{r-1} \supsetneq P_r = P$ of length $r > 0$. Let $x \in P - P_{r-1}$. Then $\dim(R/(xR+P)) \geq r-1$. Since P is a prime ideal, if λ is "left multiplication by x", then

$$0 \to R/P \xrightarrow{\lambda} R/P \to R/(xR+P) \to 0$$

is an exact sequence. Apply Proposition 9.6.8 to get $\mathrm{d}(R/(xR+P)) < \mathrm{d}(R/P)$. We always have $\mathrm{d}(R/P) \leq \mathrm{d}(R)$. By the induction hypothesis, $\mathrm{d}(R/(xR+P)) \geq \dim(R/(xR+P))$. Take together, this proves $r-1 \leq \dim(R/(xR+P)) \leq \mathrm{d}(R/(xR+P)) < \mathrm{d}(R/P) \leq \mathrm{d}(R)$.

The rest is left to the reader. □

LEMMA 9.6.10. *Let R be a commutative noetherian semilocal ring, $x \in \mathrm{J}(R)$, and M a nonzero finitely generated R-module.*

(1) $\mathrm{d}(M) \geq \mathrm{d}(M/xM) \geq \mathrm{d}(M) - 1$.
(2) If the Krull dimension of M is r, then there exist elements $x_1, \dots, x_r$ in $\mathrm{J}(R)$ such that $M/(x_1M + \cdots + x_rM)$ is an R-module of finite length.

PROOF. (1): Let I be an ideal of definition for R which contains x. By Proposition 9.6.8, $\mathrm{d}(M) \leq \mathrm{d}(M/xM)$. From the short exact sequence

$$0 \to (xM + I^nM)/I^nM \to M/I^nM \to M/(xM + I^nM) \to 0$$

we get

$$\ell\big((xM + I^nM)/I^nM\big) = \ell(M/I^nM) - \ell\big(M/(xM + I^nM)\big).$$

The kernel of the natural map $M \to xM/(xM \cap I^nM)$ is $\{m \in M \mid xm \in I^nM\} = (I^nM : x)$. Therefore,

$$(xM + I^nM)/I^nM = xM/(xM \cap I^nM) = M/(I^nM : x).$$

Since $x \in I$, $xI^{n-1}M \subseteq I^nM$, hence $I^{n-1}M \subseteq (I^nM : x)$. Therefore

$$\ell(M/I^{n-1}M) \geq \ell\big(M/(I^nM : x)\big) = \ell(M/I^nM) - \ell\big(M/(xM + I^nM)\big),$$

or

$$\ell\big(M/(xM + I^nM)\big) \geq \ell(M/I^nM) - \ell(M/I^{n-1}M),$$

which is true for all sufficiently large n. Since $M/xM \otimes R/I^n = M/(xM + I^nM)$, we can compare the Hilbert polynomials

$$\chi_{M/xM,I}(n) \geq \chi_{M,I}(n) - \chi_{M,I}(n-1).$$

Comparing degrees, we get $\mathrm{d}(M/xM) \geq \mathrm{d}(M) - 1$.

(2): The proof is by induction on $r = \dim(M)$. Lemma 9.6.4 says that M is of finite length when $r = 0$. Inductively, assume $r > 0$ and that the result holds for any module of dimension less than r. Since R is noetherian and $M \neq (0)$, Theorem 9.3.8 says $\mathrm{annih}(M)$ has a primary decomposition. By Theorem 9.2.7, there are only finitely many minimal prime over-ideals of $\mathrm{annih}(M)$. Suppose $P_1, \dots, P_t$ are those minimal prime over-ideals of $\mathrm{annih}(M)$ such that $\dim(R/P_i) = r$. Assume $\mathrm{Max}(R) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_u\}$, so that $\mathrm{J}(R) = \bigcap_{j=1}^{u} \mathfrak{m}_j$. Since $r > 0$, we know that for all i, j, there is no containment relation $\mathfrak{m}_j \subseteq P_i$. By Lemma 6.3.3, for all i there is no containment relation $\mathrm{J}(R) \subseteq P_i$. By Lemma 6.3.2, $\mathrm{J}(R)$ is not contained in the union $P_1 \cup \cdots \cup P_t$. Pick $x \in \mathrm{J}(R) - (P_1 \cup \cdots \cup P_t)$. Consider $\mathrm{annih}(M/xM) \supseteq xR + \mathrm{annih}(M)$. If $P \in \mathrm{Spec}(R)$ and $\mathrm{annih}(M) \subseteq P$, then by choice of x we know P is not in the set $\{P_1, \dots, P_t\}$. Consequently, $\dim(R/P) \leq r-1$. This proves $\dim(M/xM) \leq r-1$. By the induction hypothesis applied to M/xM, there exist $x_2, \dots, x_r$ in $\mathrm{J}(R)$ such that $M/(xM + x_2M + \cdots + x_rM)$ is an R-module of finite length. □

Let R be a commutative noetherian semilocal ring with Jacobson radical $J = \mathrm{J}(R)$. Let M be a nonzero finitely generated R-module. Let $\mathscr{S}$ be the set of all cardinal numbers r such that there exist elements $x_1, \dots, x_r$ in $\mathrm{J}(R)$ satisfying $M/(x_1M + \cdots + x_rM)$ is an R-module of finite length. By Lemma 9.6.10 (2), $\mathscr{S}$ is nonempty. By the Well Ordering Principle, there is a minimum $r \in \mathscr{S}$, which we denote by $\delta(M)$ in the next theorem.

THEOREM 9.6.11. *Let R be a commutative noetherian semilocal ring with Jacobson radical $J = \mathrm{J}(R)$. Let M be a nonzero finitely generated R-module. The three integers*

(1) $\mathrm{d}(M)$
(2) $\dim(M)$
(3) $\delta(M)$

are equal.

PROOF. If $x_1, \dots, x_r$ are in $\mathrm{J}(R)$ and $M/(x_1M + \cdots + x_rM)$ is an R-module of finite length, then by Exercise 9.6.1, $\mathrm{d}(M/(x_1M + \cdots + x_rM) = 0$ and by Lemma 9.6.10 (1), $\mathrm{d}(M/(x_1M + \cdots + x_{r-1}M) \le 1$. Iterate this argument to get $\mathrm{d}(M) \le r$, which implies $\mathrm{d}(M) \le \delta(M)$. By Lemma 9.6.10 (2) we have $\delta(M) \le \dim(M)$. To finish, it is enough to prove $\dim(M) \le \mathrm{d}(M)$.

By Theorem 9.2.10 there exists a filtration $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$ of M and a set of prime ideals $P_i \in \operatorname{Spec} R$ such that $M_i/M_{i-1} \cong R/P_i$ for $i = 1, \dots, n$. Also $\mathrm{Assoc}(M) \subseteq \{P_1, \dots, P_n\} \subseteq \mathrm{Supp}(M)$. By Exercise 9.2.8, every minimal prime over-ideal of $\mathrm{annih}(M)$ is included in the set $\{P_1, \dots, P_n\}$. By Proposition 9.6.8, $\mathrm{d}(M_i)$ is equal to the maximum of $\mathrm{d}(M_{i-1})$ and $\mathrm{d}(R/P_i)$. Iterate this n times to show that $\mathrm{d}(M)$ is equal to the maximum number in the set $\{\mathrm{d}(R/P_i) \mid 1 \le i \le n\}$. By Proposition 9.6.9, it follows that $\mathrm{d}(M)$ is greater than or equal to the maximum number in the set $\{\dim(R/P_i) \mid 1 \le i \le n\}$. A chain of prime ideals in $\mathrm{Spec}(R/\mathrm{annih}(M))$ corresponds to a chain in $\mathrm{Spec}(R)$ of prime ideals containing $\mathrm{annih}(M)$. If such a chain has maximal length, then it terminates at a minimal member of the set $\{P_1, \dots, P_n\}$. Therefore, $\dim(M)$ is equal to the maximum number in the set $\{\dim(R/P_i) \mid 1 \le i \le n\}$. This completes the proof. $\square$

COROLLARY 9.6.12. *Let R be a commutative noetherian ring and $x, x_1, \dots, x_n$ elements of R.*

(1) If P is a minimal prime over-ideal of $Rx_1 + \cdots + Rx_n$, then $\mathrm{ht}(P) \le n$.
(2) (Krull's Hauptidealsatz) If x is not a zero divisor or a unit, and P is a minimal prime over-ideal of Rx, then $\mathrm{ht}(P) = 1$.

PROOF. (1): Let $I = Rx_1 + \cdots + Rx_n$ and assume P is a minimal prime over-ideal of I. There is the containment of sets $I \subseteq P \subseteq R$. Localizing gives rise to the containment of sets $IR_P \subseteq PR_P \subseteq R_P$. Therefore R_P/IR_P has only one prime ideal, so R_P/IR_P is artinian. By Theorem 9.6.11, $n \ge \delta(R_P) = \dim(R_P)$. By Lemma 9.6.2, $\mathrm{ht}(P) = \dim(R_P)$.

(2): By Part (1), $\mathrm{ht}(P) \le 1$. If $\mathrm{ht}(P) = 0$, then P is a minimal prime in $\mathrm{Spec}(R)$. By Theorem 9.2.7 and Proposition 9.2.2, every element of P is a zero divisor. This is a contradiction, since $x \in P$. $\square$

COROLLARY 9.6.13. *Let R be a commutative noetherian local ring with maximal ideal* $\mathfrak{m} = \mathrm{J}(R)$.

(1) The numbers
 (a) $\dim(R)$*, the Krull dimension of R.*
 (b) $\mathrm{d}(R)$*, the degree of the Hilbert polynomial* $\chi_{R,\mathfrak{m}}(n) = \ell(R/\mathfrak{m}^n)$.
 (c) $\delta(R)$*, the minimum number r such that there exists a* $\mathfrak{m}$*-primary ideal with a generating set consisting of r elements.*

are equal.

(2) $\dim(R) \le \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.

(3) *If* $x \in \mathfrak{m}$ *is not a zero divisor, then* $\dim(R/xR) = \dim(R) - 1$.

(4) *Let* $\hat{R}$ *be the* $\mathfrak{m}$*-adic completion of* R*. Then* $\dim(R) = \dim(\hat{R})$.

PROOF. (1): Follows straight from Theorem 9.6.11.

(2): Let $x_1, \dots, x_t$ be elements of $\mathfrak{m}$ that restrict to a $R/\mathfrak{m}$-basis for $\mathfrak{m}/\mathfrak{m}^2$. By Lemma 3.4.1, $Rx_1 + \cdots + Rx_t = \mathfrak{m}$. By Part (1), $\dim(R) = \delta(R) \le t$.

(3): By Corollary 9.6.12 (2), $\operatorname{ht}(Rx) = 1$. By Lemma 9.6.2, $\dim(R/xR) \le \dim(R) - 1$. The reverse inequality follows from Lemma 9.6.10 (1) and Part (1).

(4): By Corollary 7.3.2, $R/\mathfrak{m}^n = \hat{R}/\hat{\mathfrak{m}}^n$, so the Hilbert polynomials $\chi_{R,\mathfrak{m}}$ and $\chi_{\hat{R},\hat{\mathfrak{m}}}$ are equal. □

DEFINITION 9.6.14. Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and assume $\dim(R) = d$. According to Corollary 9.6.13 (1) there exists a subset $\{x_1, \dots, x_d\} \subseteq \mathfrak{m}$ such that the ideal $Rx_1 + \cdots + Rx_d$ is $\mathfrak{m}$-primary. In this case, we say $x_1, \dots, x_d$ is a *system of parameters* for R. If $Rx_1 + \cdots + Rx_d = \mathfrak{m}$, then we say R is a *regular local ring* and in this case we call $x_1, \dots, x_d$ a *regular system of parameters*.

PROPOSITION 9.6.15. *Let* R *be a commutative noetherian local ring with maximal ideal* $\mathfrak{m}$ *and* $x_1, \dots, x_d$ *a system of parameters for* R*. Then*

$$\dim\big(R/(Rx_1 + \cdots + Rx_i)\big) = d - i = \dim(R) - i$$

for each i *such that* $1 \le i \le d$.

PROOF. Let $I_i = Rx_1 + \cdots + Rx_i$, $R_i = R/I_i$, $\mathfrak{m}_i = \mathfrak{m}/I_i$. Let $\eta : R \to R/I_i$. Then R_i is a noetherian local ring with maximal ideal $\mathfrak{m}_i$ and $\eta(x_{i+1}), \dots, \eta(x_d)$ generate a $\mathfrak{m}_i$-primary ideal in R_i. Therefore $\dim(R_i) = \delta(R_i) \le d - i$. Suppose we are given a system of parameters $\eta(z_1), \dots, \eta(z_e)$ for R_i. Then $Rx_1 + \cdots + Rx_i + Rz_1 + \cdots + Rz_e$ is $\mathfrak{m}$-primary. This means $\delta(R) = d \le i + e$, or $e = \dim(R_i) \ge d - i$. □

6.3. Exercises.

EXERCISE 9.6.1. Let R be a commutative noetherian semilocal ring and M a nonzero R-module of finite length. Then $\mathrm{d}(M) = 0$.

EXERCISE 9.6.2. Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. Then $\dim(R) = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ if and only if R is a regular local ring.

EXERCISE 9.6.3. Let R be a commutative ring and I an ideal of R. Then $\dim(R/I) = \dim(R/\operatorname{Rad}(I))$.

EXERCISE 9.6.4. Let R be a commutative noetherian ring. Let I be a proper ideal in R such that $\operatorname{ht}(I) = h > 0$.

(1) Let $P_1, \dots, P_t$ be the complete list of minimal prime over-ideals of (0) in R. Show that there exists $x \in I - \bigcup_{j=1}^{t} P_j$ and that $\operatorname{ht}(Rx) = 1$.
(2) If $1 \le r < h$, and $x_1, \dots, x_r$ is a sequence of elements of I such that $\operatorname{ht}(x_1, \dots, x_r) = r$, show that there exists an element x_{r+1} in I such that $\operatorname{ht}(x_1, \dots, x_r, x_{r+1}) = r + 1$.
(3) Show that there exists a sequence $x_1, \dots, x_h$ of elements of I such that if $1 \le i \le h$, then $\operatorname{ht}(x_1, \dots, x_i) = i$.

EXERCISE 9.6.5. Let R be a commutative ring and M an R-module.

(1) If N is a submodule of M, then $\dim(N) \le \dim(M)$ and $\dim(M/N) \le \dim(M)$.

(2) If $W \subseteq R$ is a multiplicative set and M is finitely generated, then

$$\dim_{W^{-1}R}(W^{-1}M) \leq \dim_R(M).$$

(Hint: Corollary 3.7.10.)

6.4. The Krull Dimension of a Fiber of a Morphism. Let $f : R \to S$ be a homomorphism of commutative rings, and $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 3.3.3. Let $P \in \operatorname{Spec} R$. The fiber over P of the map $f^\sharp$ is $\operatorname{Spec}(S \otimes_R k_p)$, which is homeomorphic to $(f^\sharp)^{-1}(P)$, by Exercise 3.4.3. By Exercise 3.4.2, if Q is a prime ideal of S lying over P, then the corresponding prime ideal of $S \otimes_R k_p$ is $Q \otimes_R k_P$ and the local ring is $S_Q \otimes_R k_P$.

THEOREM 9.6.16. *Let $f : R \to S$ be a homomorphism of commutative noetherian rings. Let $Q \in \operatorname{Spec} S$ and $P = Q \cap R$. Then*

(1) $\operatorname{ht}(Q) \leq \operatorname{ht}(P) + \operatorname{ht}(Q/PS)$.
(2) $\dim(S_Q) \leq \dim(R_P) + \dim(S_Q \otimes_R k_P)$ *where $k_P = R_P/PR_P$ is the residue field.*
(3) If going down holds for f, then equality holds in Parts (1) and (2).
(4) If going down holds for f and $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective, then
  (a) $\dim(S) \geq \dim(R)$*, and*
  (b) for any ideal $I \subseteq R$, $\operatorname{ht}(I) = \operatorname{ht}(IS)$.

PROOF. (1): Follows from (2) by Lemma 9.6.2 and Exercise 3.4.2.

(2): Replace R with R_P, S with S_Q. Assume (R,P) and (S,Q) are local rings and $f : R \to S$ is a local homomorphism of local rings. The goal is to prove that $\dim(S) \leq \dim(R) + \dim(S/PS)$. Let $x_1, \dots, x_n$ be a system of parameters for R and set $I = Rx_1 + \cdots + Rx_n$. There exists $\nu > 0$ such that $P^\nu \subseteq I$. Therefore $P^\nu S \subseteq IS \subseteq PS$ and the ideals IS and PS have the same nil radicals. By Exercise 9.6.3, $\dim(S/IS) = \dim(S/PS)$. Let $\eta : S \to S/IS$ and let $\eta(y_1), \dots, \eta(y_r)$ be a system of parameters for S/IS. Then $Sy_1 + \cdots + Sy_r + Sx_1 + \cdots + Sx_n$ is a Q-primary ideal. Then $\dim(S) \leq r + n = \dim(S/PS) + \dim(R)$.

(3): Continue to use the same notation as in Part (2). Assume $\operatorname{ht}(Q/PS) = r$ and $\operatorname{ht}(P) = n$. There exists a chain $Q = Q_0 \supsetneq Q_1 \supsetneq \cdots \supsetneq Q_r$ in $\operatorname{Spec} S$ such that $Q_r \supseteq PS$. Then $P = Q \cap R \supseteq Q_i \cap R \supseteq P$. This implies each Q_i lies over P. In $\operatorname{Spec} R$ there exists a chain $P \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$. By going down, Proposition 6.3.4, there exists a chain $Q_r \supsetneq Q_{r+1} \supsetneq \cdots \supsetneq R_{r+n}$ in $\operatorname{Spec} S$ such that $Q_{r+i} \cap R = P_i$ for $i = 0, \dots, n$. The chain $Q \supsetneq Q_1 \supsetneq \cdots \supsetneq Q_{r+n}$ shows that $\operatorname{ht}(Q) \geq r + n$.

(4): (a): Let $\mathfrak{m}$ be a maximal prime in R such that $\operatorname{ht}(\mathfrak{m}) = \dim(R)$. Let $\mathfrak{n}$ be a maximal prime in S lying over $\mathfrak{m}$. By Part (3), $\dim(S) \geq \dim(S_\mathfrak{n}) \geq \dim(R_\mathfrak{m}) = \dim(R)$.

(b): Let Q be a minimal prime over-ideal of IS such that $\operatorname{ht}(Q) = \operatorname{ht}(IS)$. If $P = Q \cap R$, then $P \supseteq I$ and $Q \supseteq PS \supseteq IS$. By the choice of Q, $\operatorname{ht}(Q/PS) = 0$. By Part (3), $\operatorname{ht}(IS) = \operatorname{ht}(Q) = \operatorname{ht}(P) \geq \operatorname{ht}(I)$. Conversely, let P be a minimal prime over-ideal of I such that $\operatorname{ht}(P) = \operatorname{ht}(I)$. Let Q be a prime ideal in S lying over P. Then $Q \supseteq PS \supseteq IS$. By Proposition 9.6.9 (4) we can assume Q is a minimal prime over-ideal of PS. Then $\operatorname{ht}(Q/PS) = 0$. By Part (3), $\operatorname{ht}(I) = \operatorname{ht}(P) = \operatorname{ht}(Q) \geq \operatorname{ht}(IS)$. □

THEOREM 9.6.17. *Let $f : R \to S$ where R and S are commutative noetherian rings. Assume S is a faithful integral R-algebra.*

(1) $\dim(R) = \dim(S)$.
(2) If $Q \in \operatorname{Spec}(S)$, then $\operatorname{ht}(Q) \leq \operatorname{ht}(Q \cap R)$.
(3) If going down holds for f, then for any ideal J of S, $\operatorname{ht}(J) = \operatorname{ht}(J \cap R)$.

PROOF. We can assume f is the set inclusion map and view R as a subring of S.

(1): It follows from Theorem 6.3.6 (2) that a chain $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ of length n in $\operatorname{Spec}(S)$ gives rise to a chain $Q_0 \cap R \subsetneq Q_1 \cap R \subsetneq \cdots \subsetneq Q_n \cap R$ of length n in $\operatorname{Spec}(R)$. Thus $\dim(S) \le \dim(R)$. By Theorem 6.3.6 (3), a chain of length n in $\operatorname{Spec}(R)$ lifts to a chain of length n in $\operatorname{Spec}(S)$. Thus $\dim(S) \ge \dim(R)$.

(2): We have $Q \subseteq (Q \cap R)S$ and by Theorem 6.3.6 (2), Q is a minimal prime over-ideal of $(Q \cap R)S$. Apply Theorem 9.6.16 (1).

(3): Since going down holds for $R \to S$, by Theorem 9.6.16 (3), equality holds in Part (2). Pick Q to be a minimal prime over-ideal of J such that $\operatorname{ht}(Q) = \operatorname{ht}(J)$. Then $\operatorname{ht}(J) = \operatorname{ht}(Q) = \operatorname{ht}(Q \cap R) \ge \operatorname{ht}(J \cap R)$. Pick P to be a minimal prime over-ideal for $J \cap R$. By Exercise 6.1.2, S/J is an integral extension of $R/(J \cap R)$. By Theorem 6.3.6 (1), there exists $Q \in \operatorname{Spec}(S)$ such that $Q \supseteq J$ and $Q \cap R = P$. Then $\operatorname{ht}(J \cap R) = \operatorname{ht}(P) = \operatorname{ht}(Q) \ge \operatorname{ht}(J)$. □

THEOREM 9.6.18. *Let $f : R \to S$ where R and S are commutative noetherian rings, and assume going up holds for f. If $p, q \in \operatorname{Spec} R$ such that $p \supseteq q$, then* $\dim(S \otimes_R k_p) \ge \dim(S \otimes_R k_q)$.

PROOF. Let $n = \dim(S \otimes_R k_q)$. Then there exists a chain $Q_0 \subsetneq \cdots \subsetneq Q_n$ in $\operatorname{Spec} S$ such that $Q_i \cap R = q$ for all $i = 0, \ldots, n$. Let $m = \operatorname{ht}(p/q)$. Then there exists a chain $q = p_0 \subsetneq \cdots \subsetneq p_m = p$ in $\operatorname{Spec} R$. Since going up holds, there exists a chain $Q_n \subsetneq \cdots \subsetneq Q_{n+m}$ in $\operatorname{Spec} S$ such that $Q_{n+i} \cap R = p_i$ for all $i = 0, \ldots, m$. The chain $Q_0 \subsetneq \cdots \subsetneq Q_{n+m}$ shows $\operatorname{ht}(Q_{n+m}/Q_0) \ge n+m$. Apply Theorem 9.6.16 to $R/q \to S/Q_0$ with the prime ideals Q_{n+m}/Q_0 and p/q playing the roles of Q and P. Then

$$\begin{aligned}
n+m &\le \operatorname{ht}(Q_{n+r}/Q_0) \\
&\le \operatorname{ht}(p/q) + \operatorname{ht}(Q_{n+m}/(Q_0 + pS)) \\
&\le \operatorname{ht}(p/q) + \operatorname{ht}(Q_{n+m}/pS) \\
&\le \operatorname{ht}(p/q) + \dim(S \otimes_R k_p).
\end{aligned}$$

From which it follows that $\dim(S \otimes_R k_q) \le \dim(S \otimes_R k_p)$. □

7. The Krull-Akizuki Theorem

This short section is devoted to a proof of Theorem 9.7.5, which is commonly known as the Krull-Akizuki Theorem. The proof we give follows [**12**, Chapter VII, § 2.5]. Throughout this section, all rings are commutative. Given an R-module M, if M has a composition series, then we say M has finite length and $\ell(M)$ denotes the length of any composition series for M (Definition 4.1.19). If R is an integral domain with field of fractions K and M is a torsion free R-module, then the natural mapping $R \otimes_R M \to K \otimes_R M$ is one-to-one (Lemma 3.1.4). We identify M with the R-submodule $1 \otimes_R M$ of $K \otimes_R M$. The *rank* of M is defined to be $\dim_K(K \otimes_R M)$. If M is finitely generated, then by Theorem 2.3.23, M has finite rank. We mention however that the converse is false. For example, if we assume R is not a field, then K is not a finitely generated R-module (Lemma 6.1.4), but K has rank 1 since $K \otimes_R K = K$.

The Krull-Akizuki Theorem is concerned with the finiteness of the integral closure S of a noetherian integral domain R in a finite algebraic field extension L of the quotient field K of R. When R is integrally closed in K and L/K is separable, Theorem 6.1.13 applies. When R is a finitely generated algebra over a field k, there is a stronger result proved below in Theorem 10.3.11. The main difference between these theorems and Theorem 9.7.5 below is that we assume only that R is noetherian with Krull dimension one, and we show that S is also noetherian and has dimension one. Also, in Corollary 9.7.6 we see that the fibers of $\operatorname{Spec} S \to \operatorname{Spec} R$ are finite. Before restricting to the case where R is noetherian, we prove in Lemma 9.7.1 that the fiber over the generic point of $\operatorname{Spec} R$ is the generic point of S.

LEMMA 9.7.1. *Let R be an integral domain with quotient field K. Let L be a finitely generated algebraic extension field of K and S a subring of L containing R. Then the following are true.*

(1) There is an R-algebra homomorphism $\gamma : K \otimes_R S \to L$ defined by $x \otimes y \mapsto xy$ which maps $K \otimes_R S$ isomorphically onto a subfield of L containing K and S.
(2) S is an R-module of finite rank.
(3) If $\mathfrak{q}$ is a prime ideal of S such that $\mathfrak{q} \cap R = (0)$, then $\mathfrak{q} = (0)$.

PROOF. (1): Consider $W = R - (0)$ which is a multiplicative subset of S contained in R. We can identify the localization $W^{-1}S$ with an R-subalgebra of L containing both K and S (Lemma 3.1.2). Since $W^{-1}S$ is finite dimensional over K, $W^{-1}S$ is a field by Lemma 6.1.4. Hence $W^{-1}S$ is isomorphic to the quotient field of S. By Lemma 3.1.4, γ maps $K \otimes_R S$ isomorphically onto $W^{-1}S$.

Part (2) follows from the fact that $K \otimes_R S$ is finite dimensional over K. Part (3) follows from Exercise 3.3.9. □

LEMMA 9.7.2. *Let R be a noetherian integral domain with* $\dim(R) = 1$. *If M is a finitely generated torsion R-module, then the length of M is finite, $\ell(M) < \infty$.*

PROOF. Since M is torsion, $\operatorname{annih}_R(M)$ is a proper ideal of R. Then $\dim(M) = \dim(R/\operatorname{annih}_R(M)) = 0$. By Lemma 9.6.4, M has finite length. □

LEMMA 9.7.3. *Let R be a commutative ring, M an R-module, and $\{M_i \mid i \in I\}$ a directed system of submodules of M ordered by set inclusion and indexed by a directed set I. If $M = \bigcup_{i \in I} M_i$, then $\ell(M) = \sup\{\ell(M_i) \mid i \in I\}$.*

PROOF. By Proposition 4.1.20, $\ell(M_i) \le \ell(M)$ for each i. If the set $\{\ell(M_i) \mid i \in I\}$ is unbounded, then $\ell(M) = \sup\{\ell(M_i) \mid i \in I\} = \infty$. Assume $N \in \mathbb{N}$ and $N = \sup\{\ell(M_i) \mid i \in I\}$. Therefore, there exists $j \in I$ such that $\ell(M_j) = N$. The family of submodules is directed, hence given any pair i, j in I, there is $k \in I$ such that $M_i \cup M_j \subseteq M_k$. So for all $k \ge j$ we have $\ell(M_j) = \ell(M_k) = N$. Since the union of the M_i is M, we have $N = \ell(M)$. □

LEMMA 9.7.4. *Let R be a noetherian integral domain with* $\dim(R) = 1$. *Let M be a torsion free R-module of finite rank n. If α is a nonzero element of R, then $R/\alpha R$ is an R-module of finite length and*

$$\ell(M/\alpha M) \le n\,\ell(R/\alpha R).$$

PROOF. Since $R/\alpha R$ is a torsion R-module, by Lemma 9.7.2, it is an R-module of finite length.

Step 1: We prove that the inequality holds if M is a finitely generated R-module. By Exercise 3.1.13, there is a free R-submodule $F \subseteq M$ such that F has rank n and M/F is a finitely generated torsion R-module. By Lemma 9.7.2, $\ell(M/F)$ is finite. Since M is torsion free, if $i \ge 0$, then multiplication by α^i defines an isomorphism $M/\alpha M \to \alpha^i M/\alpha^{i+1}M$. Fix $m \ge 1$. By Theorem 1.1.12 (2), Proposition 4.1.22 and induction on m,

$$\ell(M/\alpha^m M) = m\,\ell(M/\alpha M). \tag{7.1}$$

Since F is free of rank n, we have

$$\ell(F/\alpha^m F) = m\,\ell(F/\alpha F) = nm\,\ell(R/\alpha R). \tag{7.2}$$

Consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & F \arrow[r] \arrow[d, "\alpha^m"] & M \arrow[r] \arrow[d, "\alpha^m"] & M/F \arrow[r] \arrow[d, "\alpha^m"] & 0 \\
0 \arrow[r] & F \arrow[r] \arrow[d, "\eta_1"] & M \arrow[r] \arrow[d, "\eta_2"] & M/F \arrow[r] \arrow[d, "\eta_3"] & 0 \\
 & F/\alpha^m F \arrow[r, "\phi"] & M/\alpha^m M \arrow[r] & (M/F)/(\alpha^m(M/F)) \arrow[r] & 0
\end{tikzcd} \tag{7.3}$$

where η_1, η_2, η_3 are the natural maps and are onto. The bottom row of (7.3) is exact by Theorem 2.5.2. Viewing F as a submodule of M, the image of ϕ is $\eta_2(F)$. By Theorem 1.1.12 (2)],

$$F/\alpha^m F \xrightarrow{\phi} F/(F \cap \alpha^m M) \to 0 \tag{7.4}$$

is exact. Applying Proposition 4.1.22 to the bottom row of (7.3), (7.4), and the rightmost column of (7.3), we have

$$\begin{aligned}
\ell(M/\alpha^m M) &= \ell(\operatorname{im}\phi) + \ell\left((M/F)/(\alpha^m(M/F))\right) \\
&\le \ell(F/\alpha^m F) + \ell\left((M/F)/(\alpha^m(M/F))\right) \\
&\le \ell(F/\alpha^m F) + \ell(M/F).
\end{aligned} \tag{7.5}$$

Combining (7.5) with (7.1) and (7.2) yields

$$\ell(M/\alpha M) \le n\,\ell(R/\alpha R) + m^{-1}\,\ell(M/F). \tag{7.6}$$

Since $\ell(M/F)$ is finite and (7.6) holds for all $m \ge 1$, this completes Step 1.

Step 2: Assume M is not finitely generated. Let $\{M_i \mid i \in I\}$ be the directed system of finitely generated submodules $M_i \subseteq M$ ordered by set inclusion and where each M_i has rank n. By Step 1, $\ell(M_i/\alpha M_i) \le n\,\ell(R/\alpha R)$ for each i. Using a diagram similar to (7.3), we see that for each i, the image of $M_i/\alpha M_i \to M/\alpha M$ is $M_i/(M_i \cap \alpha M)$. Therefore,

$$\begin{aligned}
\ell(M_i/(M_i \cap \alpha M)) &\le \ell(M_i/\alpha M_i) \\
&\le n\,\ell(R/\alpha R).
\end{aligned} \tag{7.7}$$

By Lemma 9.7.3 applied to $M/\alpha M$ and the directed system $\{M_i/(M_i \cap \alpha M) \mid i \in I\}$ of submodules, we conclude that $\ell(M/\alpha M) \le n\,\ell(R/\alpha R)$. □

THEOREM 9.7.5. *(Krull-Akizuki) Let R be a noetherian integral domain with* $\dim(R) = 1$. *Let K be the quotient field of R, L a finitely generated algebraic extension of K, and S a subring of L containing R. Then S is noetherian. If S is not a field, then* $\dim(S) = 1$, *and for every nonzero ideal $\mathfrak{A}$ in S, $S/\mathfrak{A}$ is a finitely generated R-module.*

PROOF. Since a field is noetherian, assume from now on that S is not a field. By Lemma 9.7.1, S is an R-module of finite rank.

Let $\mathfrak{A}$ be a nonzero nonunit ideal of S. To show S is noetherian, it suffices to show that $\mathfrak{A}$ is finitely generated as an S-module. To show $S/\mathfrak{A}$ is finitely generated as an R-module, it suffices to show $S/\mathfrak{A}$ is an R-module of finite length.

Let $u \in \mathfrak{A} - (0)$ and let $f(x) = \operatorname{Irr.poly}_K(u)$ be the irreducible polynomial for u in $K[x]$. Then $f(u) = 0$ and after clearing denominators by multiplying by some element of R, we get an equation

$$r_n u^n + \cdots + r_2 u^2 + r_1 u + r_0 = 0$$

where $r_0, \ldots, r_n$ are elements in R. Since u is invertible in L, $r_0 \neq 0$. This shows $r_0 \in Su \subseteq \mathfrak{A}$. Apply Lemma 9.7.4 with $M = S$ and $\alpha = r_0$. Then S/r_0S is an R-module of finite length. Since $S/r_0S \to S/\mathfrak{A}$ is onto, this implies $S/\mathfrak{A}$ is an R-module of finite length.

By Exercise 4.1.14, S/r_0S is an S-module of finite length. Since $\mathfrak{A}/r_0S \to S/r_0S$ is one-to-one, it follows that $\mathfrak{A}/r_0S$ is an S-module of finite length. Hence $\mathfrak{A}/r_0S$ is a finitely generated S-module. The exact sequence

$$0 \to r_0S \to \mathfrak{A} \to \mathfrak{A}/r_0S \to 0$$

shows that $\mathfrak{A}$ is a finitely generated S-module (Lemma 3.1.13). If $\mathfrak{p}$ is a nonzero prime ideal of S, then $S/\mathfrak{p}$ is an integral domain and an S-module of finite length. By Proposition 4.1.21, $S/\mathfrak{p}$ is artinian. By Exercise 4.1.6, $S/\mathfrak{p}$ is a field. Therefore, $\mathfrak{p}$ is a maximal ideal. □

COROLLARY 9.7.6. *Let R, K, L and S be as in Theorem 9.7.5. If $\mathfrak{p}$ is a prime ideal of R, then there are only finitely many prime ideals of S lying over $\mathfrak{p}$.*

PROOF. If $\mathfrak{p} = (0)$, then there is only one prime ideal of S lying over $\mathfrak{p}$, by Lemma 9.7.1. If $\mathfrak{p} \neq (0)$, then by Theorem 9.7.5, $S \otimes_R R/\mathfrak{p}$ is a finitely generated R-module. Therefore, $S \otimes_R R/\mathfrak{p}$ is a finitely generated vector space over the field $R/\mathfrak{p}$. By Exercise 3.4.3 there is a one-to-one correspondence between prime ideals of S lying over $\mathfrak{p}$ and prime ideals of $S \otimes_R R/\mathfrak{p}$. By Exercise 4.1.13 and Proposition 4.5.3, $\operatorname{Spec}(S \otimes_R R/\mathfrak{p})$ is finite. □

CHAPTER 10

Derivations, Differentials

This chapter introduces two powerful methods for studying separable algebras over commutative rings. These new tools are the module of R-derivations on an R-algebra, and the module of Kähler differentials. Applying results about derivations allows us to prove theorems on faithfully flat descent of separability, the separability at the stalks criteria, and the residue field tests for separability. Applying results on Kähler differentials, we derive separability criteria for commutative R-algebras. For example, the vanishing of the module of Kähler differentials leads to a separability criterion for a finitely generated commutative algebra. Differentials are applied to prove jacobian criteria for separability in Section 10.2, and for regularity in Section 11.6.

Noether's Normalization Lemma is proved in Theorem 10.3.3. In summary this lemma states that if A is a finitely generated k-algebra, then A contains a subalgebra Z isomorphic to a polynomial ring in n indeterminates, where A is integral over Z and n is equal to the Krull dimension of A. When the ground field k is infinite, a second version is proved in Corollary 10.3.3. As an application, a theorem on the finiteness of the integral closure of an integral domain is proved (Theorem 10.3.11).

The useful Local Criteria for Flatness are proved in Theorem 10.4.13 and the Theorem on Generic Flatness is proved in Theorem 10.4.21.

The last section of this chapter concludes with Corollary 10.5.4. This useful result specifies sufficient criteria such that the direct limit of a directed system of noetherian local rings is again a noetherian local ring.

1. Derivations

This section contains an introduction to R-derivations on an R-algebra with coefficients in a two-sided module. General references for the material in this section are [**14**], [**36**], [**41**], [**32**], [**34**], and [**18**].

1.1. The Definition and First Results. Let R be a commutative ring and A an R-algebra. The enveloping algebra is $A^e = A \otimes_R A^o$. A left right A-bimodule M is called a two-sided A/R-module if the left and right R-actions agree (Definition 5.1.1). If M is a left A^e-module, then we can make M into a two-sided A/R-module by defining $ax = a \otimes 1 \cdot x$ and $xa = 1 \otimes a \cdot x$. In particular, A^e is a left A^e-module, hence is a two-sided A/R-module.

If M is any two-sided A/R-module, then an R-*derivation* from A to M is an R-module homomorphism $\partial : A \to M$ satisfying

$$\partial(ab) = a\partial(b) + \partial(a)b$$

for all $a, b \in A$. The set of all R-derivations from A to M is denoted $\mathrm{Der}_R(A, M)$. The reader should verify that $\mathrm{Der}_R(A, M)$ is an R-submodule of $\mathrm{Hom}_R(A, M)$ and that if ∂ is any R-derivation, then $\partial(1) = 0$.

EXAMPLE 10.1.1. Let R be any ring, x an indeterminate, and $A = R[x]$ the polynomial ring. The usual derivative with respect to x is a $\mathbb{Z}$-derivation $\partial : A \to A$.

There is an exact sequence of A^e-modules

$$0 \to J_{A/R} \to A^e \xrightarrow{\mu} A \to 0 \tag{1.1}$$

where μ is defined by $a \otimes b \mapsto ab$ and $J_{A/R}$ is defined to be the kernel of μ (Definition 5.1.1). By Definition 5.1.3, A is separable over R if and only if (1.1) is split exact as a sequence of A^e-modules. By Exercise 5.1.3, $J_{A/R}$ is generated as a left ideal in A^e by the set of all elements of the form $a \otimes 1 - 1 \otimes a$.

LEMMA 10.1.2. *Let R be a commutative ring, A an R-algebra and S a commutative R-algebra. Then the following are true.*

(1) The sequence (1.1) *is a split exact sequence of A-modules and hence a split exact sequence of R-modules.*
(2) $A^e \otimes_R S = (A \otimes_R S)^e$.
(3) $J_{A \otimes_R S/S} = J_{A/R} \otimes_R S$.

PROOF. (1): By Exercise 2.3.10, there is an R-algebra homomorphism $\rho : A \to A \otimes_R A^o$ defined by $\rho(a) = a \otimes 1$. Using ρ we view each term in (1.1) as a left A-module. The reader should verify that $\mu\rho = 1$ and that both ρ and μ are left A-module homomorphisms. Therefore, (1.1) is split exact as a sequence of left A-modules.
(2): This is left to the reader.
(3): This follows from (2) by tensoring the split exact sequence (1.1) with $(\ ) \otimes_R S$. □

EXAMPLE 10.1.3. Define an R-module homomorphism $\delta : A \to J_{A/R}$ by

$$\delta(a) = a \otimes 1 - 1 \otimes a.$$

If $a, b \in A$, then

$$\begin{aligned}
\delta(ab) &= ab \otimes 1 - 1 \otimes ab \\
&= ab \otimes 1 - a \otimes b + a \otimes b - 1 \otimes ab \\
&= (a \otimes 1)(b \otimes 1 - 1 \otimes b) + (1 \otimes b)(a \otimes 1 - 1 \otimes a) \\
&= a\delta(b) + \delta(a)b.
\end{aligned}$$

Therefore $\delta : A \to J_{A/R}$ is an R-derivation.

LEMMA 10.1.4. *If $\delta : A \to J_{A/R}$ is from Example 10.1.3, then $A\delta(A) = J_{A/R}$. That is, the image of δ generates $J_{A/R}$ as a left A-module.*

PROOF. A typical element of $J_{A/R}$ is $x = \sum_i x_i \otimes y_i$ such that $\sum_i x_i y_i = 0$. Then $\sum_i x_i(1 \otimes y_i - y_i \otimes 1) = \sum_i x_i \otimes y_i - \left(\sum_i x_i y_i\right) \otimes 1 = x$. □

LEMMA 10.1.5. *Let R be a commutative ring and A an R-algebra.*

(1) If A is commutative and is generated as an R-algebra by the set $X = \{x_i\}_{i \in I}$, then $J_{A/R}$ is generated as an A^e-module by the set $\delta(X) = \{x_i \otimes 1 - 1 \otimes x_i\}_{i \in I}$.
(2) If A is finitely generated as an R-module, then $J_{A/R}$ is finitely generated as an R-module.
(3) Assume either
   (a) A is a finitely generated R-module, or
   (b) A a finitely generated commutative R-algebra.
   Then $J_{A/R}$ is a finitely generated left ideal of A^e and A is an A^e-module of finite presentation.

PROOF. (1): A typical element of A can be written as a finite sum $a = \sum r_i m_i$, where $r_i \in R$ and m_i is a monomial in X. Since δ is R-linear, it is enough to show $\delta(x_1 \cdots x_n)$ is in $A^e\delta(X)$, where $x_1, \dots, x_n$ represent any elements (not necessarily distinct) of X. Because δ is an R-derivation, this follows from the generalized product rule, Exercise 10.1.1.

(2): By Proposition 2.3.24, A^e is a finitely generated R-module. The sequence (1.1) is split exact as a sequence of R-modules, hence $J_{A/R}$ is a homomorphic image of A^e.

(3): In both cases, $J_{A/R}$ is finitely generated over A^e. The exact sequence (1.1) shows that A is of finite presentation as a left A^e-module. □

Given any $f \in \operatorname{Hom}_{A^e}(J_{A/R}, M)$, let $\alpha_f : A \to M$ be defined by

$$\alpha_f(a) = f(\delta(a)).$$

The reader should verify that $\alpha_f \in \operatorname{Der}_R(A, M)$ and that there is a homomorphism of R-modules $\alpha : \operatorname{Hom}_{A^e}(J_{A/R}, M) \to \operatorname{Der}_R(A, M)$ defined by $f \mapsto \alpha_f$. Given any $m \in M$, let $\tau_m : A \to M$ be defined by

$$\tau_m(a) = am - ma.$$

The reader should verify that $\tau_m \in \operatorname{Der}_R(A, M)$ and that there is a homomorphism of R-modules $\tau : M \to \operatorname{Der}_R(A, M)$ defined by $m \mapsto \tau_m$.

PROPOSITION 10.1.6. *In the notation developed above, there is a commutative diagram of R-modules*

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_{A^e}(A, M) \arrow[r] \arrow[d, "\gamma"', "\cong"] & \operatorname{Hom}_{A^e}(A^e, M) \arrow[r, "\sigma"] \arrow[d, "\beta"', "\cong"] & \operatorname{Hom}_{A^e}(J_{A/R}, M) \arrow[d, "\alpha"', "\cong"] \\
0 \arrow[r] & M^A \arrow[r] & M \arrow[r, "\tau"] & \operatorname{Der}_R(A, M)
\end{tikzcd}$$

such that the three vertical maps are isomorphisms and the rows are exact.

PROOF. Applying the left exact functor $\operatorname{Hom}_{A^e}(\cdot, M)$ to the exact sequence (1.1) yields the top row. Clearly the kernel of τ is M^A, so the bottom row is exact. The isomorphism β comes from Lemma 2.4.7 and is defined by the action $f \mapsto f(1)$. The isomorphism γ comes from Lemma 5.1.5. We check that $\alpha\sigma = \tau\beta$. Suppose $f \in \operatorname{Hom}_{A^e}(A^e, M)$, $f(1) = m$, and $a \in A$. Then

$$\begin{aligned}
\alpha(\sigma(f))(a) &= f(\delta(a)) \\
&= \delta(a) f(1) \\
&= (a \otimes 1 - 1 \otimes a)m \\
&= am - ma \\
&= \tau(\beta(f))(a).
\end{aligned}$$

Next we verify that α is one-to-one. Suppose $\alpha_f = 0$. Then $f(\delta(A)) = 0$. It follows from Lemma 10.1.4 that $f(J_{A/R}) = 0$. Now we show that α is onto. Let $\partial \in \operatorname{Der}_R(A, M)$. We must show that there exists $h \in \operatorname{Hom}_{A^e}(J_{A/R}, M)$ such that $\partial = h \circ \delta$. The reader should verify that the assignment $x \otimes y \mapsto -x\partial(y)$ defines an R-module homomorphism $h : A^e \to M$

and $h(\delta(a)) = h(a \otimes 1 - 1 \otimes a) = -a\partial(1) + \partial(a) = \partial(a)$. To show that h is a homomorphism of A^e-modules, let $x = \sum_i x_i \otimes y_i$ be a typical element of $J_{A/R}$ and $a \otimes b \in A^e$. Then

$$\begin{aligned} h(a \otimes b \cdot x) &= h\Big(a \otimes b \sum_i x_i \otimes y_i\Big) \\ &= h\Big(\sum_i a x_i \otimes y_i b\Big) \\ &= -\sum_i a x_i \partial(y_i b) \\ &= -\sum_i a x_i \big(y_i \partial(b) + \partial(y_i) b\big) \\ &= -a\Big(\sum_i x_i y_i\Big)\partial(b) - a\Big(\sum_i x_i \partial(y_i)\Big) b \\ &= a \otimes b \cdot h(x) \end{aligned}$$

completes the proof. □

The image of $\tau : M \to \operatorname{Der}_R(A,M)$ is denoted $\operatorname{Inn.Der}_R(A,M)$ and is called the set of *inner derivations*. Because the diagram of Proposition 10.1.6 commutes, under the isomorphism α, the set of inner derivations corresponds to the set of $f \in \operatorname{Hom}_{A^e}(J_{A/R}, M)$ such that f extends to $A^e \to M$.

PROPOSITION 10.1.7. *Let A and C be commutative R-algebras and*

$$u : A \to C$$

a homomorphism of R-algebras. Let I be an ideal in C such that $I^2 = 0$. Consider the map on sets

$$\beta : \operatorname{Hom}_{R\text{-}alg}(A,C) \to \operatorname{Hom}_{R\text{-}alg}(A,C/I)$$

which is induced by the natural map $\eta : C \to C/I$ on R-algebras. Let $\bar{u} = \beta(u) = \eta u$. Make I into an A-module using the homomorphism u. That is, $a \cdot x = u(a)x$.

(1) If $D : A \to I$ is an R-derivation, then $u + D : A \to C$ is an R-algebra homomorphism in $\beta^{-1}(\bar{u})$.
(2) If $v : A \to C$ is in $\beta^{-1}(\bar{u})$, and $D = v - u$, then $D : A \to I$ is an R-derivation.
(3) The mapping $D \mapsto u + D$ defines a one-to-one correspondence

$$\operatorname{Der}_R(A,I) \to \{v \in \operatorname{Hom}_{R\text{-}alg}(A,C) \mid \beta(v) = \beta(u)\}.$$

PROOF. (1): Because

$$\begin{aligned} (u+D)(ab) &= u(ab) + D(ab) \\ &= u(a)u(b) + u(a)D(b) + u(b)D(a) \end{aligned}$$

is equal to

$$\begin{aligned} (u(a)+D(a))(u(b)+D(b)) &= u(a)u(b) + u(a)D(b) + u(b)D(a) + D(a)D(b) \\ &= u(a)u(b) + u(a)D(b) + u(b)D(a), \end{aligned}$$

$u + D$ is multiplicative. The rest is left to the reader.

(2): For $a \in A$, $D(a) = u(a) - v(a)$ is in I. The computation

$$\begin{aligned} v(ab) &= v(a)v(b) \\ &= (u(a)+D(a))(u(b)+D(b)) \\ &= u(a)u(b) + u(a)D(b) + u(b)D(a) + D(a)D(b) \\ &= u(a)u(b) + u(a)D(b) + u(b)D(a), \end{aligned}$$

shows that $D(ab) = u(a)D(b) + u(b)D(a)$.

Part (3) follows from (1) and (2). $\square$

1.2. Exercises.

EXERCISE 10.1.1. (Generalized Product and Power Rules) Suppose A is an R-algebra, M is a two-sided A/R-module, $\partial \in \operatorname{Der}_R(A,M)$ and $x, x_1, \dots, x_n \in A$. Prove that

$$\partial(x_1 x_2 \cdots x_n) = \partial(x_1)x_2 \cdots x_n + x_1 \partial(x_2) x_3 \cdots x_n + \cdots + x_1 \cdots x_{n-1} \partial(x_n)$$

and if $n \geq 1$, then $\partial(x^n) = \sum_{i=0}^{n-1} x^i \partial(x) x^{n-1-i}$.

EXERCISE 10.1.2. (Chain Rule) Suppose A is a commutative R-algebra and M is an A-module. Prove that if $a \in A$ and $f(x) \in R[x]$, then for any $\partial \in \operatorname{Der}_R(A,M)$, $\partial(f(a)) = f'(a)\partial(a)$.

EXERCISE 10.1.3. Let A be an R-algebra. Show that $M \mapsto \operatorname{Der}_R(A,M)$ defines a covariant functor from the category of two-sided A/R-modules to the category of R-modules.

EXERCISE 10.1.4. Suppose S is a commutative R-algebra and A is any S-algebra. Let M be a two-sided A/S-module. Show that there is an exact sequence of abelian groups

$$0 \to \operatorname{Der}_S(A,M) \xrightarrow{a} \operatorname{Der}_R(A,M) \xrightarrow{b} \operatorname{Der}_R(S,M).$$

EXERCISE 10.1.5. Let R be a commutative ring and S a commutative R-algebra. Let $A = S[x]$ be the polynomial ring over S in one variable and let M be any A-module. Show that $\operatorname{Der}_R(A,M) \to \operatorname{Der}_R(S,M)$ is onto. (Hint: If $\partial : S \to M$ is an R-derivation, show that the assignment $ax^i \mapsto x^i \partial(a)$ defines an R-derivation $D : A \to M$.)

EXERCISE 10.1.6. (The Extension of a Ring by a Module) Let A be an R-algebra and N a two-sided A/R-module (Definition 5.1.1). Define a multiplication on the two-sided A/R-module $A \oplus N$ by the formula $(a,x)(b,y) = (ab, ay + xb)$, for all a,b in A and all x,y in N.

(1) Show that the multiplication rule defined above turns the A-module $A \oplus N$ into an R-algebra with unit element $(1,0)$. Denote this R-algebra by $A * N$.
(2) Show that the subset $\{(0,x) \mid x \in N\}$ is an ideal in $A * N$ satisfying $N^2 = 0$ and that there is a split exact sequence of two-sided A/R-modules $0 \to N \to A * N \to A \to 0$. The ring $A * N$ is called the *trivial, or split extension of A by N*.
(3) Show that the map $a \mapsto (a,0)$ defines an R-algebra homomorphism $\sigma : A \to A * N$ which is a section to the natural map $\eta : A * N \to A$ (that is, $\eta\sigma = 1$).
(4) Let $D \in \operatorname{Der}_{\mathbb{Z}}(A,N)$. Define $u : A \to A * N$ by $u(a) = (a, D(a))$. Show that u is a ring homomorphism which is a section to the natural map $\eta : A * N \to A$.
(5) Prove the converse to (4). That is, show that if $u : A \to A * N$ is a $\mathbb{Z}$-algebra section to η, then $u(a) - \sigma(a) : A \to N$ is a $\mathbb{Z}$-derivation.
(6) Let B be a commutative R-algebra and I an ideal in B satisfying $I^2 = 0$. Let $A = B/I$. Show that there is an exact sequence of A-modules $0 \to I \to B \to A \to 0$. We say that B is an *extension of A by I*. Show that B is isomorphic to $A * I$ as R-algebras if and only if there is an R-algebra homomorphism $\sigma : A \to B$ which is a section to the natural map $B \to A$ (in this case the extension is also said to be trivial, or split).

EXERCISE 10.1.7. Let A be an R-algebra and $D \in \operatorname{Der}_R(A,A)$. View $\operatorname{Der}_R(A,A)$ as an R-submodule of the ring $\operatorname{Hom}_R(A,A)$ of A-module endomorphisms of A. Let D^i denote the composition map where D is applied i times. Then D^i is an element of $\operatorname{Hom}_R(A,A)$, but not necessarily an element of $\operatorname{Der}_R(A,A)$. Prove:

(1) (Leibniz Formula) For all $a, b \in A$ and $n \geq 0$,

$$D^n(ab) = \sum_{i=0}^{n} \binom{n}{i} D^i(a) D^{n-i}(b).$$

(2) If R has characteristic p, a prime number, then $D^p \in \operatorname{Der}_R(A,A)$ is an R-derivation on A.

1.3. More Tests for Separability. Now we apply the above results on derivations to establish separability criteria for algebras. The main results are the vanishing of the first Hochschild cohomology criterion, the theorems on faithfully flat descent, the separability at the stalks criteria, and the residue field tests.

Let R be a commutative ring, A an R-algebra, and $A^e = A \otimes_R A^o$ the enveloping algebra. If M is a two-sided A/R-module, then the nth Hochschild cohomology group of A with coefficients in M is defined to be $\mathrm{H}^n(A,M) = \operatorname{Ext}^n_{A^e}(A,M)$ (Definition 8.7.1).

LEMMA 10.1.8. *In the above context, the following are true.*

(1) $\mathrm{H}^0(A,M) = M^A = \{x \in M \mid ax = xa, \text{ for all } a \in A\}$.

(2) $\mathrm{H}^1(A,M) = \operatorname{Der}_R(A,M) / \operatorname{Inn.Der}_R(A,M)$.

PROOF. The sequence of left A^e-modules

$$0 \to J_{A/R} \to A^e \xrightarrow{\mu} A \to 0$$

is exact (Eq.(1.5)). Consider the associated long exact sequence

$$0 \to \operatorname{Hom}_{A^e}(A,M) \to \operatorname{Hom}_{A^e}(A^e,M) \to \operatorname{Hom}_{A^e}(J_{A/R},M) \xrightarrow{\delta^0}$$
$$\operatorname{Ext}^1_{A^e}(A,M) \to \operatorname{Ext}^1_{A^e}(A^e,M) \to \operatorname{Ext}^1_{A^e}(J_{A/R},M) \to$$

of abelian groups (Proposition 8.3.9 (2)). Since A^e is projective over A^e, it follows from Proposition 8.3.9 (3) that $\operatorname{Ext}^1_{A^e}(A^e,M) = 0$. The rest follows from Proposition 10.1.6. $\square$

THEOREM 10.1.9. *Let R be a commutative ring and A an R-algebra. The following are equivalent.*

(1) A is a separable R-algebra.

(2) $\mathrm{H}^1(A,M) = 0$ *for every two-sided A/R-module M.*

(3) The sequence

$$0 \to M^A \to M \xrightarrow{\tau} \operatorname{Der}_R(A,M) \to 0$$

is exact, for every two-sided A/R-module M.

PROOF. (1) is equivalent to (2): Let $A^e = A \otimes_R A^o$ be the enveloping algebra. By Definition 5.1.3, A is R-separable if and only if A is projective as a left A^e-module. By Proposition 8.3.9 (3), A is projective as a left A^e-module if and only if $\mathrm{H}^1(A,M) = \operatorname{Ext}^1_{A^e}(A,M) = 0$ for every two-sided A/R-module M.

(2) is equivalent to (3): This follows from an application of Proposition 10.1.6 and Lemma 10.1.8. $\square$

We now prove a faithfully flat descent theorem for separability.

THEOREM 10.1.10. *Let A be an R-algebra and S a commutative faithfully flat R-algebra. Assume $A \otimes_R S$ is separable over S and either*

(1) A is a finitely generated R-module, or

(2) A a finitely generated commutative R-algebra.

Then A is separable over R.

PROOF. By Lemma 10.1.5, A is finitely presented as an A^e-module. By Proposition 3.5.9, the functors $\operatorname{Hom}_{A^e}(A,\cdot)\otimes_R S$ and $\operatorname{Hom}_{A^e\otimes_R S}(A\otimes_R S,(\cdot)\otimes_R S)$ are isomorphic. By Corollary 5.1.8, the functor $\operatorname{Hom}_{A^e\otimes_R S}(A\otimes_R S,\cdot)$ is exact. Since S is faithfully flat, it follows that $\operatorname{Hom}_{A^e}(A,\cdot)$ is exact. By Corollary 5.1.8 again, A is separable over R. □

The next theorem provides sufficient conditions allowing us to prove that an algebra is separable if it is separable when localized at every prime.

THEOREM 10.1.11. *Let R be a commutative ring and A an R-algebra which satisfies either*

(a) *A is a finitely generated R-module, or*
(b) *A a finitely generated commutative R-algebra.*

Then the following are equivalent.

(1) A is a separable R-algebra.
(2) $A\otimes_R R_P$ is a separable R_P-algebra for every prime ideal P of R.
(3) $A\otimes_R R_{\mathfrak{m}}$ is a separable $R_{\mathfrak{m}}$-algebra for every maximal ideal $\mathfrak{m}$ of R.

PROOF. (1) implies (2): This follows straight from Corollary 5.3.2.
(2) implies (3): This is trivial.
(3) implies (1): By Proposition 5.1.2 (2), it suffices to show that sequence

$$0\to J_{A/R}\to A^e\xrightarrow{\mu} A\to 0$$

of left A^e-modules is split exact. By Exercise 2.4.9, it is enough to show that $\mu\circ(\,):\operatorname{Hom}_{A^e}(A,A^e)\to\operatorname{Hom}_{A^e}(A,A)$ is onto. By Lemma 10.1.5, A is of finite presentation as a left A^e-module. Let $\mathfrak{m}$ be any maximal ideal of R. Denote by $A_{\mathfrak{m}}$ the tensor product $A\otimes_R R_{\mathfrak{m}}$. By Lemma 10.1.2, $A^e\otimes_R R_{\mathfrak{m}}=A^e_{\mathfrak{m}}$. The diagram

$$\begin{tikzcd}
\operatorname{Hom}_{A^e}(A,A^e)\otimes_R R_{\mathfrak{m}} \arrow[r, "\mu\circ(\,)\otimes 1"] \arrow[d] & \operatorname{Hom}_{A^e}(A,A)\otimes_R R_{\mathfrak{m}} \arrow[d] \\
\operatorname{Hom}_{A^e_{\mathfrak{m}}}(A_{\mathfrak{m}},A^e_{\mathfrak{m}}) \arrow[r, "\mu\circ(\,)"] & \operatorname{Hom}_{A^e_{\mathfrak{m}}}(A_{\mathfrak{m}},A_{\mathfrak{m}})
\end{tikzcd}$$

commutes. The vertical maps are isomorphisms, by Proposition 3.5.9. By Corollary 5.1.8, the second horizontal map $\mu\circ(\,)$ is onto. Hence the top horizontal map is onto. By Exercise 3.5.1, $\mu\circ(\,):\operatorname{Hom}_{A^e}(A,A^e)\to\operatorname{Hom}_{A^e}(A,A)$ is onto. □

For an R-algebra A that is a finitely generated R-module, the next theorem and its corollaries show that separability of A over R can be reduced to the same question for certain algebras over fields. Separable algebras over fields are described by the decomposition theorems of Section 5.5.

THEOREM 10.1.12. *Let R be a commutative ring and A an R-algebra which is finitely generated as an R-module. The following are equivalent.*

(1) A is a separable R-algebra.
(2) $A/\mathfrak{m}A$ is a separable $R/\mathfrak{m}$-algebra for every maximal ideal $\mathfrak{m}$ of R.

PROOF. (1) implies (2): This follows straight from Corollary 5.3.2.

(2) implies (1): Let $\mathfrak{m}$ be any maximal ideal of R. Since $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} \cong R/\mathfrak{m}$ we have

$$\begin{aligned}(A \otimes_R R_{\mathfrak{m}})/\mathfrak{m}(A \otimes_R R_{\mathfrak{m}}) &\cong A \otimes_R (R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}})\\ &\cong A \otimes_R (R/\mathfrak{m})\\ &\cong A/\mathfrak{m}A.\end{aligned}$$

Since we already proved that (3) implies (1) in Theorem 10.1.11, it is enough to prove (2) implies (1) when R is a local ring.

Assume R is a local ring with maximal ideal $\mathfrak{m}$ and A is an R-algebra which is finitely generated as an R-module and such that $A/\mathfrak{m}A$ is separable over $R/\mathfrak{m}$. For the remainder of this proof, we write simply $J_{A/\mathfrak{m}A}$ instead of $J_{(A/\mathfrak{m}A)/(R/\mathfrak{m})}$ and J_A rather than $J_{A/R}$. Let $\delta : A/\mathfrak{m}A \to J_{A/\mathfrak{m}A}$ be the derivation defined by $\bar{a} \mapsto \bar{a} \otimes 1 - 1 \otimes \bar{a}$. By Theorem 10.1.9, $\delta = \tau_{\bar{z}}$ for some $\bar{z} \in J_{A/\mathfrak{m}A}$. In other words, for each $\bar{a} \in A/\mathfrak{m}A$, $\delta(\bar{a}) = \bar{a}\bar{z} - \bar{z}\bar{a} = (\bar{a} \otimes 1 - 1 \otimes \bar{a})\bar{z} = \delta(\bar{a})\bar{z}$. By Lemma 10.1.4, it follows that

$$J_{A/\mathfrak{m}A} = (A/\mathfrak{m}A)\delta(A/\mathfrak{m}A) = (A/\mathfrak{m}A)\delta(A/\mathfrak{m}A)\bar{z} = J_{A/\mathfrak{m}A}\bar{z}.$$

By Lemma 10.1.2, $J_{A/\mathfrak{m}A} = J_A/(\mathfrak{m}J_A)$. If $z \in J_A$ is a preimage of $\bar{z}$, then $J_A = J_A z + \mathfrak{m}J_A$. In Lemma 10.1.5 it was shown that J_A is finitely generated over R. By Nakayama's Lemma (Theorem 4.2.3), it follows that $J_A = J_A z$. Define a homomorphism ϕ in $\operatorname{Hom}_{A^e}(A^e, J_A)$ by $\phi(x) = xz$. Then $\phi(J_A) = J_A z = J_A$. By Corollary 2.4.2, $\phi : J_A \to J_A$ is an automorphism of A^e-modules. Therefore sequence (1.1) is split exact as A^e-modules. □

EXAMPLE 10.1.13. Let R be a commutative ring and $f \in R[x]$ a monic polynomial. We proved in Proposition 5.6.2 that $S = R[x]/(f)$ is separable over R if and only if $(f, f') = R[x]$. In this example, we apply the Residue Field Criterion to give another proof that S/R is separable if $(f, f') = R[x]$. Since f is monic, S is a free R-module of finite rank. By Theorem 10.1.12, S/R is separable if and only if $S \otimes_R k_{\mathfrak{m}} = k_{\mathfrak{m}}[x]/(f)$ is separable over $k_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ in R, where $k_{\mathfrak{m}}$ denotes the residue field $R/\mathfrak{m}$. By Exercise 5.5.1, $k_{\mathfrak{m}}[x]/(f)$ is separable over $k_{\mathfrak{m}}$ if and only if (f, f') is the unit ideal in $k_{\mathfrak{m}}[x]$. If (f, f') is the unit ideal in $R[x]$, then for every maximal ideal $\mathfrak{m}$, (f, f') is the unit ideal in $k_{\mathfrak{m}}[x]$ and we are done.

COROLLARY 10.1.14. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field k. The change of base functor $(\ ) \otimes_R k$ from the category of commutative separable R-algebras which are finitely generated free R-modules and the category of commutative separable k-algebras is essentially surjective.*

PROOF. A commutative separable k-algebra is a direct sum $F_1 \oplus \cdots \oplus F_n$, where each F_i is a finite separable field extension of k (Corollary 5.5.9). Let F/k be a finite separable field extension. To show $(\ ) \otimes_R k$ is essentially surjective, it is enough to show that $F = S \otimes_R k$, for an appropriate extension S/R. By Theorem 5.5.8, and Corollary 5.6.3, we are done. □

1.4. Exercises.

EXERCISE 10.1.8. This exercise is based on [**26**, Proposition I.3.1, p. 2] and [**44**, Proposition I.3.5] Let R be a commutative ring and S a commutative finitely generated R-algebra. Show that the following are equivalent.

(1) S is a separable R-algebra.
(2) The homomorphism of R-algebras $\mu : S^e \to S$ makes S into a flat S^e-module.

(3) For every $\mathfrak{q} \in \operatorname{Spec} S$, if $\mathfrak{p} = \mu^{-1}(\mathfrak{q})$, then $\mu : (S^e)_{\mathfrak{p}} \to S_{\mathfrak{q}}$ is an isomorphism. In the terminology of Algebraic Geometry, the diagonal morphism $\mu^\sharp : \operatorname{Spec} S \to \operatorname{Spec} S^e$ is said to be an open immersion (Exercise 3.5.18).

(Hint: Exercise 3.2.1 and Proposition 3.7.2.)

EXERCISE 10.1.9. Let R be a commutative ring and S a commutative R-algebra. In Algebraic Geometry, the morphism $\mu^\sharp : \operatorname{Spec} S \to \operatorname{Spec} S \otimes_R S$ associated to $\mu : S \otimes_R S \to S$ is called the *diagonal morphism*.

(1) For every $\mathfrak{q} \in \operatorname{Spec} S$, show that $\mu^{-1}(\mathfrak{q})$ is the ideal $\mathfrak{q} \otimes S + S \otimes \mathfrak{q} + J_{S/R}$.
(2) Let k be an algebraically closed field. Let $\alpha \in k$ and let $\mathfrak{q}$ be the maximal ideal in $k[x]$ generated by $x - \alpha$. Show that under the diagonal map $\mu^\sharp : \operatorname{Spec} k[x] \to \operatorname{Spec} k[x] \otimes_k k[x]$, the image of $\mathfrak{q}$ is the maximal ideal in $k[x] \otimes_k k[x]$ generated by $(x - \alpha) \otimes 1$ and $1 \otimes (x - \alpha)$.

EXERCISE 10.1.10. (An Open Immersion is Separable) Let $f : R \to S$ be a homomorphism of commutative rings. Show that if the continuous map $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is an open immersion (see Exercise 3.5.18), then S is separable over R. (Use Corollary 3.5.17 to show S is a finitely generated R-algebra.)

2. Differentials

This section contains an introduction to the module of Kähler differentials associated to a commutative R-algebra. The module of differentials is defined and its fundamental properties are proved. These results are applied in Section 10.2.2 to derive new tests for separability, in Section 10.3.2 to study separably generated field extensions, and in Section 11.6 to derive new tests for regularity.

2.1. The Definition and Fundamental Exact Sequences. A general reference for this section is [**41**]. Let A be a commutative R-algebra and $A^e = A \otimes_R A$. The multiplication map $a \otimes b \mapsto ab$ induces a homomorphism of R-algebras $\mu : A \otimes_R A \to A$ (see Exercise 2.3.11). As in Eq.(1.5), the kernel of μ is denoted $J_{A/R}$ and there is an exact sequence of A^e-modules

$$0 \to J_{A/R} \to A^e \xrightarrow{\mu} A \to 0.$$

Using the R-algebra homomorphism $\rho : A \to A^e$ defined by $a \mapsto a \otimes 1$, we turn A^e into a left A-module. Consequently $J_{A/R}$ and $J^2_{A/R}$ are also A-modules. Let $\Omega_{A/R}$ be defined by the exact sequence

$$0 \to J^2_{A/R} \to J_{A/R} \xrightarrow{\pi} \Omega_{A/R} \to 0.$$

The left A-module $\Omega_{A/R}$ is called the *module of Kähler differentials*. As in Example 10.1.3, there is an R-derivation $\delta : A \to J_{A/R}$ defined by $a \mapsto a \otimes 1 - 1 \otimes a$. Let $d_{A/R} = \pi\delta$. The reader should verify that $d_{A/R} : A \to \Omega_{A/R}$ is an R-derivation. The derivation $d_{A/R}$, together with the module of Kähler differentials satisfies a universal mapping property. In Theorem 10.2.1, a left A-module is made into a two-sided A/R-module by making the right multiplication agree with the left multiplication. An R-module homomorphism $\partial : A \to M$ is an R-derivation of A, if $\partial(ab) = a\partial(b) + b\partial(a)$, for all $a, b \in A$.

THEOREM 10.2.1. *Let A be a commutative R-algebra. For any left A-module M, if $\partial : A \to M$ is an R-derivation of A, then there exists a unique A-module homomorphism*

$f : \Omega_{A/R} \to M$ such that the diagram

$$\begin{tikzcd}
A \arrow[rr, "\partial"] \arrow[dr, "d_{A/R}"'] & & M \\
& \Omega_{A/R} \arrow[ur, dashed, "\exists f"'] &
\end{tikzcd}$$

commutes. The assignment $f \mapsto f d_{A/R}$ defines an isomorphism of A-modules $\operatorname{Hom}_A(\Omega_{A/R}, M) \cong \operatorname{Der}_R(A, M)$.

PROOF. The exact sequence

$$J_{A/R} \xrightarrow{\pi} \Omega_{A/R} \to 0$$

gives rise to the exact sequence

$$0 \to \operatorname{Hom}_A(\Omega_{A/R}, M) \to \operatorname{Hom}_A(J_{A/R}, M).$$

Let $f \in \operatorname{Hom}_A(\Omega_{A/R}, M)$. For any $a, b, x \in A$,

$$\begin{aligned}
(f\pi)\big((a \otimes b)(x \otimes 1 - 1 \otimes x)\big) &= (f\pi)\Big(\big(a(1 \otimes b - b \otimes 1) \\
&\qquad + ab \otimes 1\big)(x \otimes 1 - 1 \otimes x)\Big) \\
&= (f\pi)\big(a(1 \otimes b - b \otimes 1)(x \otimes 1 - 1 \otimes x) \\
&\qquad + ab(x \otimes 1 - 1 \otimes x)\big) \\
&= f\big(ab(x \otimes 1 - 1 \otimes x)\big) \\
&= abf(x \otimes 1 - 1 \otimes x).
\end{aligned}$$

This means $f\pi$ is in $\operatorname{Hom}_{A^e}(J_{A/R}, M)$, so the sequence

$$0 \to \operatorname{Hom}_A(\Omega_{A/R}, M) \xrightarrow{\zeta} \operatorname{Hom}_{A^e}(J_{A/R}, M)$$

is exact. Let $g \in \operatorname{Hom}_{A^e}(J_{A/R}, M)$. For all $a, b \in A$,

$$\begin{aligned}
g\big((a \otimes 1 - 1 \otimes a)(b \otimes 1 - 1 \otimes b)\big) &= g\big(a \otimes 1(b \otimes 1 - 1 \otimes b)\big) \\
&\quad - g\big(1 \otimes a(b \otimes 1 - 1 \otimes b)\big) \\
&= ag(b \otimes 1 - 1 \otimes b) - g(b \otimes 1 - 1 \otimes b)a \\
&= 0.
\end{aligned}$$

Since g annihilates $J^2_{A/R}$, there exists $f : \Omega_{A/R} \to M$ such that $g = f\pi$. This proves ζ is an isomorphism. Combined with Proposition 10.1.6, this shows that there is an isomorphism $\operatorname{Hom}_A(\Omega_{A/R}, M) \cong \operatorname{Der}_R(A, M)$ which is defined by $f \mapsto f\pi\delta$. Because A is commutative, the maps are A-linear. □

PROPOSITION 10.2.2. *Let S be a commutative R-algebra which is generated as an R-algebra by the set $X = \{x_i\}_{i \in I}$. Then*

1. *$\Omega_{S/R}$ is generated as an S-module by $d_{S/R}(X) = \{d_{S/R}x_i\}_{i \in I}$.*
2. *If S is a polynomial ring over R (that is, if X is a set of indeterminates), then $\Omega_{S/R}$ is a free S-module with basis $d_{S/R}(X)$.*
3. *If S is a finitely generated R-algebra, then $\Omega_{S/R}$ is a finitely generated S-module.*

PROOF. Part (3) follows directly from Part (1).

(1): By Lemma 10.1.5, $J_{S/R}$ is generated as an S^e-module by the set $\delta(X) = \{x_i \otimes 1 - 1 \otimes x_i\}_{i \in I}$. Let $\pi : J_{S/R} \to J_{S/R}/J^2_{S/R}$ be the natural map. Given any $a, b \in S$ and $x \in X$,

$$\begin{aligned}\pi\big(a \otimes b(x \otimes 1 - 1 \otimes x)\big) &= \pi\big((a(1 \otimes b - b \otimes 1) + (ab \otimes 1))(x \otimes 1 - 1 \otimes x)\big)\\ &= \pi\big(a(1 \otimes b - b \otimes 1)(x \otimes 1 - 1 \otimes x)\big)\\ &\quad + \pi\big((ab \otimes 1)(x \otimes 1 - 1 \otimes x)\big)\\ &= \pi\big((ab \otimes 1)(x \otimes 1 - 1 \otimes x)\big).\end{aligned}$$

It follows from this that $\Omega_{S/R} = J_{S/R}/J^2_{S/R}$ is generated as a left S-module by the set $\pi\delta(X) = d_{S/R}(X)$.

(2): For each $i \in I$, let $\partial_i : S \to S$ represent the "partial derivative with respect to x_i" function. By the Universal Mapping Property (Theorem 10.2.1), there exists a unique $b_i \in \operatorname{Hom}_S(\Omega_{S/R}, S)$ such that for all $j \in I$

$$b_i d_{S/R} x_j = \partial_i x_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Suppose $\sum_j s_j d_{S/R} x_j = 0$ is a finite dependence relation in $\Omega_{S/R}$ where each $s_j \in S$. Applying b_i we see that $s_i = 0$. $\square$

2.1.1. *The Fundamental Exact Sequences.* Now we derive the so-called fundamental exact sequences for the module of differentials.

THEOREM 10.2.3. *(The First Fundamental Exact Sequence) Let S be a commutative R-algebra and A a commutative S-algebra.*

(1) There is an exact sequence of natural homomorphisms of A-modules

$$\Omega_{S/R} \otimes_S A \xrightarrow{a} \Omega_{A/R} \xrightarrow{b} \Omega_{A/S} \to 0.$$

(2) There is a split exact sequence of natural homomorphisms of A-modules

$$0 \to \Omega_{S/R} \otimes_S A \xrightarrow{a} \Omega_{A/R} \xrightarrow{b} \Omega_{A/S} \to 0$$

if and only if given any A-module M and any R-derivation $\partial : S \to M$, there exists an R-derivation $D : A \to M$ such that the diagram

$$\begin{tikzcd} S \arrow[rr, "\partial"] \arrow[dr] & & M \\ & A \arrow[ur, dashed, "D"'] & \end{tikzcd}$$

commutes.

PROOF. (1): Step 1: Define the map a. By Exercise 10.2.1, the commutative diagram of commutative rings

$$\begin{tikzcd} R \arrow[r] \arrow[d] & R \arrow[d] \\ S \arrow[r] & A \end{tikzcd}$$

induces a natural homomorphism of A-modules $a : \Omega_{S/R} \otimes_S A \to \Omega_{A/R}$.

Step 2: Define the map b. Again, by Exercise 10.2.1, the commutative diagram of commutative rings

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ A & \longrightarrow & A \end{array}$$

induces a natural homomorphism of A-modules $b : \Omega_{A/R} \to \Omega_{A/S}$.

Step 3: b is onto. A generating set for A as an R-algebra is a generating set for A as an S-algebra. It is evident that b is onto, by Proposition 10.2.2.

Step 4: The sequence is a complex. In the commutative diagram

$$\begin{array}{ccc} S & \longrightarrow & A \\ {\scriptstyle d_{S/R}}\downarrow & & \downarrow{\scriptstyle d_{A/S}} \\ \Omega_{S/R} & \xrightarrow{c} & \Omega_{A/S} \end{array}$$

c is the zero map. Therefore, $ba = 0$.

Step 5: $\ker b = \operatorname{im} a$. By Lemma 2.4.6, this is true if

(2.1) $$0 \to \operatorname{Hom}_A(\Omega_{A/S}, M) \xrightarrow{\mathrm{H}_b} \operatorname{Hom}_A(\Omega_{A/R}, M) \xrightarrow{\mathrm{H}_a} \operatorname{Hom}_A(\Omega_{S/R} \otimes_S A, M)$$

is exact for all A-modules M. By the adjoint isomorphism of Theorem 2.4.10 and Theorem 10.2.1, (2.1) is naturally isomorphic to

$$0 \to \operatorname{Der}_S(A, M) \to \operatorname{Der}_R(A, M) \to \operatorname{Der}_R(S, M)$$

which is exact, by Exercise 10.1.4.

(2): By Exercise 2.4.2, there is a left inverse for a if and only if for all all A-modules M, the map H_a in (2.1) is onto. Equivalently, $\operatorname{Der}_R(A, M) \to \operatorname{Der}_R(S, M) \to 0$ is exact, for all A-modules M. □

Let R be a commutative ring and S a commutative R-algebra. Let I be an ideal of S and set $A = S/I$. Define a function $\gamma : I \to \Omega_{S/R} \otimes_S A$ by $x \mapsto d_{S/R}x \otimes 1$. If $x, y \in I$, then $\gamma(xy) = xd_{S/R}y \otimes 1 + yd_{S/R}x \otimes 1 = d_{S/R}y \otimes x + d_{S/R}x \otimes y = 0$. Therefore, γ factors through I^2 and we have the A-module homomorphism (also denoted by γ)

$$\gamma : I/I^2 \to \Omega_{S/R} \otimes_S A.$$

THEOREM 10.2.4. *(The Second Fundamental Exact Sequence) Let S be a commutative R-algebra, I an ideal in S, and $A = S/I$. The sequence of A-modules*

$$I/I^2 \xrightarrow{\gamma} \Omega_{S/R} \otimes_S A \xrightarrow{a} \Omega_{A/R} \to 0$$

is exact.

PROOF. Step 1: a is onto and the sequence is a complex. By Exercise 10.2.1, the diagram

$$\begin{array}{ccc} S & \xrightarrow{\theta} & A \\ {\scriptstyle d_{S/R}}\downarrow & & \downarrow{\scriptstyle d_{A/R}} \\ \Omega_{S/R} & \xrightarrow{a} & \Omega_{A/R} \end{array}$$

commutes. Since θ is onto and the vertical maps are onto, a is onto. If $x \in I$, then $d_{A/R}\theta(x) = 0$, hence $\operatorname{im}\gamma \subseteq \ker a$.

Step 2: $\operatorname{im}\gamma = \ker a$. As in the proof of Theorem 10.2.3, it suffices to prove

$$0 \to \operatorname{Hom}_A(\Omega_{A/R}, M) \xrightarrow{\mathrm{H}_a} \operatorname{Hom}_A(\Omega_{S/R} \otimes_S A, M) \xrightarrow{\mathrm{H}_\gamma} \operatorname{Hom}_A(I/I^2, M)$$

is exact, for every A-module M. By the adjoint isomorphism of Theorem 2.4.10 and Theorem 10.2.1, this last sequence is isomorphic to

$$0 \to \operatorname{Der}_R(A, M) \to \operatorname{Der}_R(S, M) \to \operatorname{Hom}_S(I, M).$$

The reader should verify that this last sequence is exact. □

2.2. More Tests for Separability. In this section ideas from Section 10.2 are applied to derive separability criteria for commutative R-algebras. For example, for a finitely generated algebra, the vanishing of the module of Kähler differentials is equivalent to being separable (Theorem 10.2.5). As an application, we prove the Jacobian Criterion for Separability (Proposition 10.2.7). General references for the material in this section are [**18**], [**36**] and [**48**].

THEOREM 10.2.5. *Let S be a commutative finitely generated R-algebra. The following are equivalent.*

(1) S is a separable R-algebra.
(2) $\operatorname{Der}_R(S, M) = 0$ for every left S-module M.
(3) $\Omega_{S/R} = 0$.

PROOF. (3) implies (2): This follows from Theorem 10.2.1.

(2) implies (3): If $\operatorname{Der}_R(S, \Omega_{S/R}) = 0$, then $\operatorname{Hom}_S(\Omega_{S/R}, \Omega_{S/R}) = 0$, by Theorem 10.2.1. From this we conclude that $\Omega_{S/R} = 0$.

(1) implies (3): By Proposition 5.1.2, $J_{S/R}$ is an idempotent generated ideal in S^e. Therefore, $J_{S/R}^2 = J_{S/R}$, by Exercise 2.2.11 (1).

(3) implies (1): This is the only part of the proof where we need to assume S is finitely generated. By Lemma 10.1.5, $J_{S/R}$ is a finitely generated ideal of S^e. We are given that $J_{S/R}^2 = J_{S/R}$. It follows from Exercise 2.2.11 (2) and Proposition 5.1.2 that S/R is separable. □

THEOREM 10.2.6. *Let S be a commutative finitely generated R-algebra with structure homomorphism $\theta : R \to S$. The following are equivalent.*

(1) S is a separable R-algebra.
(2) For every $\mathfrak{p} \in \operatorname{Spec} R$, if $k_\mathfrak{p} = R_\mathfrak{p}/(\mathfrak{p}R_\mathfrak{p})$, then $S \otimes_R k_\mathfrak{p}$ is a separable $k_\mathfrak{p}$-algebra.
(3) For every $\mathfrak{p} \in \operatorname{Spec} R$, and every $\mathfrak{q} \in \operatorname{Spec} S$ such that $\mathfrak{p} = \theta^{-1}(\mathfrak{q})$, $\mathfrak{p}S_\mathfrak{q} = \mathfrak{q}S_\mathfrak{q}$, and $k_\mathfrak{q} = S_\mathfrak{q}/(\mathfrak{q}S_\mathfrak{q})$ is a finite separable extension of the field $k_\mathfrak{p} = R_\mathfrak{p}/(\mathfrak{p}R_\mathfrak{p})$.
(4) For every algebraically closed field F and homomorphism of rings $\phi : R \to F$, $S \otimes_R F$ is a separable F-algebra.

PROOF. (1) implies (2): This follows directly from Corollary 5.3.2.

(1) implies (4): This follows directly from Corollary 5.3.2.

(4) implies (2): Let $\mathfrak{p} \in \operatorname{Spec} R$. Let F be the algebraic closure of $k_\mathfrak{p} = R_\mathfrak{p}/(\mathfrak{p}R_\mathfrak{p})$ and $\phi : R \to F$ the natural map. By assumption, $S \otimes_R F$ is separable over F. Corollary 5.3.5 implies $S \otimes_R k_\mathfrak{p}$ is separable over $k_\mathfrak{p}$.

(2) implies (1): By Proposition 10.2.2, $\Omega_{S/R}$ is a finitely generated S-module. By Theorem 10.2.5, to finish the proof it is enough to show $\Omega_{S/R} = 0$. By Proposition 3.1.9, it is enough to show $\Omega_{S/R} \otimes_S S_\mathfrak{q} = 0$ for every $\mathfrak{q} \in \operatorname{Spec} S$. Fix $\mathfrak{q} \in \operatorname{Spec} S$ and let $\mathfrak{p} = \mathfrak{q} \cap R$. Since $\left(\Omega_{S/R}\right)_\mathfrak{q} = \Omega_{S/R} \otimes_S S_\mathfrak{q}$ is finitely generated over $S_\mathfrak{q}$ and $\mathfrak{m}_\mathfrak{p} \subseteq \mathfrak{m}_\mathfrak{q}$, by Theorem 4.2.3

(Nakayama's Lemma), it is enough to show $\left(\Omega_{S/R}\right)_{\mathfrak{q}}/\mathfrak{m}_{\mathfrak{p}}\left(\Omega_{S/R}\right)_{\mathfrak{q}}=0$. By Exercise 10.2.2, $\Omega_{S/R}\otimes_R k_{\mathfrak{p}}=\Omega_{S\otimes_R k_{\mathfrak{p}}/k_{\mathfrak{p}}}$, and by Theorem 10.2.5, $\Omega_{S\otimes_R k_{\mathfrak{p}}/k_{\mathfrak{p}}}=0$. The reader should verify that

$$\begin{aligned}
\left(\Omega_{S/R}\right)_{\mathfrak{q}}/\mathfrak{m}_{\mathfrak{p}}\left(\Omega_{S/R}\right)_{\mathfrak{q}} &= \left(\Omega_{S/R}\right)_{\mathfrak{q}}\otimes_{R_{\mathfrak{p}}} R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}\\
&= \left(\Omega_{S/R}\right)_{\mathfrak{q}}\otimes_R k_{\mathfrak{p}}\\
&\cong S_{\mathfrak{q}}\otimes_S \Omega_{S/R}\otimes_R k_{\mathfrak{p}}\\
&\cong S_{\mathfrak{q}}\otimes_S \Omega_{S\otimes_R k_{\mathfrak{p}}/k_{\mathfrak{p}}}\\
&= 0.
\end{aligned}$$

(1) implies (3): Assume S is R-separable, $\mathfrak{q}\in\operatorname{Spec}S$ and $\mathfrak{p}=\mathfrak{q}\cap R$. By Exercise 5.4.1, $S_{\mathfrak{q}}$ is separable over $R_{\mathfrak{p}}$. By Exercise 5.5.4, $\mathfrak{m}_{\mathfrak{p}}S_{\mathfrak{q}}=\mathfrak{m}_{\mathfrak{q}}$ and $k_{\mathfrak{q}}=S_{\mathfrak{q}}\otimes_R k_{\mathfrak{p}}$ is a separable field extension of $k_{\mathfrak{p}}$.

(3) implies (2): Fix $\mathfrak{p}\in\operatorname{Spec}R$ such that there exists some $\mathfrak{q}\in\operatorname{Spec}S$ and $\mathfrak{p}=\mathfrak{q}\cap R$. By Exercise 3.1.11, $\mathfrak{q}_{\mathfrak{p}}=\mathfrak{q}\otimes_R R_{\mathfrak{p}}$ is a prime ideal of $S_{\mathfrak{p}}=S\otimes_R R_{\mathfrak{p}}$ and the local ring of $S_{\mathfrak{p}}$ at $\mathfrak{q}_{\mathfrak{p}}$ is $S_{\mathfrak{q}}$. By Exercise 3.1.6, $S_{\mathfrak{p}}/\mathfrak{q}_{\mathfrak{p}}$ is an integral domain with quotient field $k_{\mathfrak{q}}=S_{\mathfrak{q}}/\mathfrak{m}_{\mathfrak{q}}$. The diagram

$$\begin{tikzcd}
S_{\mathfrak{p}}/\mathfrak{q}_{\mathfrak{p}} \arrow[r] & k_{\mathfrak{q}}\\
R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} \arrow[u] \arrow[r, "="] & k_{\mathfrak{p}} \arrow[u]
\end{tikzcd}$$

commutes. By hypothesis, $k_{\mathfrak{q}}/k_{\mathfrak{p}}$ is a finite dimensional field extension. It follows from Lemma 6.1.4 that $S_{\mathfrak{p}}/\mathfrak{q}_{\mathfrak{p}}$ is a field. That is, $\mathfrak{q}_{\mathfrak{p}}$ is a maximal ideal in $S_{\mathfrak{p}}$. It follows from Exercise 3.4.2 that every prime ideal in $S\otimes_R k_{\mathfrak{p}}$ is a maximal ideal, and moreover each maximal ideal is of the form $\mathfrak{q}\otimes_R k_{\mathfrak{p}}$ for some $\mathfrak{q}$ lying over $\mathfrak{p}$. Because $S\otimes_R k_{\mathfrak{p}}$ is finitely generated as a $k_{\mathfrak{p}}$-algebra, $S\otimes_R k_{\mathfrak{p}}$ is noetherian by the Hilbert Basis Theorem (Theorem 6.2.1). By Proposition 4.5.4, $S\otimes_R k_{\mathfrak{p}}$ is artinian. By Theorem 4.5.6, if $\operatorname{Max}(S\otimes_R k_{\mathfrak{p}})=\{\mathfrak{n}_1,\dots,\mathfrak{n}_n\}$, then $S\otimes_R k_{\mathfrak{p}}=(S\otimes_R k_{\mathfrak{p}})_{\mathfrak{n}_1}\oplus\cdots\oplus(S\otimes_R k_{\mathfrak{p}})_{\mathfrak{n}_n}$. Suppose $\mathfrak{n}_i=\mathfrak{q}_i\otimes_R k_{\mathfrak{p}}$ is an arbitrary maximal ideal of $S\otimes_R k_{\mathfrak{p}}$. By Exercise 3.4.2,

$$(S\otimes_R k_{\mathfrak{p}})_{\mathfrak{n}_i}=(S\otimes_R k_{\mathfrak{p}})_{\mathfrak{q}_i\otimes_R k_{\mathfrak{p}}}=S_{\mathfrak{q}_i}/\mathfrak{m}_{\mathfrak{p}}S_{\mathfrak{q}_i}=S_{\mathfrak{q}_i}/\mathfrak{m}_{\mathfrak{q}_i}=k_{\mathfrak{q}_i}.$$

This proves that $S\otimes_R k_{\mathfrak{p}}\cong k_{\mathfrak{q}_1}\oplus\cdots\oplus k_{\mathfrak{q}_n}$ and by Corollary 5.5.9, we are done. $\square$

We conclude this section with a proof of a jacobian criterion for separability. For computations it turns out to be one of the most useful tests for separability. Proposition 10.2.7 is a generalization of Proposition 5.6.2.

PROPOSITION 10.2.7. *Let R be a commutative ring. Let $I=(f_1,\dots,f_n)$ be an ideal in $S=R[x_1,\dots,x_n]$ generated by a set of n polynomials in n indeterminates. Then S/I is separable over R if and only if the determinant of the jacobian matrix $(\partial f_i/\partial x_j)$ maps to a unit in S/I.*

PROOF. Let $A=S/I$. We use the notation of Theorem 10.2.4. The sequence

$$I/I^2\xrightarrow{\gamma}\Omega_{S/R}\otimes_S A\xrightarrow{a}\Omega_{A/R}\to 0$$

is exact. By Theorem 10.2.5, A/R is separable if and only if γ is onto. By Proposition 10.2.2, $\Omega_{S/R}\otimes_S A$ is a free A-module on the basis $\{dx_1,\dots,dx_n\}$. For each i,

$$\gamma(f_i)=\sum_{j=1}^{n}\frac{\partial f_i}{\partial x_j}dx_j.$$

Thus, $\Omega_{A/R}$ is isomorphic to the cokernel of the A-module homomorphism

$$A^{(n)} \xrightarrow{J} A^{(n)}$$

where J denotes multiplication by the jacobian matrix $(\partial f_i/\partial x_j)$. The matrix J is invertible if and only if the determinant of J is a unit (Lemma 1.7.5). By Corollary 2.4.2, if J is onto, then J is invertible. $\square$

2.3. An Application to Algebraic Varieties. Let k be a field and B a finitely generated k-algebra such that B is an integral domain with Krull dimension one. Let $\mathfrak{q}$ be a maximal ideal of B such that the local ring $B_{\mathfrak{q}}$ is a PID with maximal ideal $\mathfrak{m}(\mathfrak{q})$ and residue field $k(\mathfrak{q})$. Using Exercise 3.1.17 we see that there exists $\pi \in B$ such that $\mathfrak{m}(\mathfrak{q}) = \pi B_{\mathfrak{q}}$. Hence π is a local parameter for $B_{\mathfrak{q}}$ (see Theorem 11.2.10). Proposition 10.2.8 is from [**55**, Proposition II.1.4, p. 18].

PROPOSITION 10.2.8. *Let k be a field and B a finitely generated k-algebra such that B is an integral domain with Krull dimension one and quotient field L. Let $\mathfrak{q}$ be a maximal ideal in B such that $B_{\mathfrak{q}}$ is a PID with maximal ideal $\mathfrak{m}(\mathfrak{q})$ and residue field $k(\mathfrak{q})$. Let $\pi \in B$ such that $\mathfrak{m}(\mathfrak{q}) = \pi B_{\mathfrak{q}}$. Then π is transcendental over k, $k(\pi)$ is a subfield of L, and if $k(\mathfrak{q})$ is a separable extension of k, then L is a separable field extension of $k(\pi)$.*

PROOF. Since $\pi \in \mathfrak{q}$, π is not invertible in $B_{\mathfrak{q}}$. Therefore, the map $k[x] \to B_{\mathfrak{q}}$ defined by $x \mapsto \pi$, maps $k[x]$ isomorphically onto $k[\pi]$. So π is transcendental over k. Let $A = k[\pi] \subseteq B$. Let R be the local ring $A_{\mathfrak{p}}$, where $\mathfrak{p} = \pi A$. Then $A_{\mathfrak{p}}$ is a local PID with maximal ideal $\pi A_{\mathfrak{p}}$. We have the commutative diagram of subrings:

$$\begin{tikzcd}
 & & L \\
 & B_{\mathfrak{q}} \arrow[ur] & k(\pi) \arrow[u] \\
B \arrow[ur] & A_{\mathfrak{p}} \arrow[u] \arrow[ur] & \\
A = k[\pi] \arrow[u] \arrow[ur] & &
\end{tikzcd}$$

Since B is a finitely generated k-algebra, L is a finitely generated field extension of $k(\pi)$. By Corollary 10.3.3, L has transcendence degree 1 over k. Therefore, L is a finitely generated algebraic extension of $k(\pi)$. Let $S = B \otimes_A R$ the localization of B in L with respect to the multiplicative set $A - \mathfrak{p}$. Then S is a finitely generated R-algebra. Consider the tower of subrings $B \subseteq S \subseteq B_{\mathfrak{q}} \subseteq L$. By Corollary 9.7.6, $\operatorname{Spec} S$ is finite, and by Corollary 3.5.18, B_q is a finitely generated S-algebra. It follows that B_q is a finitely generated R-algebra. By Theorem 10.2.6, $B_{\mathfrak{q}}$ is a separable R-algebra. Then by Exercise 5.4.1, L is separable over $k(\pi)$. $\square$

Now we prove a converse to Proposition 10.2.8.

PROPOSITION 10.2.9. *Let k be a field, S/R an extension of finitely generated commutative k-algebras. Assume S and R are integral domains and let L/K be the corresponding extension of the fields of fractions. If L is a finitely generated separable extension field of K, then there exists a maximal ideal $\mathfrak{m} \in \operatorname{Max} S$ such that $S_{\mathfrak{m}}$ is separable over R.*

PROOF. Let U be the set of all points P in $\operatorname{Spec} S$ such that S_P is a separable R-algebra. By Exercise 10.2.5, U is an open subset of $\operatorname{Spec} S$. By Exercise 5.1.2, Proposition 5.5.6, and Theorem 5.4.2, L is separable over R. Therefore, U is an open neighborhood of (0). By Exercise 6.3.2, U contains a closed point of $\operatorname{Spec} S$. □

2.4. Exercises.

EXERCISE 10.2.1. Let

$$\begin{tikzcd} R \arrow[r] \arrow[d] & S \arrow[d] \\ A \arrow[r, "\theta"] & B \end{tikzcd}$$

be a commutative diagram of commutative rings. Show that there exists a unique homomorphism ψ such that the diagram

$$\begin{tikzcd} A \arrow[r, "\theta"] \arrow[d, "d_{A/R}"'] & B \arrow[d, "d_{B/S}"] \\ \Omega_{A/R} \arrow[r, dashed, "\exists\psi"] & \Omega_{B/S} \end{tikzcd}$$

of A-modules commutes. Show that ψ induces a homomorphism $\Omega_{A/R} \otimes_A B \to \Omega_{B/S}$ of B-modules.

EXERCISE 10.2.2. Suppose A and S are commutative R-algebras. Show that there exists a unique isomorphism ϕ such that the diagram

$$\begin{tikzcd} A \otimes_R S \arrow[rr, "d_{A/R}\otimes 1"] \arrow[dr, "d_{A\otimes_R S/S}"'] & & \Omega_{A/R} \otimes_R S \\ & \Omega_{A\otimes_R S/S} \arrow[ur, dashed, "\exists\phi"'] & \end{tikzcd}$$

of S-modules commutes. (Hint: The inverse of ϕ is constructed in Exercise 10.2.1.)

EXERCISE 10.2.3. Let A be a commutative R-algebra and $W \subseteq A$ a multiplicative set. Let A_W denote the localization $W^{-1}A$. Show that there exists an isomorphism of A_W-modules $\Omega_{A_W/R} \cong \Omega_{A/R} \otimes_A A_W = W^{-1}\Omega_{A/R}$. (Hint: Construct $\Omega_{A/R} \otimes_A A_W \to \Omega_{A_W/R}$ using Exercise 10.2.1.)

EXERCISE 10.2.4. Let R be a commutative ring and S a commutative R-algebra. Let $A = S[x_1,\dots,x_n]$ be the polynomial ring over S in n variables. Show that the sequence

$$0 \to \Omega_{S/R} \otimes_S A \xrightarrow{a} \Omega_{A/R} \xrightarrow{b} \Omega_{A/S} \to 0$$

is split exact.

EXERCISE 10.2.5. Let S be a finitely generated commutative R-algebra. Let U be the set of all points P in $\operatorname{Spec} S$ such that S_P is a separable R-algebra. Prove that U is an open (possibly empty) subset of $\operatorname{Spec} S$. (Hint: Apply Exercise 9.2.6 to $\Omega_{S/R}$.)

3. Noether Normalization

This section is devoted to proving Emmy Noether's Normalization Lemma. We actually prove two different versions. The first form appears in Corollary 10.3.3. In summary, it says that if A is a finitely generated commutative algebra over a field k with Krull dimension $\dim(A) = m$, then there is a subring S of A which is isomorphic to a polynomial ring in m variables over k and A is integral over S. Section 10.3.2 contains an introduction to the notion of separably generated field extensions. We prove a strong version of the Noether Normalization Lemma (Theorem 10.3.10) and apply it to prove the theorem on the finiteness of the integral closure of a finitely generated k-algebra (Theorem 10.3.11). General references for this section are [**18**], [**41**] and [**61**].

3.1. First Form of the Normalization Lemma.

THEOREM 10.3.1. *Let R be a commutative noetherian ring and $x_1,\dots,x_n$ some indeterminates.*

(1) $\dim(R[x_1,\dots,x_n]) = \dim(R) + n$.
(2) If R is a field, $\dim(R[x_1,\dots,x_n]) = n$ *and the ideal* $(x_1,\dots,x_j)$ *is a prime ideal of height j for all $j = 1,\dots,n$.*

PROOF. (2): Is left to the reader.

(1): It is enough to prove $\dim(R[x]) = \dim(R)+1$. For notational simplicity, write $S = R[x]$. Since S is a free R-module, it is a faithfully flat R-module. Therefore $\operatorname{Spec} S \to \operatorname{Spec} R$ is onto and going down holds. Let $P \in \operatorname{Spec} R$ and choose $Q \in \operatorname{Spec} S$ to be maximal among all primes lying over P. The prime ideals lying over P are in one-to-one correspondence with the elements of the fiber over P. But the fiber over P is $\operatorname{Spec}(R[x] \otimes_R k_P)$, which we can identify with $\operatorname{Spec}(k_P[x])$. The ring $k_P[x]$ is a PID, so a maximal ideal has height one. This proves $\operatorname{ht}(Q/PS) = 1$. If we pick $P \in \operatorname{Spec}(R)$ such that $\operatorname{ht}(P) = \dim(R)$, then by Theorem 9.6.16, $\dim(S) \ge \dim(S_Q) = \dim(R_P)+1 = \dim(R)+1$. Conversely, pick $Q \in \operatorname{Spec}(S)$ such that $\operatorname{ht}(Q) = \dim(S)$. Set $P = Q \cap R$. By Theorem 9.6.16, $\dim(S) = \dim(S_Q) = \dim(R_P)+1 \le \dim(R)+1$. □

THEOREM 10.3.2. *Let k be a field and $A = k[x_1,\dots,x_n]$. Let I be a nonunit ideal of A such that I has height r. There exist $y_1,\dots,y_n$ in A such that*

(1) the set $\{y_1,\dots,y_n\}$ is algebraically independent over k,
(2) A is integral over $k[y_1,\dots,y_n]$,
(3) $I \cap k[y_1,\dots,y_n] = (y_1,\dots,y_r)$, and
(4) $y_1,\dots,y_n$ can be chosen in such a way that for $1 \le j \le n-r$, $y_{r+j} = x_{r+j} + h_j(x_1,\dots,x_r)$, where h_j is a polynomial in the image of $\mathbb{Z}[x_1,\dots,x_r] \to A$. Moreover, if $\operatorname{char} k = p > 0$, *then h_j can be chosen to be in the image of $\mathbb{Z}[x_1^p,\dots,x_r^p] \to A$.*

PROOF. The proof is by induction on r. If $r = 0$, then $I = (0)$ because A is an integral domain. Take each y_i to be equal to x_i.

Step 1: $r = 1$. Pick $y_1 = f(x_1,\dots,x_n)$ to be any nonzero element in I. Write

$$y_1 = f(x_1,\dots,x_n) = \sum_{i=1}^{t} a_i f_i$$

as a sum of distinct monomials, where each a_i is an invertible element of k and $f_i = x_1^{e_{1i}} \cdots x_n^{e_{ni}}$. The exponents e_{ji} define t distinct monomials, hence they also define t distinct polynomials $q_i(z) = e_{1i} + e_{2i}z^2 + \cdots + e_{ni}z^n$ in $\mathbb{Z}[z]$. For some sufficiently large positive integer v, the values $q_1(v),\dots,q_t(v)$ are distinct. Define a weight function μ on the set of monomials in $k[x_1,\dots,x_n]$ by the rule $\mu(x_1^{e_1}\cdots x_n^{e_n}) = e_1 + e_2 v^2 + \cdots + e_n v^n$. So $\mu(f_1),\dots,\mu(f_t)$ are distinct positive integers. Without loss of generality, assume $\mu(f_1)$ is maximal. Set $y_2 = x_2 - x_1^{v^2},\dots,y_n = x_n - x_1^{v^n}$. Consider

$$\begin{aligned} y_1 &= f(x_1, y_2 + x_1^{v^2},\dots,y_n + x_1^{v^n}) \\ &= \sum_{i=1}^t a_i f_i(x_1, y_2 + x_1^{v^2},\dots,y_n + x_1^{v^n}) \\ &= \sum_{i=1}^t a_i x_1^{e_{1i}} (y_2 + x_1^{v^2})^{e_{2i}} \cdots (y_n + x_1^{v^n})^{e_{ni}} \\ &= \sum_{i=1}^t a_i \bigl(x_1^{\mu(f_i)} + g_i(x_1,y_2,\dots,y_n)\bigr) \end{aligned}$$

where each g_i is a polynomial in $k[x_1,y_2,\dots,y_n]$ and the degree of g_i in x_1 is less than $\mu(f_i)$. Assuming $\mu(f_1)$ is maximal, we can write

$$y_1 = a_1 x_1^{\mu(f_i)} + g(x_1,y_2,\dots,y_n) \tag{3.1}$$

where g is a polynomial in $k[x_1,y_2,\dots,y_n]$, and the degree of g in x_1 is less than $\mu(f_i)$. Equation (3.1) shows that x_1 is integral over $k[y_1,\dots,y_n]$. It follows that $A = k[x_1,\dots,x_n] = k[y_1,\dots,y_n][x_1]$ is integral over $k[y_1,\dots,y_n]$. Therefore the extension of quotient fields $k(x_1,\dots,x_n)/k(y_1,\dots,y_n)$ is algebraic. By Theorem 1.8.8, the set $\{y_1,\dots,y_n\}$ is algebraically independent over k. Up to isomorphism, the ring $B = k[y_1,\dots,y_n]$ is a polynomial ring in n variables over k, hence is integrally closed in its field of quotients. By Theorem 6.3.6 (5), going down holds between B and A. By Theorem 10.3.1, the ideal (y_1) in $k[y_1,\dots,y_n]$ is prime of height one. By Theorem 9.6.17, $\operatorname{ht}(I) = \operatorname{ht}(I\cap B)$. Since $(y_1) \subseteq I \cap B$, putting all this together proves that $(y_1) = I\cap B$.

Step 2: $r > 1$. By Exercise 9.6.4, let $J \subseteq I$ be an ideal such that the height of J is equal to $r-1$. By induction on r, there exist $z_1,\dots,z_n$ in A such that A is integral over $B = k[z_1,\dots,z_n]$ and $J\cap B = (z_1,\dots,z_{r-1}) \subseteq I\cap B$. Write $I' = I\cap B$. By Theorem 9.6.17, $\operatorname{ht}(I) = \operatorname{ht}(I') = r$. There exists a polynomial f in $I' - (z_1,\dots,z_{r-1})$ and by subtracting off an element of $(z_1,\dots,z_{r-1})$, we can assume f is a nonzero polynomial in $k[z_r,\dots,z_n]$. Set $y_1 = z_1,\dots,y_{r-1} = z_{r-1}$. Set $y_r = f$. Proceed as in Step 1. Let v be a positive integer and set $y_{r+1} = z_{r+1} - z_r^{v^{r+1}},\dots,y_n = z_n - z_r^{v^n}$. For a sufficiently large v, B is integral over $C = k[y_1,\dots,y_n]$. The set $\{y_1,\dots,y_n\}$ is algebraically independent over k. The height of $I\cap C$ is equal to the height of I. Since $(y_1,\dots,y_r)$ is a prime ideal of height r which is contained in $I\cap C$, the two ideals are equal. □

COROLLARY 10.3.3. *(E. Noether's Normalization Lemma) Let k be a field and A a finitely generated commutative k-algebra. There exist $z_1,\dots,z_m$ in A such that*

(1) *the set $\{z_1,\dots,z_m\}$ is algebraically independent over k,*
(2) *A is integral over $k[z_1,\dots,z_m]$,*
(3) *$\dim(A) = m$, and*
(4) *if A is an integral domain with quotient field K, then $\operatorname{tr.deg}_k(K) = m$.*

PROOF. Let $\alpha_1,\dots,\alpha_n$ be a generating set for A as a k-algebra. The assignments $x_i \mapsto \alpha_i$ define an epimorphism $\phi : k[x_1,\dots,x_n] \to A$. Let I be the kernel of ϕ. Assume $\operatorname{ht}(I) = r$. By Theorem 10.3.2, there exist $y_1,\dots,y_n$ in $k[x_1,\dots,x_n]$ which are algebraically independent over k such that $k[x_1,\dots,x_n]$ is integral over $k[y_1,\dots,y_n]$ and $I\cap k[y_1,\dots,y_n] =$

$(y_1,\dots,y_r)$. The diagram

$$\begin{tikzcd} k[y_1,\dots,y_n] \arrow[r, "\psi"] \arrow[d] & k[x_1,\dots,x_n] \arrow[d, "\phi"] \\ k[y_{r+1},\dots,y_n] \arrow[r, "\theta"] & A = k[x_1,\dots,x_n]/I \end{tikzcd}$$

commutes. The vertical maps are onto. The horizontal maps ψ and θ are one-to-one. Since A is integral over $k[y_1,\dots,y_n]$, θ is integral. Let $m = n-r$ and set $z_1 = \theta(y_{r+1}),\dots,z_m = \theta(y_n)$. The set $\{z_1,\dots,z_m\}$ is algebraically independent over k and A is integral over $k[z_1,\dots,z_m]$. By Theorem 9.6.17, it follows that $\dim(A) = m$. If A is an integral domain, then the quotient field of A is algebraic over $k(z_1,\dots,z_m)$, so Part (4) follows from results in Section 1.8.4. □

COROLLARY 10.3.4. *Let k be a field and A an integral domain which is a finitely generated commutative k-algebra.*

(1) *If $p \in \operatorname{Spec} A$, then* $\dim(A/p) + \operatorname{ht}(p) = \dim(A)$.
(2) *If p and q are in* $\operatorname{Spec} A$ *such that $p \supseteq q$, then* $\operatorname{ht}(p/q) = \operatorname{ht}(p) - \operatorname{ht}(q)$.

PROOF. (1): By Corollary 10.3.3, there exist $y_1,\dots,y_n$ in A such that A is integral over $B = k[y_1,\dots,y_n]$ and $n = \dim(B) = \dim(A)$. By Theorem 6.3.6 (5) and Theorem 9.6.17 (3), $\operatorname{ht}(p\cap B) = \operatorname{ht}(p)$. Since A/p is integral over B, we have A/p is integral over $B/p\cap B$. By Theorem 9.6.17 (1), $\dim(A/p) = \dim(B/p\cap B)$. By Theorem 10.3.2, if $r = \operatorname{ht}(p\cap B)$, then there exist $z_1,\dots,z_n$ in B such that B is integral over $C = k[z_1,\dots,z_n]$, $p\cap C = (z_1,\dots,z_r)$ and $\dim(B/p\cap B) = \dim(C/p\cap C) = n-r$. This proves (1).

(2): By Part (1), $\dim(A/p) + \operatorname{ht}(p) = \dim(A) = \dim(A/q) + \operatorname{ht}(q)$, which implies $\operatorname{ht}(p) - \operatorname{ht}(q) = \dim(A/q) - \dim(A/p)$. By Part (1) applied to the prime ideal p/q in $\operatorname{Spec}(A/q)$, $\dim(A/p) + \operatorname{ht}(p/q) = \dim(A/q)$. Combine these results to get (2). □

3.2. Separably Generated Extension Fields. This section contains an introduction to the notion of separably generated field extensions.

LEMMA 10.3.5. *Let $k \subseteq K \subseteq F$ be a tower of field extensions. If $F = K(\alpha)$ is a simple algebraic extension of K, then*

$$\dim_K \Omega_{K/k} \le \dim_F \Omega_{F/k} \le 1 + \dim_K \Omega_{K/k}.$$

PROOF. Let $f \in K[x]$ be the irreducible polynomial of α. Let I be the principal ideal in $K[x]$ generated by f. By Theorem 10.2.4,

$$I/I^2 \xrightarrow{\gamma} \Omega_{K[x]/k} \otimes_{K[x]} F \xrightarrow{a} \Omega_{F/k} \to 0$$

is an exact sequence of F-vector spaces. By Exercise 10.2.4 and Proposition 10.2.2, $\Omega_{K[x]/k}$ is a free $K[x]$-module of rank $1 + \dim_K \Omega_{K/k}$. The image of γ is generated over F by $\gamma(f)$, hence has dimension less than or equal to one. □

Let F/k be a finitely generated extension of fields. Let $\Xi \subseteq F$ be a transcendence base for F/k. We say Ξ is a *separating transcendence base* of F/k in case F is a separable algebraic extension of $k(\Xi)$. We say F/k is *separably generated* if there exists a separating transcendence base for F/k.

THEOREM 10.3.6. *Let F be a finitely generated extension field of k.*

(1) $\dim_F \Omega_{F/k} \ge \operatorname{tr.deg}_k F$.
(2) $\dim_F \Omega_{F/k} = \operatorname{tr.deg}_k F$ *if and only if F/k is separably generated.*

(3) $\Omega_{F/k} = 0$ *if and only if* F *is separable over* k.

PROOF. (3): This part follows from Theorem 10.2.5, Corollary 5.5.3, and Proposition 5.5.6.

(1): A transcendence base $\xi_1, \dots, \xi_n$ exists for F/k, by Theorem 1.8.8. If we set $K = k(\xi_1, \dots, \xi_n)$, then F/K is finite dimensional. Applying Lemma 10.3.5 iteratively, we get $\dim_F \Omega_{F/k} \geq \dim_K \Omega_{K/k}$. Note that K is the quotient field of $k[\xi_1, \dots, \xi_n]$. By Proposition 10.2.2 and Exercise 10.2.3, $\dim_K \Omega_{K/k} = n = \operatorname{tr.deg}_k F$.

(2): Assume $\xi_1, \dots, \xi_n$ is a transcendence base and $K = k(\xi_1, \dots, \xi_n)$. If F/K is separable, then $\Omega_{F/K} = 0$, by Theorem 10.2.5. Theorem 10.2.3 implies

$$\Omega_{K/k} \otimes_K F \xrightarrow{a} \Omega_{F/k} \to 0$$

is exact. Therefore, equality holds in Part (1). Conversely, suppose in Part (1) that equality holds. Let $n = \operatorname{tr.deg}_k F$ and choose $\xi_1, \dots, \xi_n$ in F such that the set $d_{F/k}(\xi_1), \dots, d_{F/k}(\xi_n)$ is a basis for the F-vector space $\Omega_{F/k}$. Let $K = k(\xi_1, \dots, \xi_n)$. The diagram

$$\begin{tikzcd} K \arrow[r] \arrow[d, "d_{K/k}"'] & F \arrow[d, "d_{F/k}"] \\ \Omega_{K/k} \arrow[r, "\psi"] & \Omega_{F/k} \end{tikzcd}$$

commutes. The image of ψ contains a generating set for $\Omega_{F/k}$, hence $a : \Omega_{K/k} \otimes_R F \to \Omega_{F/k}$ is onto. By Theorem 10.2.3, $\Omega_{F/K} = 0$. By Part (3), F/K is separable and finite dimensional. By Theorem 1.8.8, the set $\{\xi_1, \dots, \xi_n\}$ contains a transcendence base for F/k. Since $n = \operatorname{tr.deg}_k F$, Theorem 1.8.8 implies that the set $\xi_1, \dots, \xi_n$ is a transcendence base for F/k. $\square$

PROPOSITION 10.3.7. *(S. MacLane) Let* k *be a field and* $F = k(a_1, \dots, a_n)$ *a finitely generated extension field of* k. *If* F/k *is separably generated, then there exists a subset of* $\{a_1, \dots, a_n\}$ *which is a separating transcendence base for* F/k.

PROOF. Let $r = \operatorname{tr.deg}_k(F)$. Let $S = k[x_1, \dots, x_n]$ be the polynomial ring over k in n indeterminates. Define $\phi : S \to F$ by $x_i \mapsto a_i$. Since the image of ϕ is $k[a_1, \dots, a_n]$, an integral domain, the kernel of ϕ is a prime ideal P of S. The ideal P is finitely generated, hence we can write $P = (f_1, \dots, f_m)$. Let $A = S/P$. Then F is the quotient field of A. The sequence

$$P/P^2 \xrightarrow{\gamma} \Omega_{S/k} \otimes_S A \xrightarrow{a} \Omega_{A/k} \to 0 \tag{3.2}$$

of Theorem 10.2.4 is exact, $\Omega_{S/k} \otimes_S A$ is a free A-module, and $\{dx_1, \dots, dx_n\}$ is a free basis. For each i,

$$\gamma(f_i) = \sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j} dx_j.$$

Tensor (3.2) with $(\ ) \otimes_A F$. The sequence

$$F^{(m)} \xrightarrow{J} F^{(n)} \to \Omega_{F/k} \to 0$$

is exact, where J is multiplication by the jacobian matrix $J = (\partial f_i / \partial x_j)$. Since F/k is separably generated, by Theorem 10.3.6, the rank of J is $n - r$. This implies there exists an $(n-r)$-by-$(n-r)$ submatrix of J which also has rank $n-r$. Relabel the x_i if necessary and assume the rank of the submatrix

$$(\partial f_i / \partial x_j \mid 1 \leq i \leq n-r, r+1 \leq j \leq n)$$

is $n-r$. The proof of Theorem 10.3.6 shows the set $\{d_{F/k}(a_1),\dots,d_{F/k}(a_r)\}$ is a basis for $\Omega_{F/k}$ over F and $a_1,\dots,a_r$ is a separating transcendence base for F/k. □

LEMMA 10.3.8. *Let k be a field and $F=k(a_1,\dots,a_n)$ a finitely generated extension field of k. If $\operatorname{tr.deg}_k F=r$ and F/k is not separably generated, then upon relabeling the a_i, the field $k(a_1,\dots,a_{r+1})$ is of transcendence degree r over k, and is not separably generated over k.*

PROOF. The proof is by induction on n. If $n=r+1$, then there is nothing to prove. Assume $n>r+1$ and that the result is true for $n-1$. Relabel the a_i and assume a_1 is algebraically dependent on $a_2,\dots,a_n$ over k. Then $k(a_2,\dots,a_n)$ has transcendence degree r over k. If $k(a_2,\dots,a_n)$ is not separably generated over k, then by induction we are done. Assume $k(a_2,\dots,a_n)$ is separably generated over k. By Proposition 10.3.7, we can relabel the a_i and assume $a_2,\dots,a_{r+1}$ is a separating transcendence base for $k(a_2,\dots,a_n)$ over k. Then $k(a_2,\dots,a_n)$ is separable and finite dimensional over $k(a_2,\dots,a_{r+1})$. It follows that $k(a_1,a_2,\dots,a_n)$ is separable and finite dimensional over $k(a_1,a_2,\dots,a_{r+1})$. By the transitive property of separable field extensions, Theorem 5.4.2, it follows that $k(a_1,a_2,\dots,a_{r+1})$ is not separably generated over k. □

THEOREM 10.3.9. *Let k be a perfect field, and F/k a finitely generated extension of fields.*

(1) (F. K. Schmidt) F/k is separably generated.
(2) (Primitive Element Theorem) If $r=\operatorname{tr.deg}_k F$, then there exists a transcendence base $\Xi=\{\xi_1,\dots,\xi_r\}$ for F/k, an element $u\in F$ which is separable over $k(\Xi)$, and $F=k(\Xi)[u]$.

PROOF. (1): Let $r=\operatorname{tr.deg}_k F$ and assume $F=k(a_1,\dots,a_n)$. For contradiction's sake, assume F/k is not separably generated. Let $p=\operatorname{char} k$. By Lemma 10.3.8, we reduce to the case where $n=r+1$. Let $S=k[x_1,\dots,x_n]$ be the polynomial ring over k in n indeterminates. Define $\phi: S\to F$ by $x_i\mapsto a_i$. Since the image of ϕ is $k[a_1,\dots,a_n]$, an integral domain, the kernel of ϕ is a prime ideal P of S. By Noether's Normalization Lemma (Corollaries 10.3.3 and 10.3.4), P has height one. Since S is a unique factorization domain, there exists an irreducible polynomial f in S such that $P=(f)$. View $f(a_1,\dots,a_r,x_{r+1})$ as an element of $k(a_1,\dots,a_r)[x_{r+1}]$. Since a_{r+1} is not separable over $k(a_1,\dots,a_r)$, it follows that f is a polynomial in $k[x_1,\dots,x_r][x_{r+1}^p]$. Iterate this argument $r+1$ times. Then $f\in k[x_1^p,\dots,x_r^p,x_{r+1}^p]$. Since k is perfect, $f=g^p$ for some $g\in S$, a contradiction.

(2): This follows from Part (1), Proposition 10.3.7, and Theorem 5.5.8, the Primitive Element Theorem. □

3.3. Second Form of the Normalization Lemma. We prove a second version of Emmy Noether's Normalization Lemma (Corollary 10.3.3). It requires the ground field to be infinite. The advantage of this version is that it allows us to construct the underlying polynomial ring in such a way that it contains a separating transcendence base. As an application, we derive in Theorem 10.3.11 sufficient conditions for the integral closure of an integral domain A to be a finitely generated A-module.

THEOREM 10.3.10. *(Emmy Noether's Normalization Lemma) Let k be an infinite field and A a finitely generated commutative k-algebra. Assume A is an integral domain with field of fractions K. Then there exist $z_1,\dots,z_m$ in A such that*

(1) the set $\{z_1,\dots,z_m\}$ is algebraically independent over k,
(2) A is integral over $k[z_1,\dots,z_m]$,

(3) $\dim(A) = m$,
(4) $\operatorname{tr.deg}_k(K) = m$, *and*
(5) *if A is generated as a k-algebra by $x_1, \dots, x_n$, then there are elements a_{ij} in k such that $z_i = \sum_{j=1}^{n} a_{ij} x_j$.*
(6) *If K is separably generated over k, then $\{z_1, \dots, z_m\}$ can be chosen in such a way that K is separable over $k(z_1, \dots, z_m)$.*

PROOF. We prove (6). The other cases are left to the reader. Our proof is based on [**61**, I, Chapter V, Theorem 8, p. 266]. Let $x_1, \dots, x_n$ be a generating set for A as a k-algebra. By Proposition 10.3.7, resort the list and assume $\{x_1, \dots, x_m\}$ is a separating transcendence base for K over k. Proceed by induction on n. If $m = n$, then take $z_i = x_i$, for $1 \le i \le m$, and stop. Otherwise, assume $n > m$ and assume the claim is true for any algebra on $n-1$ generators. Then each of $x_{m+1}, \dots, x_n$ is algebraic over $k(x_1, \dots, x_m)$.

Let $A' = k[x_1, \dots, x_{n-1}]$, and K' the field of fractions of A'. By assumption, x_n is separable over K'. Starting with the minimum polynomial for x_n over K', we can find a polynomial P in $k[X_1, \dots, X_n]$ such that $P(x_1, \dots, x_{n-1}, X_n)$ is a separable polynomial in $K'[X_n]$ and such that $P(x_1, \dots, x_{n-1}, x_n) = 0$. Write P as a sum

$$P(X_1, \dots, X_n) = \sum_{i=0}^{q} P_i(X_1, \dots, X_n) \tag{3.3}$$

where $P_i(X_1, \dots, X_n)$ is a homogeneous polynomial of degree i in the polynomial ring $k[X_1, \dots, X_n]$, and $P_q \neq 0$. Introduce new indeterminates $Z_1, \dots, Z_{n-1}$, $\Lambda_1, \dots, \Lambda_{n-1}$ and define an embedding of k-algebras

$$\begin{aligned} \theta : k[X_1, \dots, X_n] &\to k[Z_1, \dots, Z_{n-1}, \Lambda_1, \dots, \Lambda_{n-1}, X_n] \\ X_1 &\mapsto Z_1 + \Lambda_1 X_n \\ &\vdots \\ X_{n-1} &\mapsto Z_{n-1} + \Lambda_{n-1} X_n. \end{aligned}$$

If we denote by F the image of P under θ, then

$$\begin{aligned} F &= F(Z_1, \dots, Z_{n-1}, \Lambda_1, \dots, \Lambda_{n-1}, X_n) \\ &= P(Z_1 + \Lambda_1 X_n, \dots, Z_{n-1} + \Lambda_{n-1} X_n, X_n) \\ &= \sum_{i=0}^{q} P_i(Z_1 + \Lambda_1 X_n, \dots, Z_{n-1} + \Lambda_{n-1} X_n, X_n). \end{aligned} \tag{3.4}$$

Because each P_i is homogeneous of degree i, if we expand F as a polynomial in X_n, the highest degree term is

$$X_n^q P_q(\Lambda_1, \dots, \Lambda_{n-1}, 1). \tag{3.5}$$

By $\mathbb{A}_k^{n-1}$ we denote affine $n-1$-space over k with the Zariski topology (Section 6.2.2). The zero set of $P_q(\Lambda_1, \dots, \Lambda_{n-1}, 1)$ in $\mathbb{A}_k^{n-1}$ is a closed subset, call it V_1. Because the polynomial $P_q(\Lambda_1, \dots, \Lambda_{n-1}, 1)$ is nonzero and k is infinite, we know that $V_1 \neq \mathbb{A}_k^{n-1}$. There exists a point $(\lambda_1, \dots, \lambda_{n-1}) \in \mathbb{A}_k^{n-1}$ such that if we set $z_1 = x_1 - \lambda_1 x_n, z_{n-1} = x_{n-1} - \lambda_{n-1} x_n$, then

$$F(z_1, \dots, z_{n-1}, \lambda_1, \dots, \lambda_{n-1}, X_n) \tag{3.6}$$

is a polynomial of degree q in $k[z_1, \dots, z_{n-1}][X_n]$ and the leading coefficient is a nonzero element of k. Since $F(z_1, \dots, z_{n-1}, \lambda_1, \dots, \lambda_{n-1}, x_n) = P(x_1, \dots, x_n) = 0$, this shows x_n is integral over $k[z_1, \dots, z_{n-1}]$. To finish the proof, we show that there exists a choice for

$(\lambda_1,\dots,\lambda_{n-1})$ such that x_n is a simple root of the polynomial in (3.6). In (3.4), compute the derivative of F with respect to X_n:

$$\frac{\partial F}{\partial X_n} = \sum_{i=1}^{n-1} \Lambda_i \frac{\partial P}{\partial X_i} + \frac{\partial P}{\partial X_n}. \tag{3.7}$$

Substituting $X_1 = x_1,\dots,X_n = x_n$, we have

$$\frac{\partial F}{\partial X_n}(x_1,\dots,x_n) = \sum_{i=1}^{n-1} \Lambda_i \frac{\partial P}{\partial X_i}(x_1,\dots,x_n) + \frac{\partial P}{\partial X_n}(x_1,\dots,x_n). \tag{3.8}$$

which is a linear polynomial in $k[\Lambda_1,\dots,\Lambda_{n-1}]$. The polynomial (3.8) is not identically zero, because for $\Lambda_1 = 0,\dots,\Lambda_{n-1} = 0$ it evaluates to $\partial P/\partial X_n(x_1,\dots,x_n)$ which is nonzero since x_n is separable over K'. The zero set of (3.8) in $\mathbb{A}_k^{n-1}$ is a proper closed subset, call it V_2. Since $V_1 \cup V_2$ is the zero set of a nonzero polynomial in $k[\Lambda_1,\dots,\Lambda_{n-1}]$, it is a proper closed subset. Therefore, there is a point $(\lambda_1,\dots,\lambda_{n-1})$ such that (3.8) is nonzero and x_n is a simple root of the polynomial (3.6). $\square$

As an application, we get the following finiteness theorem for the integral closure of an integral domain in an extension of its quotient field. Theorem 10.3.11, which requires A to be a finitely generated algebra over a field, is a strong version of Theorem 6.1.13.

THEOREM 10.3.11. *Let A be an integral domain which is a finitely generated algebra over a field k. Let K be the quotient field of A, and let L be a finitely generated algebraic extension of K. If S is the integral closure of A in L, then S is a finitely generated A-module, and is also a finitely generated k-algebra.*

PROOF. Our proof is based on [**61**, I, Chapter V, Theorem 9, p. 267]. By the proof of Theorem 6.1.13, there are elements $\lambda_1,\dots,\lambda_n$ in S which generate L as a vector space over K. Let B be the A-subalgebra of L generated by $\lambda_1,\dots,\lambda_n$. Then B is finitely generated as an A-module, finitely generated as a k-algebra, L is the field of fractions of B, and S is the integral closure of B in L. After replacing A with B and K with L, we assume S is the integral closure of A in K. It is enough to show S is finitely generated as an A-module.

Let Ω be an algebraically closed field containing K. For the remainder of this proof, every k-algebra is tacitly assumed to be a subring of Ω. Assume A is generated as a k-algebra by $x_1,\dots,x_n$. Let $\bar{k}$ be the algebraic closure of k, and $\bar{A}$ the $\bar{k}$-algebra generated by $x_1,\dots,x_n$. Let $\bar{K}$ be the field of fractions of $\bar{A}$. By Theorem 10.3.9, $\bar{K}$ is separably generated over $\bar{k}$. By Theorem 10.3.10, there are elements $z_1,\dots,z_m$ in $\bar{A}$ which satisfy:

(a) $\bar{k}[z_1,\dots,z_m]$ is a polynomial subring of $\bar{A}$,
(b) $\bar{A}$ is integral over $\bar{k}[z_1,\dots,z_m]$,
(c) there are elements a_{ij} in $\bar{k}$ such that $z_i = \sum_{j=1}^{n} a_{ij}x_j$, for $1 \le i \le m$,
(d) $\bar{K}$ is separable over $\bar{k}(z_1,\dots,z_m)$.

Let P_j be the minimum polynomial for x_j over $\bar{k}(z_1,\dots,z_m)$. By Theorem 6.1.11, P_j is a polynomial with coefficients in $\bar{k}[z_1,\dots,z_m]$. Let F be the subfield of $\bar{k}$ generated by adjoining to k all of the elements a_{ij} of (c), and all of the $\bar{k}$-coefficients that appear in $P_1,\dots,P_n$. Let A' be the F-algebra generated by $x_1,\dots,x_n$ and let K' be the field of fractions of A'. By construction, we have:

(e) $F[z_1,\dots,z_m]$ is a polynomial subring of A',
(f) A' is integral over $F[z_1,\dots,z_m]$, and
(g) K' is separable over $F(z_1,\dots,z_m)$.

Let T be the integral closure of $F[z_1, \ldots, z_m]$ in K'. By Theorem 6.1.13, T is a finitely generated $F[z_1, \ldots, z_m]$-module. By (f), T contains A', hence T is a finitely generated A'-module. Since $\dim_k(F)$ is finite, A' is a finitely generated A-module. Therefore, T is a finitely generated A-module. Since $S = T \cap K$, S is an A-submodule of T. Since A is noetherian, S is a finitely generated A-module (Corollary 4.1.12). $\square$

4. More Flatness Criteria

In this section we prove some necessary results on flatness. The material in this section is from various sources, including [**41**], [**22**], [**40**], and [**48**].

4.1. Constructible Sets. Let X be a topological space and $Z \subseteq X$. We say Z is *locally closed* in X if Z is an open subset of $\bar{Z}$, the closure of Z in X.

LEMMA 10.4.1. *The following are equivalent for a subset Z of a topological space X.*

(1) Z is locally closed.
(2) For every point $x \in Z$, there exists an open neighborhood U_x such that $Z \cap U_x$ is closed in U_x.
(3) There exists a closed set F in X and an open set G in X such that $Z = F \cap G$.

PROOF. Is left to the reader. $\square$

We say that Z is a *constructible set* in X if Z is a finite union of locally closed sets in X. By Lemma 10.4.1, a constructible set Z has a representation

$$Z = \bigcup_{i=1}^{r} (U_i \cap F_i)$$

where each U_i is open in X and each F_i is closed in X.

LEMMA 10.4.2. *If Y and Z are constructible in X, then so are $Y \cup Z$, $Y - Z$, $Y^c = X - Y$, and $Y \cap Z$.*

PROOF. Write $Y = (U_1 \cap E_1) \cup \cdots \cup (U_r \cap E_r)$ and $Z = (V_1 \cap F_1) \cup \cdots \cup (V_s \cap F_s)$ where U_i, V_j are open and E_j, F_j are closed for all i and j. Using the identity

$$\begin{aligned} U \cap E - V \cap F &= U \cap E \cap (V \cap F)^c \\ &= U \cap E \cap (V^c \cup F^c) \\ &= (U \cap E \cap V^c) \cup (U \cap E \cap F^c) \\ &= \big(U \cap (E \cap V^c)\big) \cup \big((U \cap F^c) \cap E\big) \end{aligned}$$

the reader should verify that $Y - V_1 \cap F_1$ is constructible. Now use induction on s to prove $Y - Z$ is constructible. This also proves $Y^c = X - Y$ and $Z^c = X - Z$ are constructible. Hence $Y \cap Z = (Y^c \cup Z^c)^c$ is constructible. $\square$

PROPOSITION 10.4.3. *Let X be a noetherian topological space and Z a subset of X. The following are equivalent.*

(1) Z is constructible in X.
(2) For each irreducible closed set Y in X, either $Y \cap Z$ is not dense in Y, or $Y \cap Z$ contains a nonempty open set of Y.

PROOF. (1) implies (2): Write $Z = (U_1 \cap E_1) \cup \cdots \cup (U_r \cap E_r)$. Since Y is closed, by Proposition 1.3.7 we can decompose each $Y \cap E_i$ into its irreducible components. Therefore, we can write $Y \cap Z = (V_1 \cap F_1) \cup \cdots \cup (V_s \cap F_s)$ where each V_i is open in X, each F_i is closed and irreducible in X, and $V_i \cap F_i$ is nonempty for each i. By Lemma 1.3.4, $\overline{V_i \cap F_i} = F_i$. Therefore, $\overline{Y \cap Z} = F_1 \cup \cdots \cup F_s$. If $Y \cap Z$ is dense in Y, then $Y = F_1 \cup \cdots \cup F_s$, so that for some i we have $Y = F_i$. Then $U_i \cap Y = U_i \cap F_i$ is a nonempty open subset of Y contained in $Y \cap Z$.

(2) implies (1): Let $\mathscr{S}$ be the set of all closed sets of the form $\bar{Z}$ where Z is a subset of X that satisfies (2) but not (1). For contradiction's sake, assume $\mathscr{S}$ is nonempty. By Lemma 1.3.5 (4), let Z be a subset of X satisfying (2) but not (1) such that $\bar{Z}$ is minimal in $\mathscr{S}$. The empty set is constructible, so $Z \neq \emptyset$. Let $\bar{Z} = Z_1 \cup \cdots \cup Z_r$ be the decomposition into irreducible closed components. Then $Z \cap Z_1 \neq \emptyset$ and $\overline{Z \cap Z_1}$ is a closed subset of Z_1. Since $Z_1 = \overline{Z \cap Z_1} \cup (Z_1 \cap Z_2) \cdots \cup (Z_1 \cap Z_r)$, it follows that $\overline{Z \cap Z_1} = Z_1$. By (2) there exists a nonempty open $U \subseteq Z_1$ such that $U \subseteq Z$. Notice that U is locally closed in X. The set $Z_1' = Z_1 - U$ is a proper closed subset of Z_1. Write $Z^* = Z_1' \cup Z_2 \cup \cdots \cup Z_r$, a proper closed subset of $\bar{Z}$. We have $\overline{Z \cap Z^*} \subseteq Z^* \subsetneq \bar{Z}$.

We next show $Z \cap Z^*$ satisfies (2). To this end, assume Y is an irreducible closed in X such that $\overline{Y \cap Z \cap Z^*} = Y$. In this case, the closed set Z^* contains Y, hence $Y \cap Z \cap Z^* = Z \cap Y$. Since Z satisfies (2), $Z \cap Y$ contains a nonempty open set of Y. This proves $Z \cap Z^*$ satisfies (2). Since $\bar{Z}$ was a minimal member of $\mathscr{S}$, $Z \cap Z^*$ is constructible. Therefore $Z = U \cup (Z \cap Z^*)$ is constructible, a contradiction. □

4.1.1. *Chevalley's Theorem.*

LEMMA 10.4.4. *Let $\theta : R \to S$ be a homomorphism of commutative rings and $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 3.3.3. The following are equivalent.*

(1) The image of $\theta^\sharp$ is dense in $\operatorname{Spec} R$.

(2) $\ker \theta \subseteq \operatorname{Rad}_R(0)$.

In particular, if $\operatorname{Rad}_R(0)$*, then the image of $\theta^\sharp$ is dense if and only if θ is one-to-one.*

PROOF. The image of $\theta^\sharp$ is $\operatorname{im} \theta^\sharp = \{\theta^{-1}(Q) \mid Q \in \operatorname{Spec} S\}$. By Lemma 3.3.8, the closure of $\operatorname{im} \theta^\sharp$ is $V(I)$, where I is the ideal

$$I = \bigcap_{Q \in \operatorname{Spec} S} \theta^{-1}(Q) = \theta^{-1}\left(\bigcap_{Q \in \operatorname{Spec} S} Q\right) = \theta^{-1}\left(\operatorname{Rad}_S(0)\right).$$

It is clear that $\ker \theta \subseteq I$.

(1) implies (2): If $V(I) = \operatorname{Spec} R$, then $I \subseteq \operatorname{Rad}_R(0)$, and this implies (2).

(2) implies (1): The reader should verify that if $x \in R$ and $\theta(x) \in \operatorname{Rad}_S(0)$, then $x \in \operatorname{Rad}(\ker \theta)$. By (2), $I = \theta^{-1}(\operatorname{Rad}_S(0)) \subseteq \operatorname{Rad}_R(0)$. Therefore, $V(I) = \operatorname{Spec} R$, which implies (1). □

LEMMA 10.4.5. *Let R be a noetherian integral domain and S a commutative faithful finitely generated R-algebra with structure map $\theta : R \to S$. There exists an element $a \in R - (0)$ such that the basic open set $U(a) = \operatorname{Spec} R - V(a)$ is contained in the image of the natural map $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$.*

PROOF. Since θ is one-to-one, we assume $R \subseteq S$. Find $x_1, \ldots, x_n$ in S such that $S = R[x_1, \ldots, x_n]$. Further, assume $x_1, \ldots, x_r$ are algebraically independent over R, while each of the elements $x_{r+1}, \ldots, x_n$ satisfies an algebraic relation over $T = R[x_1, \ldots, x_r]$. For each $j = r+1, \ldots, n$ find a polynomial $f_j(x) \in T[x]$ satisfying

(1) $f_j(x_j) = 0$,
(2) f_j has degree $d_j \geq 1$, and
(3) the leading coefficient of f_j is f_{j0}, an element of T.

Then $f = \prod_{j=r+1}^{n} f_{j0}$ is a nonzero element of T. Let a be any nonzero coefficient of f, where we view f as a polynomial over R in the variables $x_1, \ldots, x_r$. We show that this a is satisfactory. Let P be an arbitrary element of $U(a)$. Then $P \in \operatorname{Spec} R$ and $a \notin P$. We show that $P \in \operatorname{im} \theta^\sharp$. The reader should verify that $PT = P[x_1, \ldots, x_r]$ is a prime ideal in T. Since $f \notin PT$, each x_j is integral over T_{PT}. Therefore S_{PT} is integral over T_{PT}. By Theorem 6.3.6, there exists a prime ideal Q in S_{PT} lying over $(PT)T_{PT}$. On the left side of this diagram

$$
\begin{tikzcd}[column sep=small]
 & S_{PT} = S \otimes_T T_{PT} \arrow[dl, dash] \arrow[dr, dash] & \\
S \arrow[dr, dash] \arrow[dd, dash] & & T_{PT} \arrow[dl, dash] \\
 & T = R[x_1, \ldots, x_r] \arrow[dl, dash] & \\
R & &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & Q \arrow[dl, dash] \arrow[dr, dash] & \\
Q \cap S \arrow[dr, dash] \arrow[dd, dash] & & (PT)T_{PT} \arrow[dl, dash] \\
 & Q \cap T = PT \arrow[dl, dash] & \\
P & &
\end{tikzcd}
$$

is the lattice of subrings, on the right, the lattice of prime ideals. We have $Q \cap R = Q \cap T \cap R = PT \cap R = P$. Therefore, $P = Q \cap R = Q \cap S \cap R = \theta^\sharp(Q \cap S)$. $\square$

LEMMA 10.4.6. *Let R be a commutative noetherian ring and Z a constructible set in* $\operatorname{Spec} R$. *There exists a finitely generated R-algebra S such that the image of the natural map* $\operatorname{Spec} S \to \operatorname{Spec} R$ *is Z.*

PROOF. Case 1: $Z = U(a) \cap V(I)$, where I is an ideal of R and $U(a) = \operatorname{Spec} R - V(a)$ is a basic open set, for some $a \in R$. By Exercise 3.3.9, $\operatorname{Spec} R[a^{-1}]$ maps homeomorphically onto $U(a)$. By Exercise 3.3.8, $\operatorname{Spec} R/I$ maps homeomorphically onto $V(I)$. The reader should verify that $S = R/I \otimes_R R[a^{-1}]$ is satisfactory.

Case 2: Z is an arbitrary constructible set. Then Z is a finite union of sets of the form $U \cap Y$ where U is open and F is closed. An arbitrary open is of the form $R - V(I)$, where I is a finitely generated ideal in the noetherian ring R. Therefore, U can be written as a finite union of basis open sets. We can write $Z = \bigcup_{i=1}^{n} U(a_i) \cap V(I_i)$. By Case 1, $U(a_i) \cap V(I_i)$ is the image of $\operatorname{Spec} S_i$ for some finitely generated R-algebra S_i. Let S be the finitely generated R-algebra $S_1 \oplus \cdots \oplus S_n$. By Exercise 3.3.6, $\operatorname{Spec} S$ decomposes into the disjoint union $\operatorname{Spec} S_1 \cup \cdots \cup \operatorname{Spec} S_n$. The image of $\operatorname{Spec} S$ is Z. $\square$

THEOREM 10.4.7. *(Chevalley) Let R be a commutative noetherian ring and S a finitely generated R-algebra. Under the natural map $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$, the image of a constructible set is a constructible set.*

PROOF. Step 1: $\operatorname{im} \theta^\sharp$ is a constructible set. Let Y be an irreducible closed in $\operatorname{Spec} R$. In order to apply Proposition 10.4.3, assume $\operatorname{im} \theta^\sharp \cap Y$ is dense in Y. By Lemma 3.3.10,

$Y = V(P)$ for some prime ideal P in R. Consider the two commutative diagrams.

$$\begin{tikzcd} S \arrow[r] & S/PS \\ R \arrow[u, "\theta"] \arrow[r, "\eta"] & R/P \arrow[u, "\bar\theta"'] \end{tikzcd} \qquad \begin{tikzcd} \operatorname{Spec} S \arrow[d, "\theta^\sharp"'] & \operatorname{Spec}(S/PS) \arrow[l] \arrow[d, "\bar\theta^\sharp"] \\ \operatorname{Spec} R \supseteq Y & \operatorname{Spec}(R/P) \arrow[l, "\eta^\sharp"'] \end{tikzcd}$$

The map $\eta^\sharp$ maps $\operatorname{Spec} R/P$ homeomorphically onto Y. The set $\operatorname{im}\theta^\sharp \cap Y$ is equal to the image of $\eta^\sharp\bar\theta^\sharp$. By Lemma 10.4.4, $\bar\theta$ is one-to-one. By Lemma 10.4.5, $\operatorname{im}\theta^\sharp \cap Y$ contains a nonempty open subset of Y. Proposition 10.4.3 implies $\operatorname{im}\theta^\sharp$ is constructible.

Step 2: Let Z be a constructible set in $\operatorname{Spec} S$. By Lemma 10.4.6 there exists a finitely generated S-algebra T with structure homomorphism $\phi : S \to T$ such that the image of the natural map $\phi^\sharp : \operatorname{Spec} T \to \operatorname{Spec} S$ is equal to Z. Notice that T is a finitely generated R-algebra with structure homomorphism $\phi\theta : R \to T$ and the image of $\theta^\sharp\phi^\sharp$ is equal to $\theta^\sharp(Z)$. By Step 1 applied to T, the image of $\theta^\sharp\phi^\sharp$ constructible. □

4.1.2. *Submersive morphisms.* Let X be a noetherian topological space. A subset Z of X is said to be *pro-constructible* if there exists a family $\{Z_i \mid i \in I\}$ of constructible sets such that $Z = \bigcap_{i\in I} Z_i$. We say Z is *ind-constructible* if such a family of constructible sets exists and $Z = \bigcup_{i\in I} Z_i$.

PROPOSITION 10.4.8. *Let R be a noetherian commutative ring and S a commutative R-algebra with structure homomorphism $\theta : R \to S$. The image of $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is a pro-constructible set in* $\operatorname{Spec} R$.

PROOF. By Exercise 2.7.4, $S = \varinjlim_\alpha S_\alpha$, where S_α runs through the set of all finitely generated R-subalgebras of S. For each α, let $\phi_\alpha : R \to S_\alpha$ be the structure homomorphism and let $\psi_\alpha : S_\alpha \to S$ be the set inclusion map. For each α, we have $\theta^\sharp = \phi_\alpha^\sharp\psi_\alpha^\sharp$. Therefore, $\operatorname{im}(\theta^\sharp) \subseteq \bigcap_\alpha \operatorname{im}(\phi_\alpha^\sharp)$. To show that these sets are equal, suppose $P \in \operatorname{Spec} R - \operatorname{im}(\theta^\sharp)$. Let $S_P = S \otimes_R R_P$. The reader should verify that $PS_P = S_P$. We can write $1 \in PS_P$ as a finite sum, $1 = \sum_{i=1}^n a_i s_i w^{-1}$, where $w \in R - P$ and for each i, $a_i \in P$ and $s_i \in S$. Let $T = R[s_1, \dots, s_n]$ be the R-subalgebra of S generated by $s_1, \dots, s_n$. Then $PT_P = T_P$, so P is not in the image of $\operatorname{Spec} T \to \operatorname{Spec} R$. This proves $\operatorname{im}(\theta^\sharp) = \bigcap_\alpha \operatorname{im}(\phi_\alpha^\sharp)$. By Theorem 10.4.7, the image of $\theta^\sharp$ is pro-constructible. □

Let R be a commutative ring and $P, Q \in \operatorname{Spec} R$. If $P \subseteq Q$, then we say that Q is a *specialization* of P and P is a *generalization* of Q. The set of all specializations of P is equal to the irreducible closed set $V(P)$. If $Z \subseteq \operatorname{Spec} R$ we say Z is *stable under specialization* if Z contains all specializations of every point in Z. We say Z is *stable under generalization* if Z contains all generalizations of every point in Z. The reader should verify that a closed set is stable under specialization and an open set is stable under generalization.

LEMMA 10.4.9. *Let R be a commutative noetherian ring.*

(1) Let Z be a subset of $\operatorname{Spec} R$ *which satisfies*
   (a) Z is pro-constructible and
   (b) Z is stable under specialization.
   Then Z is closed.
(2) Let U be a subset of $\operatorname{Spec} R$ *which satisfies*
   (a) U is stable under generalization and
   (b) if $P \in U$, then U contains a nonempty open subset of the irreducible closed set $V(P)$.

Then U is open.

PROOF. (1): Write $Z = \bigcap_{\alpha \in I} Z_\alpha$, where each Z_α is constructible. Let $\bar{Z} = Y_1 \cup \cdots \cup Y_m$ be the decomposition into irreducible closed components. Fix i such that $1 \le i \le m$. Then $Y_i = V(P_i)$, where P_i is the generic point of Y_i. As in the proof of Proposition 10.4.3, $Y_i \cap Z$ is a dense subset of Y_i. For each α, $Y_i \cap Z_\alpha$ is dense in Y_i. By Proposition 10.4.3, $Y_i \cap Z_\alpha$ contains a nonempty open subset of Y_i. Therefore, $P \in Y_i \cap Z_\alpha$ for each α. Hence $P_i \in \bigcap_{\alpha \in I} Z_\alpha = Z$. Since Z is stable under specialization, $Y_i = V(P_i) \subseteq Z$. Since i was arbitrary, $\bar{Z} \subseteq Z$, so Z is closed.

(2): Let $Z = \operatorname{Spec} R - U$ and let $\bar{Z} = Y_1 \cup \cdots \cup Y_m$ be the decomposition into irreducible closed components. Fix i such that $1 \le i \le m$. Then $Y_i = V(P_i)$, where P_i is the generic point of Y_i. For contradiction's sake, assume $P_i \in U$. By (b) there exists a nonempty set $V \subseteq Y_i$ such that V is open in Y_i and $V \subseteq Y_i \cap U$. Since $Y_i \not\subseteq Y_j$ if $i \neq j$, $W = V - \bigcup_{j \neq i} Y_j$ is a nonempty open subset of Y_i, W is open in $\bar{Z}$, and $W \subseteq U$. Then $\bar{Z} - W$ is a closed set containing Z which is a proper closed subset of $\bar{Z}$, a contradiction. We conclude that $P_i \in Z$. If P is a specialization of P_i, then by (a), $P \in Z$. That is, $Y_i \subseteq Z$. This proves $\bar{Z} \subseteq Z$, so Z is closed. □

We say that a homomorphism of commutative rings $\phi : R \to S$ is *submersive* if $\phi^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is onto and the topology on $\operatorname{Spec} R$ is equal to the quotient topology of $\operatorname{Spec} S$. That is, $Y \subseteq \operatorname{Spec} R$ is closed if and only if $(\phi^\sharp)^{-1}(Y)$ is closed.

THEOREM 10.4.10. *Let R be a commutative noetherian ring and S a commutative R-algebra with structure homomorphism $\phi : R \to S$. If one of the following three conditions is satisfied, then ϕ is submersive.*

(1) S is a faithfully flat R-module.
(2) R is an integrally closed integral domain and S is an integral domain which is a faithful integral R-algebra.
(3) $\phi^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is onto, and going down holds for ϕ.

PROOF. If condition (1) is satisfied, then by Theorem 6.3.5, going down holds and by Lemma 3.5.4, $\phi^\sharp$ is onto. This case reduces to (3).

If condition (2) is satisfied, then by Theorem 6.3.6, so is condition (3).

Assume (3) is satisfied. Let Y be any subset of $\operatorname{Spec} R$ such that $(\phi^\sharp)^{-1}(Y)$ is closed in $\operatorname{Spec} S$. It suffices to show that Y is closed. There exists an ideal J in S such that $(\phi^\sharp)^{-1}(Y) = V(J)$. Since $\phi^\sharp$ is onto, $\phi^\sharp(\phi^\sharp)^{-1}(Y) = Y$. Let $\eta : S \to S/J$ be the natural map. The image of $\phi^\sharp \eta^\sharp$ is equal to Y, so by Proposition 10.4.8, Y is pro-constructible. By Lemma 10.4.9, if we show that Y is stable under specialization, the proof is complete. Assume $P_1 \in Y$ and P_2 is a specialization of P_1 in $\operatorname{Spec} R$ such that $P_1 \subsetneq P_2$. It suffices to show $P_2 \in Y$. Since $\phi^\sharp$ is onto, there exists $Q_2 \in \operatorname{Spec} S$ lying over P_1. Since going down holds, by Proposition 6.3.4, there exists $Q_1 \in \operatorname{Spec} S$ lying over P_1 such that $Q_1 \subsetneq Q_2$. So Q_2 is a specialization of Q_1. Since Q_1 is in the closed set $(\phi^\sharp)^{-1}(Y)$, so is Q_2. Therefore $P_2 = \phi^\sharp(Q_2) \in \phi^\sharp(\phi^\sharp)^{-1}(Y) = Y$. □

THEOREM 10.4.11. *Let R be a commutative noetherian ring and S a commutative finitely generated R-algebra with structure homomorphism $\phi : R \to S$. Assume going down holds for ϕ. Then $\phi^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is an open map.*

PROOF. Start with U an open in $\operatorname{Spec} S$ and show that $\phi^\sharp(U)$ is open in $\operatorname{Spec} R$. By Theorem 10.4.7, $\phi^\sharp(U)$ is constructible in $\operatorname{Spec} R$. Let $P_2 \in \phi^\sharp(U)$. There exists $Q_2 \in U$ lying over P_2. Assume P_1 is a generalization of P_2, $P_1 \subseteq P_2$. By Proposition 6.3.4, since going down holds, there exists $Q_1 \in \operatorname{Spec} S$ lying over P_1 such that $Q_1 \subseteq Q_2$. Therefore $Q_1 \in U$, since Q_1 is a generalization of Q_2 and U is open. Hence $P_1 \in \phi^\sharp(U)$, which proves $\phi^\sharp(U)$ is stable under generalization. By Lemma 10.4.9, $\operatorname{Spec} R - \phi^\sharp(U)$ is closed. □

4.2. Local Criteria for Flatness. References for the material in this section are [**41**, Chapter 8, Section 20], [**22**, Chapitre 0, § 10], and [**40**].

Let R be a commutative ring and I an ideal of R. Let M be an R-module. In Example 7.2.3 and Example 7.2.5 we defined the associated graded ring

$$\operatorname{gr}_I(R) = \bigoplus_{n\geq 0} I^n/I^{n+1}$$

and the associated graded module

$$\operatorname{gr}_I(M) = \bigoplus_{n=0}^{\infty} I^n M/I^{n+1}M.$$

Then $\operatorname{gr}_I(M)$ is a graded $\operatorname{gr}_I(R)$-module. For the following, set $R_0 = \operatorname{gr}_I(R)_0 = R/I$ and $M_0 = \operatorname{gr}_I(M)_0 = M/I$. The ring $\operatorname{gr}_I(R)$ is an R_0-algebra, and M_0 is an R_0-module. For all $n \geq 0$, the multiplication map

$$\mu_{n0} : \frac{I^n}{I^{n+1}} \otimes_{R_0} M_0 \to \frac{I^n M}{I^{n+1}M}$$

is onto. Taking the direct sum, there is a surjective degree-preserving homomorphism

$$\mu : \operatorname{gr}_I(R) \otimes_{R_0} M_0 \to \operatorname{gr}_I(M)$$

of R_0-modules. We say that M is *ideal-wise separated for I* if for each finitely generated ideal J of R, the R-module $J \otimes_R M$ is separated in the I-adic topology.

EXAMPLE 10.4.12. Some examples of modules that are ideal-wise separated are listed here.

(1) Let S be a commutative R-algebra and M a finitely generated S-module. Suppose S is noetherian and I is an ideal of R such that $IS \subseteq \mathrm{J}(S)$. Let J be any ideal of R. The reader should verify that the I-adic topology on $J \otimes_R M$ is equal to the $I \otimes_R S$-adic topology, which is equal to the IS-adic topology. Since $J \otimes_R M$ is a finitely generated S-module, Corollary 7.3.6 (1) says $J \otimes_R M$ is separated in the I-adic topology. Therefore M is ideal-wise separated for I.
(2) Let R be a commutative ring and M a flat R-module. If J is an ideal of R, then $0 \to J \otimes_R M \to M \to M/JM \to 0$ is exact. That is, $J \otimes_R M = JM$. If I is an ideal of R and M is separated for the I-adic topology, then $I^n JM \subseteq I^n M$ so JM is separated for the I-adic topology. Therefore M is ideal-wise separated for I.
(3) Let R be a principal ideal domain. Let I and J be ideals of R and M an R-module. If $w \in I^n(J \otimes_R M)$, then w can be written in the form $1 \otimes z$ where $z \in I^n M$. If M is separated in the I-adic topology, then M is ideal-wise separated for I.

THEOREM 10.4.13. *(Local Criteria for Flatness) Let R be a commutative ring, I an ideal of R, and M an R-module. Let $\operatorname{gr}_I(M)$ be the associated graded $\operatorname{gr}_I(R)$-module. Set $R_0 = R/I$ and $M_0 = M/I$. Assume*

(A) I is nilpotent, or
(B) R is noetherian and M is ideal-wise separated for I.

Then the following are equivalent.

(1) M is a flat R-module.
(2) $\operatorname{Tor}_1^R(N,M) = 0$ for all R_0-modules N.

(3) *M_0 is a flat R_0-module and $0 \to I \otimes_R M \to IM$ is an exact sequence.*
(4) *M_0 is a flat R_0-module and $\operatorname{Tor}_1^R(R_0, M) = 0$.*
(5) *M_0 is a flat R_0-module and the multiplication maps*

$$\mu_{n0} : \frac{I^n}{I^{n+1}} \otimes_{R_0} M_0 \to \frac{I^n M}{I^{n+1} M}$$

are isomorphisms for all $n \geq 0$.
(6) *$M_n = M/I^{n+1}M$ is a flat $R_n = R/I^{n+1}$-module for each $n \geq 0$.*

PROOF. Notice that (A) or (B) is used to prove that (6) implies (1). The rest of the proof is valid for an arbitrary module M.

Throughout the proof we will frequently make use of the natural isomorphism

$$N \otimes_R M = N \otimes_{R/J} (R/J) \otimes_R M = N \otimes_{R/J} (M/JM)$$

for any ideal J of R and any R/J-module N.

(1) implies (2): If N is an R_0-module, then N is an R-module. This follows from Lemma 8.3.3.

(2) implies (3): Start with an exact sequence

$$0 \to A \to B \to C \to 0$$

of $R_0 = R/I$-modules. The sequence

$$\operatorname{Tor}_1^R(C, M) \to A \otimes_{R_0} M_0 \to B \otimes_{R_0} M_0 \to C \otimes_{R_0} M_0 \to 0$$

is also exact. But $\operatorname{Tor}_1^R(C, M) = 0$, so we conclude that M_0 is a flat R_0-module.

(3) implies (4): Follows easily from the exact sequence

$$\operatorname{Tor}_1^R(R, M) \to \operatorname{Tor}_1^R(R/I, M) \to I \otimes_R M \to M.$$

(4) implies (2): Let N be an R_0-module and write N as a quotient of a free R_0-module F,

$$0 \to K \to F \to N \to 0.$$

By Lemma 8.3.2 (7) and hypothesis (4) $\operatorname{Tor}_1^R(F, M) = \bigoplus_\alpha \operatorname{Tor}_1^R(R_0, M) = 0$. The sequence

$$0 \to \operatorname{Tor}_1^R(N, M) \to K \otimes_{R_0} M_0 \to F \otimes_{R_0} M_0 \to N \otimes_{R_0} M_0 \to 0$$

is exact. But M_0 is a flat R_0-module, so we conclude that $\operatorname{Tor}_1^R(N, M) = 0$.

(2) implies (5): Start with the exact sequence of R-modules

$$0 \to I^{n+1} \to I^n \to I^n/I^{n+1} \to 0$$

where $n \geq 0$. The multiplication homomorphisms combine to make up a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & I^{n+1} \otimes_R M \arrow[r] \arrow[d, "\gamma_{n+1}"] & I^n \otimes_R M \arrow[r] \arrow[d, "\gamma_n"] & I^n/I^{n+1} \otimes_{R_0} M_0 \arrow[r] \arrow[d, "\mu_{n0}"] & 0 \\
0 \arrow[r] & I^{n+1}M \arrow[r] & I^n M \arrow[r] & I^n M/I^{n+1}M \arrow[r] & 0
\end{tikzcd}$$

The top row is exact because of hypothesis (2). The second row is clearly exact. The multiplication maps γ_{n+1}, γ_n, μ_{n0} are all onto. For $n = 0$, μ_{n0} is an isomorphism. For $n = 1$, γ_n is an isomorphism by the proof of (2) implies (3). By induction on n, we see that γ_n is an isomorphism for all $n \geq 0$. By the Snake Lemma (Theorem 2.5.2) it follows that μ_{n0} is an isomorphism for all $n \geq 0$.

(5) implies (6): Fix an integer $n > 0$. For each $i = 1,2,\dots,n$ there is a commutative diagram

$$\begin{tikzcd}
& I^{i+1}/I^{n+1} \otimes_R M \arrow[r] \arrow[d, "\alpha_{i+1}"] & I^i/I^{n+1} \otimes_R M \arrow[r] \arrow[d, "\alpha_i"] & I^i/I^{i+1} \otimes_{R_0} M_0 \arrow[r] \arrow[d, "\mu_{i0}"] & 0 \\
0 \arrow[r] & I^{i+1}M/I^{n+1}M \arrow[r] & I^iM/I^nM \arrow[r] & I^iM/I^{i+1}M \arrow[r] & 0
\end{tikzcd}$$

with exact rows. By hypothesis, μ_{i0} is an isomorphism for all i. For $i = n$, the diagram collapses and we see immediately that α_n is an isomorphism. By descending induction on i we see that each α_i is an isomorphism. In particular, α_1 is an isomorphism. That is,

$$\begin{tikzcd}
I/I^{n+1} \otimes_R M \arrow[r, "\alpha_1"] \arrow[d, "="'] & IM/I^{n+1}M \arrow[d, "="] \\
IR_n \otimes_{R_n} M_n \arrow[r, "\cong"] & IM_n
\end{tikzcd}$$

commutes and the arrows are all isomorphisms. This proves that hypothesis (3) is satisfied for the ring R_n, the ideal IR_n and the module M_n. Because (3) implies (2), $\operatorname{Tor}_1^{R_n}(N,M_n) = 0$ for all R_0-modules N. Say $1 \le j \le n$ and A is an $R_j = R/I^{j+1}$-module. Then IA and A/IA are R/I^j-modules. From the exact sequence

$$0 \to IA \to A \to A/IA \to 0$$

we get the exact sequence

$$\operatorname{Tor}_1^{R_n}(IA,M_n) \to \operatorname{Tor}_1^{R_n}(A,M_n) \to \operatorname{Tor}_1^{R_n}(A/IA,M_n).$$

If $j = 1$, this implies $\operatorname{Tor}_1^{R_n}(A,M_n) = 0$. Induction on j shows $\operatorname{Tor}_1^{R_n}(A,M_n) = 0$ for any R_n-module A. This implies M_n is a flat R_n-module.

(1) implies (6): The attribute of being flat is preserved under change of base (Theorem 2.3.23).

(6) and (A) implies (1): If I is nilpotent, then $I^n = 0$ for some n. In this case, $M/I^nM = M$ is a flat $R/I^n = R$-module.

(6) and (B) implies (1). Let J be any finitely generated ideal of R. By Corollary 3.7.4 it is enough to show

$$0 \to J \otimes_R M \xrightarrow{\mu} M \to M/JM$$

is an exact sequence. We are assuming (B), which implies $\bigcap_n I^n(J \otimes_R M) = 0$. It is enough to show $\ker(\mu) \subseteq I^n(J \otimes_R M)$ for each $n > 0$. By Corollary 7.2.14 there exists $\nu \ge n$ such that $J \cap I^\nu \subseteq I^nJ$. Consider the commutative diagram

$$\begin{tikzcd}
J \otimes_R M \arrow[r, "\phi"] \arrow[d, "\mu"] & \big(J/(J \cap I^\nu)\big) \otimes_R M \arrow[r, "\psi"] \arrow[d, "\tau"] & \big(J/I^nJ\big) \otimes_R M \arrow[d] \\
M \arrow[r] & M/I^\nu M \arrow[r] & M/I^nM
\end{tikzcd} \tag{4.1}$$

The kernel of the composition $\psi\phi$ is $\ker(\psi\phi) = I^nJ \otimes_R M = I^n(J \otimes_R M)$. By hypothesis (6), $M/I^\nu M$ is a flat module over R/I^ν. Since $J/(J \cap I^\nu)$ is an ideal in R/I^ν, by Corollary 3.7.4, the sequence

$$0 \to \big(J/(J \cap I^\nu)\big) \otimes_{R/I^\nu} \big(M/I^\nu M\big) \to M/I^\nu M$$

is exact. Since $\left(J/J\cap I^{\nu}\right)\otimes_{R/I^{\nu}}\left(M/I^{\nu}M\right)=\left(J/J\cap I^{\nu}\right)\otimes_R M$, this implies the sequence

$$0\to\left(J/J\cap I^{\nu}\right)\otimes_R M\xrightarrow{\tau}M/I^{\nu}M$$

is exact. In (4.1), since τ is one-to-one it follows that $\ker(\mu)\subseteq\ker(\psi\phi)=I^n(J\otimes_R M)$. $\square$

As an application of Theorem 10.4.13 we prove the following generalization of Corollary 3.4.3.

PROPOSITION 10.4.14. *Assume all of the following are satisfied.*

(A) R *is a noetherian local ring with maximal ideal* $\mathfrak{m}$ *and residue field* $k(\mathfrak{m})$.
(B) S *is a noetherian local ring with maximal ideal* $\mathfrak{n}$ *and residue field* $k(\mathfrak{n})$.
(C) $f:R\to S$ *is a local homomorphism of local rings (that is,* $f(\mathfrak{m})\subseteq\mathfrak{n}$*).*
(D) A *and* B *are finitely generated* S*-modules,* $\sigma\in\operatorname{Hom}_S(A,B)$*, and* B *is a flat* R*-module.*

Then the following are equivalent.

(1) The sequence

$$0\to A\xrightarrow{\sigma}B\to\operatorname{coker}(\sigma)\to 0$$

is exact and $\operatorname{coker}(\sigma)$ *is a flat* R*-module.*

(2) The sequence

$$0\to A\otimes_R k(\mathfrak{m})\xrightarrow{\sigma\otimes 1}B\otimes_R k(\mathfrak{m})\to\operatorname{coker}(\sigma)\otimes_R k(\mathfrak{m})\to 0$$

is exact.

PROOF. (1) implies (2): Start with the short exact sequence in (1). Apply the functor $(\ )\otimes_R k(\mathfrak{m})$. The long exact Tor sequence includes these terms

$$\cdots\to\operatorname{Tor}_1^R(\operatorname{coker}(\sigma),k(\mathfrak{m}))\to A\otimes_R k(\mathfrak{m})\xrightarrow{\sigma\otimes 1}B\otimes_R k(\mathfrak{m})\to\operatorname{coker}(\sigma)\otimes_R k(\mathfrak{m})\to 0.$$

Use the fact that $\operatorname{coker}(\sigma)$ is flat to get (2).

(2) implies (1): For any R-module M, identify $M\otimes_R k(\mathfrak{m})$ with $M/\mathfrak{m}M$. The diagram

$$\begin{tikzcd}
 & \mathfrak{m}A \arrow[d] & \mathfrak{m}B \arrow[d] & \mathfrak{m}\operatorname{coker}\sigma \arrow[d] & \\
 & A \arrow[r, "\sigma"] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & \operatorname{coker}\sigma \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A/\mathfrak{m}A \arrow[r, "\tau"] & B/\mathfrak{m}B \arrow[r] & \operatorname{coker}\sigma/\mathfrak{m}\operatorname{coker}\sigma \arrow[r] & 0
\end{tikzcd}$$

commutes. The rows and columns are exact. The three vertical arrows α,β,γ are onto.

Step 1: Show that $\ker(\sigma)=0$. If $x\in\ker(\sigma)$, then $x\in\mathfrak{m}A$. The idea is to show

$$x\in\bigcap_{n\geq 1}\mathfrak{m}^nA\subseteq\bigcap_{n\geq 1}\mathfrak{n}^nA,$$

which proves $x=0$, by Corollary 7.3.6. Fix $n\geq 1$ and assume $x\in\mathfrak{m}^nA$. Since $\mathfrak{m}^n$ is finitely generated over R, the vector space $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is finite dimensional over $k(\mathfrak{m})$. Let $\pi_1,\dots,\pi_r$ be a set of generators for $\mathfrak{m}^n$ which restricts to a $k(\mathfrak{m})$-basis for $\mathfrak{m}^n/\mathfrak{m}^{n+1}$. Write $x=\sum_{i=1}^r\pi_i x_i$ where $x_i\in A$. Then $0=\sigma(x)=\sum\pi_i\sigma(x_i)$ in the flat R-module B. By Corollary 3.7.4 there exist an integer s, elements $\{b_{ij}\mid 1\leq i\leq r,1\leq j\leq s\}$ in R, and $y_1,\dots,y_s$ in B satisfying $\sum_i\pi_i b_{ij}=0$ for all j and $\sigma(x_i)=\sum_j b_{ij}y_j$ for all i. Since $\pi_1,\dots,\pi_r$ are linearly independent over $k(\mathfrak{m})$, each b_{ij} is in $\mathfrak{m}$. This implies each $\sigma(x_i)$ is in $\mathfrak{m}B$. Since τ is one-to-one, this implies each x_i is in $\mathfrak{m}A$. We conclude that $x \in \mathfrak{m}^{n+1}A$. As stated already, this proves $x = 0$.

Step 2: Show that $\operatorname{coker}(\sigma)$ is a flat R-module. By Step 1, the sequence

$$0 \to A \xrightarrow{\sigma} B \to \operatorname{coker}(\sigma) \to 0$$

is exact. Apply the functor $(\,) \otimes_R k(\mathfrak{m})$. Since B is a flat R-module, the long exact Tor sequence reduces to the exact sequence

$$0 \to \operatorname{Tor}_1^R(\operatorname{coker}(\sigma), k(\mathfrak{m})) \to A \otimes_R k(\mathfrak{m}) \xrightarrow{\sigma\otimes 1} B \otimes_R k(\mathfrak{m}) \to \operatorname{coker}(\sigma) \otimes_R k(\mathfrak{m}) \to 0.$$

By assumption, $\sigma \otimes 1$ is one-to-one, so $\operatorname{Tor}_1^R(\operatorname{coker}(\sigma), k(\mathfrak{m})) = 0$. By Example 10.4.12 (1) the hypotheses of Theorem 10.4.13 (4) are satisfied. Therefore $\operatorname{coker}(\sigma)$ is a flat R-module. □

COROLLARY 10.4.15. *Assume all of the following are satisfied.*

(1) R is a noetherian commutative ring.
(2) S is a noetherian commutative R-algebra.
(3) M is a finitely generated S-module which is a flat R-module and $f \in S$.
(4) For each maximal ideal $\mathfrak{m} \in \operatorname{Max} S$,

$$0 \to M/(\mathfrak{m}\cap R)M \xrightarrow{\ell_f} M/(\mathfrak{m}\cap R)M$$

is exact, where ℓ_f is left multiplication by f.

Then

$$0 \to M \xrightarrow{\ell_f} M \to M/fM \to 0$$

is exact and M/fM is a flat R-module.

PROOF. Let $\mathfrak{m} \in \operatorname{Max} S$ and $\mathfrak{n} = \mathfrak{m} \cap R$. Then $M_{\mathfrak{m}}$ is a finitely generated $S_{\mathfrak{m}}$-module. By Corollary 8.3.6, $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{n}}$-module. By assumption,

$$0 \to M \otimes_R (R/\mathfrak{n}) \xrightarrow{\ell_f} M \otimes_R (R/\mathfrak{n})$$

is exact. Since $S_{\mathfrak{m}}$ is a flat S-module,

$$0 \to M_{\mathfrak{m}} \otimes_R (R/\mathfrak{n}) \xrightarrow{\ell_f} M_{\mathfrak{m}} \otimes_R (R/\mathfrak{n})$$

is exact. By Exercise 3.1.6, $R_{\mathfrak{n}}/(\mathfrak{n}R_{\mathfrak{n}})$ is a flat $R/\mathfrak{n}$-module. Therefore,

$$0 \to M_{\mathfrak{m}} \otimes_{R_{\mathfrak{n}}} (R_{\mathfrak{n}}/\mathfrak{n}R_{\mathfrak{n}}) \xrightarrow{\ell_f} M_{\mathfrak{m}} \otimes_{R_{\mathfrak{n}}} (R_{\mathfrak{n}}/\mathfrak{n}R_{\mathfrak{n}})$$

is exact. We are in the context of Proposition 10.4.14 with the rings being $R_{\mathfrak{n}}$, $S_{\mathfrak{m}}$, and σ being $\ell_f : M_{\mathfrak{m}} \to M_{\mathfrak{m}}$. We have shown that Proposition 10.4.14 condition (2) is satisfied. Therefore, the sequence

$$0 \to M_{\mathfrak{m}} \xrightarrow{\ell_f} M_{\mathfrak{m}} \to M_{\mathfrak{m}}/fM_{\mathfrak{m}} \to 0$$

is exact, and $(M/fM) \otimes_S S_{\mathfrak{m}} = M_{\mathfrak{m}}/fM_{\mathfrak{m}}$ is a flat $R_{\mathfrak{n}}$-module. By Proposition 3.1.9, $\ell_f : M \to M$ is one-to-one. By Corollary 8.3.6, M/fM is a flat R-module. □

COROLLARY 10.4.16. *Let R be a commutative noetherian ring and $S = R[x_1, \dots, x_n]$ the polynomial ring over R in n indeterminates. Let $f \in S$ and assume the coefficients of f generate the unit ideal in R. Then f is not a zero divisor of S and S/fS is a flat R-algebra.*

PROOF. Let $\mathfrak{m} \in \operatorname{Max} S$ and $\mathfrak{n} = \mathfrak{m} \cap R$. Then $R/\mathfrak{n}$ is an integral domain and $f \notin \mathfrak{n}[x_1, \dots, x_n]$. Moreover, $S/\mathfrak{n}S = S \otimes_R R/\mathfrak{n} = (R/\mathfrak{n})[x_1, \dots, x_n]$, so $\ell_f : S/\mathfrak{n}S \to S/\mathfrak{n}S$ is one-to-one. The rest follows from Corollary 10.4.15. □

COROLLARY 10.4.17. *Let $\theta : R \to S$ be a local homomorphism of commutative noetherian local rings. Let M be a finitely generated S-module which is flat over R. Let $\mathfrak{m}$ be the maximal ideal of R and $k(\mathfrak{m})$ the residue field. For any $f \in S$, let ℓ_f be the left multiplication by f map. Then the following are equivalent.*

(1) The sequence

$$0 \to M \xrightarrow{\ell_f} M \to M/fM \to 0$$

is exact, and M/fM is flat over R.

(2) The sequence

$$0 \to M \otimes_R k(\mathfrak{m}) \xrightarrow{\ell_f} M \otimes_R k(\mathfrak{m})$$

is exact.

PROOF. Apply Proposition 10.4.14. □

In Corollary 10.4.18, the reader is referred to Definition 11.3.1 for the definition of a regular sequence for an R-module contained in an ideal of R.

COROLLARY 10.4.18. *Let $\theta : R \to S$ be a local homomorphism of commutative noetherian local rings. Let M be a finitely generated S-module which is flat over R. Let $\mathfrak{m}$ be the maximal ideal of R and $k(\mathfrak{m})$ the residue field. Let $\mathfrak{n}$ be the maximal ideal of S, and $(f_1,\dots,f_r)$ a regular sequence for $M \otimes_R k(\mathfrak{m})$ in $\mathfrak{n}$. Then $(f_1,\dots,f_r)$ is a regular sequence for M and $M/(f_1,\dots,f_r)M$ is flat over R.*

PROOF. Use Corollary 10.4.17 and induction on r. □

4.3. Theorem of Generic Flatness.

THEOREM 10.4.19. *Let R be a noetherian integral domain and S a finitely generated commutative R-algebra. For any finitely generated S-module M, there exists a nonzero element f in R such that the localization $M[f^{-1}] = M \otimes_R R[f^{-1}]$ is a free $R[f^{-1}]$-module.*

PROOF. Step 1: If M is not a faithful R-module, then we can take f to be a nonzero element of $\operatorname{annih}_R(M)$. From now on we assume S is an extension ring of R and M is a faithful R-module.

Step 2: By Theorem 9.2.10, there exists a filtration $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$ of M and a set of prime ideals $P_i \in \operatorname{Spec} S$ such that $M_i/M_{i-1} \cong S/P_i$ for $i = 1,\dots,n$. If

$$0 \to A \to B \to C \to 0$$

is an exact sequence of R-modules where A and C are free, then so is B. It is enough to prove the theorem for the case where $M = S/P$, for a prime ideal P in S. From now on assume $M = S$ and S is an integral domain which is an extension ring of R.

Step 3: Let K be the quotient field of R and L the quotient field of S. Consider $SK = S \otimes_R K$, the K-subalgebra of L generated by S. Since S is a finitely generated R-algebra, SK is a finitely generated K-algebra. The Krull dimension of SK, $n = \dim(SK)$, is finite. The proof is by induction on the integer n.

Step 4: Assume $n = 0$. That is, $SK = L$ is the quotient field of S. Let $s_1,\dots,s_k$ be a set of generators for S as an R-algebra. Each s_i is integral over K, so there exists a polynomial $p_i(x) \in K[x]$ such that $p_i(s_i) = 0$. There exists a nonzero element α in $R - (0)$ such that $\alpha p_i(x) \in R[x]$ for all i. Therefore, $R[\alpha^{-1}] \subseteq S[\alpha^{-1}]$ is a finitely generated integral extension of integral domains. By Theorem 6.1.3 (1), $S_1 = S[\alpha^{-1}]$ is finitely generated as an $R_1 = R[\alpha^{-1}]$-module. Let $u_1,\dots,u_\nu$ be a maximal subset in S_1 which is linearly independent over R_1. Define $\phi : R_1^{(\nu)} \to S_1$ by $(a_1,\dots,a_\nu) \mapsto \sum a_i u_i$. Let $C = \operatorname{coker}\phi$.

Then C is a finitely generated torsion R_1-module. Let $\gamma \in \operatorname{annih}_{R_1}(C)$. Tensor ϕ with $R_1[\gamma^{-1}]$ to get $R_1[\gamma^{-1}] \cong S_1[\gamma^{-1}]$. Take f to be $\alpha\gamma$.

Step 5: Assume $n \geq 1$. By Noether's Normalization Lemma (Corollary 10.3.3), there exist $y_1, \ldots, y_n$ in SK which are algebraically independent over K and such that SK is integral over $K[y_1, \ldots, y_n]$. For some element β of $R - (0)$, $\beta y_i \in S$. Re-label if necessary, and assume $R[y_1, \ldots, y_n] \subseteq S$. There exist $s_1, \ldots, s_k$ such that $S = R[s_1, \ldots, s_k]$. Each s_i is integral over $K[y_1, \ldots, y_n]$, so there exists a polynomial $p_i(x) \in K[y_1, \ldots, y_n][x]$ such that $p_i(s_i) = 0$. There exists a nonzero element α in $R - (0)$ such that $\alpha p_i(x) \in R[y_1, \ldots, y_n][x]$ for all i. Therefore, $R[\alpha^{-1}][y_1, \ldots, y_n] \subseteq S[\alpha^{-1}]$ is an integral extension of integral domains. Let $R_1 = R[\alpha^{-1}]$, $S_1 = S[\alpha^{-1}]$, and $T = R_1[y_1, \ldots, y_n]$. Then S_1 is a finitely generated integral extension of T, so by Theorem 6.1.3 (1), S_1 is finitely generated as a T-module. Let $u_1, \ldots, u_\nu$ be a maximal subset in S_1 which is linearly independent over T. Define $\phi : T^{(\nu)} \to S_1$ by $(a_1, \ldots, a_\nu) \mapsto \sum a_i u_i$. Let $C = \operatorname{coker} \phi$. Then C is a finitely generated T-module. As in Step 2, there is a filtration of the T-module C. Since C is a torsion T-module, for each prime ideal P of T that occurs in the filtration, $\operatorname{ht}(P) \geq 1$. Consider one such prime $P \in \operatorname{Spec} T$. By Step 1, assume T/P is an extension of R_1. Then

$$T/P \otimes_R K = \frac{T \otimes_R K}{P \otimes_R K}.$$

Since $P \otimes_R K$ is a nonzero prime ideal in $T \otimes_R K$, $\dim_K(T/P \otimes_R K) < n$. By induction, there exists $g \in R_1 - (0)$ such that $T/P \otimes_{R_1} R_1[g^{-1}]$ is a free $R_1[g^{-1}]$-module. Since R_1 is an integral domain, we can find one $g \in R_1 - (0)$ such that $C \otimes_{R_1} R_1[g^{-1}]$ is a free $R_1[g^{-1}]$-module. Since T is a free R_1-module, this proves $S_1 \otimes_{R_1} R_1[g^{-1}] = S \otimes_R R[f^{-1}]$ is a free $R[f^{-1}]$-module for $f = \alpha g$. $\square$

COROLLARY 10.4.20. *Let R be a noetherian integral domain and S a faithful finitely generated commutative R-algebra. There exists a nonzero element f in R such that $S[f^{-1}]$ is a faithful $R[f^{-1}]$-algebra which is free as an $R[f^{-1}]$-module.*

In the language of Algebraic Geometry, Corollary 10.4.20 has the following interpretation. Let $\phi : R \to S$ be the structure homomorphism. Then over the nonempty open subscheme $U = U(f) = \operatorname{Spec} R - V(f)$, $\phi^\sharp$ is faithfully flat. That is, if $V = (\phi^\sharp)^{-1}(U)$, then the restriction of $\phi^\sharp$ to $V \to U$ is a faithfully flat morphism.

THEOREM 10.4.21. *Let R be a commutative noetherian ring, S a finitely generated commutative R-algebra, and M a finitely generated S-module. Let U be the set of all points P in $\operatorname{Spec} S$ such that $M_P = M \otimes_S S_P$ is a flat R-module. Then*

(1) U is an open (possibly empty) subset of $\operatorname{Spec} S$.
(2) If going down holds for $R \to S$ (in particular, if S is flat over R), then the image of U in $\operatorname{Spec} R$ is open.

PROOF. The idea is to apply Lemma 10.4.9 (2) to show that U is open. If U is empty, there is nothing to prove.

Step 1: First we show that U is stable under generalization. Let $P \in U$ and assume Q is a generalization of P. The functor $(\cdot) \otimes_R M_P$ from $\mathfrak{M}_R$ to $\mathfrak{M}_{S_P}$ is exact since $P \in U$. The functor $(\cdot) \otimes_{S_P} S_Q$ from $\mathfrak{M}_{S_P}$ to $\mathfrak{M}_{S_Q}$ is exact since S_Q is a localization of S_P. Thus $(\cdot) \otimes_R M_P \otimes_{S_P} S_Q = (\cdot) \otimes_R M_Q$ is exact. This shows $Q \in U$.

Step 2: Assume $P \in U$ and prove that U contains a nonempty open subset of the irreducible closed set $V(P)$. Let $I = P \cap R$ and let $Q \in V(P)$. Then $IS_Q \subseteq QS_Q$, so by Example 10.4.12 (1), M_Q is ideal-wise separated for I. Let $R_0 = R/I$ and $(M_Q)_0 = M_Q/IM_Q$.

By the local criteria for flatness (Theorem 10.4.13), M_Q is a flat R-module if and only if $(M_Q)_0$ is a flat R_0-module and $\operatorname{Tor}_1^R(M_Q,R_0)=(0)$.

Step 2.1: By Theorem 10.4.19 applied to R_0, $S_0=S/IS$, and $M_0=M/IM$, there exists $f\in(R-I)\subseteq(S-P)$ such that $M_0[f^{-1}]$ is a free $R_0[f^{-1}]$-module. Let $W=(\operatorname{Spec}S-V(f))\cap V(P)$. Since W consists of those specializations of P that do not contain f, W is an open subset of $V(P)$ which contains P. For $Q\in W$, S_Q is a localization of $S[f^{-1}]$, so by Exercise 3.1.7, S_Q/IS_Q is a localization of $S_0[f^{-1}]$. It follows from these observations that the functor $(\cdot)\otimes_{R_0}M_0[f^{-1}]$ from $\mathfrak{M}_{R_0}$ to $\mathfrak{M}_{S_0[f^{-1}]}$ is exact, and the functor $(\cdot)\otimes_{S_0[f^{-1}]}(S_Q/IS_Q)$ from $\mathfrak{M}_{S_0[f^{-1}]}$ to $\mathfrak{M}_{S_Q/IS_Q}$ is exact. Combining the two, it follows that $(\cdot)\otimes_{R_0}M_0[f^{-1}]\otimes_{S_0[f^{-1}]}(S_Q/IS_Q)=(\cdot)\otimes_{R_0}(M_Q)_0$ is exact. This shows $(M_Q)_0$ is R_0-flat for all Q in the nonempty open $W\subseteq V(P)$.

Step 2.2: Since $P\in U$, $\operatorname{Tor}_1^R\big(M_P,R_0\big)=0$. By Lemma 8.3.5, $\operatorname{Tor}_1^R(M,R_0)\otimes_S S_P=0$. Again by Lemma 8.3.5, $\operatorname{Tor}_1^R(M,R_0)$ is a finitely generated S-module. By Lemma 3.1.10, there exists an open neighborhood T of P in $\operatorname{Spec}S$ such that $\operatorname{Tor}_1^R(M,R_0)\otimes_S S_Q=0$ for all $Q\in T$. By Lemma 8.3.5, $\operatorname{Tor}_1^R\big(M_Q,R_0\big)=0$ for all Q in the nonempty open $T\subseteq V(P)$.

Step 2.3: If W is from Step 2.1 and T is from Step 2.2, then for all Q in $W\cap T$, M_Q is flat over R. Therefore U contains $W\cap T$ which is a nonempty open subset of $V(P)$. $\square$

5. Complete I-adic Rings and Inverse Limits

The main result of this section, Corolary 10.5.4, provides sufficient conditions on a directed system of noetherian local rings such that the direct limit is again a noetherian local ring. The proof is a compilation of results from all of the following sources: [**41**], [**12**], [**48**], and [**22**].

PROPOSITION 10.5.1. *Let $\{A_i,\phi_i^j\}$ be an inverse system of discrete commutative rings for the index set $\{0,1,2,\dots\}$. Let $\{M_i,\psi_i^j\}$ be an inverse system of modules over the inverse system of rings $\{A_i,\phi_i^j\}$. For each $0\le i\le j$, define $\mathfrak{n}_j$ to be the kernel of $\phi_0^j:A_j\to A_0$, assume $\phi_i^i:A_i\to A_i$ is the identity mapping, and*

$$0\to\mathfrak{n}_j^{i+1}\to A_j\xrightarrow{\phi_i^j}A_i\to 0$$

and

$$0\to\mathfrak{n}_j^{i+1}M_j\to M_j\xrightarrow{\psi_i^j}M_i\to 0$$

are exact sequences. If $A=\varprojlim A_i$ and $M=\varprojlim M_i$, then the following are true.

(1) *A is a separated and complete topological ring, M is a separated and complete topological A-module, and the natural maps $\alpha_j:A\to A_j$, $\beta_j:M\to M_j$, are onto.*
(2) *If M_0 is a finitely generated A_0-module, then M is a finitely generated A-module. More specifically, if S is a finite subset of M and $\beta_0(S)$ is a generating set for M_0, then S is a generating set for M.*

PROOF. (1): This follows from Proposition 7.1.7, Corollary 7.1.10, and the definition of inverse limit (Definition 2.7.12).

(2): For all $\ell \leq k$, the diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{n}_{i+\ell}^{i+1} \arrow[r] \arrow[d] & A_{i+\ell} \arrow[r, "\phi_i^{i+\ell}"] \arrow[d, "\phi_{i+k}^{i+\ell}"] & A_i \arrow[r] \arrow[d, "\phi_i^i"] & 0 \\ 0 \arrow[r] & \mathfrak{n}_{i+k}^{i+1} \arrow[r] & A_{i+k} \arrow[r, "\phi_i^{i+k}"] & A_i \arrow[r] & 0 \end{tikzcd}$$

commutes and the vertical arrows are onto. By Proposition 2.7.19, if we define $\mathfrak{m}_{i+1}$ to be the kernel of $\alpha_i : A \to A_i$, then

$$\mathfrak{m}_{i+1} = \varprojlim_k \mathfrak{n}_{i+k}^{i+1}.$$

Similarly, if we set N_{i+1} to be the kernel of $\beta_i : M \to M_i$, then

$$N_{i+1} = \varprojlim_k \mathfrak{n}_{i+k}^{i+1} M_{i+k}.$$

It follows from the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{m}_{i+k+1} \arrow[r] \arrow[d] & A \arrow[r, "\alpha_{i+k}"] \arrow[d, "="] & A_{i+k} \arrow[r] \arrow[d, "\phi_i^{i+k}"] & 0 \\ 0 \arrow[r] & \mathfrak{m}_{i+1} \arrow[r] & A \arrow[r, "\alpha_i"] & A_i \arrow[r] & 0 \end{tikzcd}$$

that

$$\alpha_{i+k}(\mathfrak{m}_{i+1}) = \ker \phi_i^{i+k} = \mathfrak{n}_{i+k}^{i+1}. \tag{5.1}$$

Likewise,

$$\beta_{i+k}(N_{i+1}) = \mathfrak{n}_{i+k}^{i+1} M_{i+k}. \tag{5.2}$$

For $i \geq 1$ and $j \geq 1$,

$$\begin{aligned} \beta_{i+j-1}(\mathfrak{m}_i N_j) &= \alpha_{i+j-1}(\mathfrak{m}_i)\beta_{i+j-1}(N_j) \\ &= \mathfrak{n}_{i+j-1}^i \mathfrak{n}_{i+j-1}^j M_{i+j-1} \\ &= \mathfrak{n}_{i+j-1}^{i+j} M_{i+j-1} \\ &= 0 \end{aligned}$$

since $\mathfrak{n}_{i+j-1}^{i+j}$ is the kernel of α_{i+j}^{i+j}. This shows that $\mathfrak{m}_i N_j \subseteq \ker \beta_{i+j-1} = N_{i+j}$. Similarly, one checks that $\mathfrak{m}_i \mathfrak{m}_j \subseteq \mathfrak{m}_{i+j}$. Defining $\mathfrak{m}_0 = A$, and $N_0 = M$, $\{\mathfrak{m}_i\}$ is a filtration on A and $\{N_i\}$ is a compatible filtration on M. The reader should verify that the topologies on A and M are those defined by the filtrations $\{\mathfrak{m}_i\}$ and $\{N_i\}$.

Let S be a finite subset of M and assume $\beta_0(S)$ is a generating set for M_0. Let M' be the submodule of M generated by S. Let $\mathfrak{a}$ be an ideal in A such that $\alpha_1(\mathfrak{a}) = \mathfrak{n}_1$. We are going to prove

$$N_i = \mathfrak{a}^i M' + N_{i+1} \tag{5.3}$$

for all $i \geq 0$. Define $\mathfrak{a}_i = \alpha_i(\mathfrak{a})$ and $M'_i = \beta_i(M')$. Since $N_{i+1} = \ker \beta_i$, to prove (5.3) it suffices to prove

$$\beta_i(N_i) = \beta_i(\mathfrak{a}^i M') = \alpha_i(\mathfrak{a}^i)\beta_i(M') = \mathfrak{a}_i^i M'_i. \tag{5.4}$$

Since $\beta_0(N_0) = \beta_0(M) = M_0$ is equal to $M'_0 = \beta_0(M') = M_0$, we see that (5.4) is satisfied for $i = 0$. For $i \geq 1$, the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{n}_i \arrow[r] \arrow[d] & A_i \arrow[r, "\phi_0^i"] \arrow[d, "\phi_1^i"] & A_0 \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & \mathfrak{n}_1 \arrow[r] & A_1 \arrow[r, "\phi_0^1"] & A_0 \arrow[r] & 0
\end{tikzcd}$$

commutes and the vertical arrows are onto. Therefore, $\phi_1^i(\mathfrak{n}_i) = \mathfrak{n}_1$. Since the diagram

$$\begin{tikzcd}
A \arrow[r, "\alpha_1"] \arrow[dr, "\alpha_i"'] & A_1 \\
& A_i \arrow[u, "\phi_1^i"']
\end{tikzcd}$$

commutes, $\phi_1^i(\mathfrak{n}_i) = \mathfrak{n}_1 = \alpha_1(\mathfrak{a}) = \phi_1^i\alpha_i(\mathfrak{a}) = \phi_1^i(\mathfrak{a}_i)$. Since $\mathfrak{n}_i^2 = \ker\phi_1^i$, it follows that $\mathfrak{n}_i = \mathfrak{a}_i + \mathfrak{n}_i^2$. For $i \geq 1$ the diagram

$$\begin{tikzcd}
M \arrow[r, "\beta_0"] \arrow[dr, "\beta_i"'] & M_0 \\
& M_i \arrow[u, "\psi_0^i"']
\end{tikzcd}$$

commutes and ψ_0^i is onto. Therefore, $\psi_0^i(M'_i) = \psi_0^i\beta_i(M') = \beta_0(M') = M_0 = \psi_0^i(M_i)$. Since $\mathfrak{n}_iM_i = \ker\psi_0^i$, it follows that $M_i = M'_i + \mathfrak{n}_iM_i$. Combining these results, we have

$$\mathfrak{n}_i^iM_i = (\mathfrak{a}_i + \mathfrak{n}_i^2)^i(M'_i + \mathfrak{n}_iM_i). \tag{5.5}$$

For $0 \leq k \leq i$ we have $\mathfrak{a}_i^k\mathfrak{n}_i^{i+1-k} \subseteq \mathfrak{n}_i^{i+1} = 0$. From this and (5.2), we see that (5.5) collapses to

$$\beta_i(N_i) = \mathfrak{n}_i^iM_i = \mathfrak{a}_i^iM'_i.$$

Together with (5.4), this proves (5.3).

From (5.1), $\mathfrak{m}_1 = \alpha_1^{-1}(\mathfrak{n}_1)$. Therefore, $\mathfrak{a} \subseteq \mathfrak{m}_1$, and $\mathfrak{a}^i \subseteq \mathfrak{m}_1^i \subseteq \mathfrak{m}_i$. From (5.3), this shows $N_i \subseteq m_iM' + N_{i+1}$. On the other hand, $m_iM \subseteq N_i$, from which it follows that

$$N_i = m_iM' + N_{i+1}.$$

It follows from Corollary 7.3.13 that $M' = M$. □

COROLLARY 10.5.2. *In the context of Proposition 10.5.1, assume M_0 is a finitely generated A_0-module and that the ideal $\mathfrak{n}_1$ of A_1 is finitely generated. Let $\mathfrak{m}_1$ be the kernel of $\alpha_0 : A \to A_0$. Then the following are true.*

(1) *The topologies on A and M are the $\mathfrak{m}_1$-adic topologies.*
(2) *For all $i \geq 0$, the sequences*

$$0 \to \mathfrak{m}_1^{i+1} \to A \xrightarrow{\alpha_i} A_i \to 0$$

and

$$0 \to \mathfrak{m}_1^{i+1}M \to M \xrightarrow{\beta_i} M_i \to 0$$

are exact.

(3) *$\mathfrak{m}_1/\mathfrak{m}_1^2$ is a finitely generated A-module.*

PROOF. We retain the notation established in the proof of Proposition 10.5.1. Since $\mathfrak{n}_1$ is a finitely generated ideal in A_1, we assume $\mathfrak{a}$ is a finitely generated ideal in A such that $\alpha_1(\mathfrak{a}) = \mathfrak{n}_1$. Let $i \geq 0$ be any integer. Since $\mathfrak{a}$ and M are finitely generated A-modules, so is $\mathfrak{a}^i M$. For all $j \geq 0$, it follows from (5.3) that

$$N_{i+j} = \mathfrak{a}^j(\mathfrak{a}^i M) + N_{i+j+1} \subseteq \mathfrak{m}_j(\mathfrak{a}^i M) + N_{i+j+1}.$$

On the other hand, $\mathfrak{m}_j(\mathfrak{a}^i M) \subseteq \mathfrak{m}_j \mathfrak{m}_i M \subseteq \mathfrak{m}_{i+j} M \subseteq N_{i+j}$. This shows

$$N_{i+j} = \mathfrak{m}_j(\mathfrak{a}^i M) + N_{i+j+1}.$$

Define a filtration $\{N_{ij}\}_{j \in \mathbb{Z}}$ on N_i by

$$N_{ij} = \begin{cases} N_i & \text{if } j < 0 \\ N_{i+j} & \text{if } j \geq 0. \end{cases}$$

Applying Corollary 7.3.13, we obtain $N_i = \mathfrak{a}^i M$. Since $\mathfrak{a}^i \subseteq \mathfrak{m}_1^i \subseteq \mathfrak{m}_i$, we have $N_i \subseteq \mathfrak{m}_1^i M \subseteq \mathfrak{m}_i M \subseteq N_i$. Hence, $N_i = \mathfrak{m}_1^i M$. If we take $M_i = A_i$, this shows $\mathfrak{m}_i = \mathfrak{m}_1^i$, and the proof of (1) is complete. Part (2) follows from (1) and the definitions for $\mathfrak{m}_i$ and N_i. By (5.3), $\mathfrak{m}_1 = \mathfrak{a} + \mathfrak{m}_1^2$, which proves Part (3). □

EXAMPLE 10.5.3. Let R be a commutative ring and I an ideal in R such that I/I^2 is a finitely generated R/I-module. Let $\hat{R} = \varprojlim_n R/I^n$ be the separated completion of R. With respect to the filtration $\{\widehat{I^n}\}$, $\hat{R}$ is separated and complete (Corollary 7.1.10). The reader should verify that the inverse system of rings $\{R/I^n\}$ satisfies the hypotheses of Corollary 10.5.2, hence the topology on $\hat{R}$ is the $\hat{I}$-adic topology. Moreover, $\hat{I}/\hat{I}^2 \cong I/I^2$ is finitely generated over $\hat{R}/\hat{I}$.

COROLLARY 10.5.4. *Let $\{A_i, \phi_j^i\}$ be a directed system of commutative local rings for a directed index set I. Let $\mathfrak{m}_i$ denote the maximal ideal of A_i. For each $i \leq j$, assume $\phi_j^i : A_i \to A_j$ is a local homomorphism of local rings. If $A = \varinjlim A_i$, then the following are true.*

(1) A is a local ring with maximal ideal $\mathfrak{m} = \varinjlim_i \mathfrak{m}_i$, each homomorphism $\alpha_i : A_i \to A$ is a local homomorphism of local rings, and the residue field of A is $\varinjlim_i A_i/\mathfrak{m}_i$.
(2) If $\mathfrak{m}_j = \mathfrak{m}_i A_j$, for each $i \leq j$, then $\mathfrak{m}_i A = \mathfrak{m}$.
(3) For each $i \leq j$, assume $\mathfrak{m}_j = \mathfrak{m}_i A_j$ and A_j is a faithfully flat A_i-module. If each A_i is noetherian, then A is noetherian.

PROOF. (1): Let $\mathfrak{m} = \bigcup_i \alpha_i(\mathfrak{m}_i)$. The reader should verify that $\mathfrak{m}$ is the unique maximal ideal of A. Take the direct limit of the exact sequences

$$0 \to \mathfrak{m}_i \to A_i \to A_i/\mathfrak{m}_i \to 0$$

and apply Theorem 2.7.6 to get the exact sequence

$$0 \to \mathfrak{m} \to A \to A/\mathfrak{m} \to 0.$$

(2): The sequence $\mathfrak{m}_i \otimes_{A_i} A_j \to \mathfrak{m}_j \to 0$ is exact. The functor $\varinjlim_j(\ )$ is exact (Theorem 2.7.6) and commutes with tensor products (Proposition 2.7.8). Hence the sequence $\mathfrak{m}_i \otimes_{A_i} A \to \mathfrak{m} \to 0$ is exact.

(3): By Exercise 2.7.8 and Exercise 3.5.12, A is faithfully flat over each A_i. Therefore, $0 \to \mathfrak{m}_i^n \otimes_{A_i} A \to A_i \otimes_{A_i} A$ is exact, and $\mathfrak{m}_i^n \otimes_{A_i} A \to \mathfrak{m}_i^n A = \mathfrak{m}^n$ is an isomorphism. It follows that

$$\begin{aligned}
\mathfrak{m}^n/\mathfrak{m}^{n+1} &\cong (\mathfrak{m}_i^n A)/\left(\mathfrak{m}_i^{n+1}A\right) \\
&\cong \left(\mathfrak{m}_i^n/\mathfrak{m}_i^{n+1}\right) \otimes_{A_i} A \\
&\cong \left(\mathfrak{m}_i^n/\mathfrak{m}_i^{n+1}\right) \otimes_{A_i/\mathfrak{m}_i} (A_i/\mathfrak{m}_i \otimes_{A_i} A) \\
&\cong \left(\mathfrak{m}_i^n/\mathfrak{m}_i^{n+1}\right) \otimes_{A_i/\mathfrak{m}_i} A/\mathfrak{m}
\end{aligned}$$

are isomorphisms of $A/\mathfrak{m}$-vector spaces. Since A_i is noetherian, $\mathfrak{m}_i^n/\mathfrak{m}_i^{n+1}$ is a finite dimensional $A_i/\mathfrak{m}_i$-vector space. Therefore, $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is finite dimensional over $A/\mathfrak{m}$. Let $\hat{A} = \varprojlim A/\mathfrak{m}^n$. By (2), $\hat{A} = \varprojlim A/\mathfrak{m}_i^n A$, for each i. By Example 10.5.3 and Proposition 7.2.2, $\hat{A}$ is noetherian.

The maximal ideal of $\hat{A}$ is $\hat{\mathfrak{m}}$. By Proposition 7.3.1, we have $\hat{\mathfrak{m}} = \mathfrak{m}\hat{A} = \mathfrak{m}_i\hat{A}$, for each i. Because A is flat over A_i, $(A_i/\mathfrak{m}_i{}^n) \otimes_{A_i} A$ is flat over $A_i/\mathfrak{m}_i^n$. Therefore,

$$\hat{A}/\mathfrak{m}_i{}^n\hat{A} = A/\mathfrak{m}_i{}^n A = A_i/\mathfrak{m}_i^n \otimes_{A_i} A$$

is flat over $A_i/\mathfrak{m}_i^n$. In the terminology of Example 10.4.12 (1), the A_i-module $\hat{A}$ is idealwise separated for $\mathfrak{m}_i$. By (6) implies (1) of Theorem 10.4.13, it follows that $\hat{A}$ is flat over A_i. By Exercise 3.5.12, $\hat{A}$ is faithfully flat over A_i. By Exercise 2.7.9, $\hat{A}$ is faithfully flat over A. By Exercise 4.1.7, A is noetherian. □

CHAPTER 11

Normal Integral Domains

A commutative ring R is called a normal ring in case R_P is an integrally closed local integral domain, for every $P \in \operatorname{Spec} R$. The commutative ring R is called a regular ring in case R_P is a regular local ring, for every $P \in \operatorname{Spec} R$.

Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field k. In Theorem 11.1.8 we show that R is regular of Krull dimension n if and only if the graded ring $\operatorname{gr}_{\mathfrak{m}}(R)$ is isomorphic to a polynomial ring $k[x_1,\dots,x_n]$. In two important corollaries, we show that if R is regular, then R is normal. Also, the completion of R, $\hat{R}$, is noetherian, and $\hat{R}$ is regular if and only if R is regular.

Section 11.2 contains an introduction to valuations on a field F and the valuation ring associated to a valuation. A valuation ring is a normal integral domain, and if R is any subring of F, the integral closure of R in F is shown to be the intersection of the valuation rings of F that contain R. An important and useful type of valuation on a field is a discrete valuation. In this case, the associated valuation ring is a local principal ideal domain.

The subject of Section 11.3 are Cohen-Macaulay local rings. This class of rings properly contains the class of regular local rings.

The subject of Section 11.4 are noetherian normal integral domains. If R is a noetherian normal integral domain with field of fractions K, we show that for every height one prime P of R, the local ring R_P is a discrete valuation ring of K. The discrete valuation on K^* defined by the height one prime P is denoted ν_P. The free abelian group on the set of all height one primes of R, denoted $\operatorname{Div}(R)$, is called the group of Weil divisors of R. The divisor of $\alpha \in K^*$, denoted $\operatorname{Div}(\alpha)$, is the element of $\operatorname{Div}(R)$ which in coordinate P has coefficient $\nu_P(\alpha)$. The set of all such $\operatorname{Div}(\alpha)$ is a subgroup of $\operatorname{Div}(R)$ and the quotient group, denoted $\operatorname{Cl}(R)$, is called the class group of R. The class group of R is trivial if and only if R is a unique factorization domain.

The context of Section 11.5 is a faithfully flat extension $f : R \to S$ of commutative noetherian rings. We consider which properties of R are inherited by S. Conversely, we ask "If S has a certain property, does R also have that property?"

In Section 11.6 we derive some useful sets of sufficient criteria for a ring to be regular.

1. Normal Rings and Regular Rings

An integral domain R is said to be normal if R is integrally closed in its quotient field K. A commutative ring R is called normal if R_P is a normal local integral domain, for each prime P in $\operatorname{Spec} R$. A commutative ring R is called regular, if R_P is a regular local integral domain, for each prime P in $\operatorname{Spec} R$. We show that if R is normal, then $R[x]$ is normal. When I is an ideal of R contained in the Jacobson radical of R, important tests in terms of the graded ring $\operatorname{gr}_I(R)$ are derived for normality of R (Theorems 11.1.7 and 11.1.8). One corollary of this is that a regular local ring is normal (Corollary 11.1.9). Another corollary is that a noetherian local ring R is regular if and only if the completion $\hat{R}$ is regular (Corollary 11.1.10). A general reference for this section is [**41**, §17].

1.1. Normal Integral Domains.

DEFINITION 11.1.1. Let R be an integral domain with quotient field K. If R is integrally closed in K, then we say R is *normal*. Let $u \in K$. We say u is *almost integral over* R in case there exists $r \in R-(0)$ such that $ru^n \in R$ for all $n > 0$. We say R is *completely normal* in case the set of all elements in K that are almost integral over R is equal to R itself.

LEMMA 11.1.2. *Let R be an integral domain with quotient field K.*

(1) *If $u \in K$ and u is integral over R, then u is almost integral over R.*
(2) *If $u, v \in K$ are both almost integral over R, then $u+v$ and uv are almost integral over R.*
(3) *If R is noetherian and $u \in K$, then u is almost integral over R if and only if u is integral over R.*

PROOF. (1): By Proposition 6.1.2, there exists $m \geq 1$ such that $R[u]$ is generated as an R-module by $1, u, u^2, \dots, u^{m-1}$. Write $u = a/b$ for some $a, b \in R$. For $i = 1, \dots, m-1$ we have $b^{m-1}u^i \in R$. The rest is left to the reader.

(2): Is left to the reader.

(3): Assume u is almost integral and $r \in R-(0)$ such that $ru^n \in R$ for all $n > 0$. Consider $r^{-1}R$, which is a principal R-submodule of K. Hence $R[u]$ is an R-submodule of the finitely generated R-module $r^{-1}R$. By Corollary 4.1.12, $R[u]$ is finitely generated. By Proposition 6.1.2, u is integral over R. The converse follows from Part (1). $\square$

EXAMPLE 11.1.3. If R is a noetherian normal integral domain, then Lemma 11.1.2 (3) implies that R is completely normal. In particular, if R is a UFD, then R is normal by Example 6.1.6. If R is a noetherian UFD, then R is completely normal. If k is a field, then $k[x]$ and $k[[x]]$ are completely normal.

DEFINITION 11.1.4. Let R be a commutative ring. We say R is a *normal ring* in case R_P is a normal local integral domain for each $P \in \operatorname{Spec} R$. We say R is a *regular ring* in case R_P is a regular local ring (see Definition 9.6.14) for each $P \in \operatorname{Spec} R$.

LEMMA 11.1.5. *Let R be a commutative noetherian ring with the property that $R_{\mathfrak{m}}$ is an integral domain, for each maximal ideal $\mathfrak{m} \in \operatorname{Max} R$. Let $P_1, \dots, P_n$ be the distinct minimal primes of R.*

(1) *The natural map*
$$R \xrightarrow{\phi} R/P_1 \oplus \cdots \oplus R/P_n$$
is an isomorphism.
(2) *The nil radical of R, $\operatorname{Rad}(0)$, is equal to (0).*
(3) *R is a normal ring if and only if each ring R/P_i is a normal integral domain.*

PROOF. By Corollary 4.1.15, there are only finitely many minimal prime over-ideals of (0).

(1) and (2): For each maximal ideal $\mathfrak{m} \in \operatorname{Max} R$, the local ring $R_{\mathfrak{m}}$ is an integral domain. If $I = \operatorname{Rad}(0)$ is the nil radical of R, then $I_{\mathfrak{m}} = 0$ for each $\mathfrak{m}$. By Proposition 3.1.9, $I = 0$. By Exercise 9.2.9, $P_1 \cap \cdots \cap P_n = (0)$. Suppose $\mathfrak{m}$ is a maximal ideal such that $P_i + P_j \subseteq \mathfrak{m}$. The integral domain $R_{\mathfrak{m}}$ has a unique minimal prime ideal, namely (0). This means $P_i R_{\mathfrak{m}} = P_j R_{\mathfrak{m}} = (0)$. By Exercise 3.3.9, we conclude $i = j$. If $n > 1$, then the minimal prime ideals of R are pairwise comaximal. The rest follows from the Chinese Remainder Theorem, Theorem 1.1.7.

(3): Is left to the reader. $\square$

LEMMA 11.1.6. *Let R be a commutative ring.*

(1) *If R is a completely normal integral domain, then so is $R[x_1,\dots,x_n]$.*
(2) *If R is a completely normal integral domain, then so is $R[[x_1,\dots,x_n]]$.*
(3) *If R is a normal ring, then so is $R[x_1,\dots,x_n]$.*

PROOF. (1): It is enough to prove $R[x]$ is completely normal. Let K be the quotient field of R. We have the tower of subrings $R[x] \subseteq K[x] \subseteq K(x)$ and $K(x)$ is the quotient field of $R[x]$ as well as $K[x]$. By Example 11.1.3, $K[x]$ is completely normal. Let $u \in K(x)$ and assume u is almost integral over $R[x]$. Then u is almost integral over $K[x]$, hence $u \in K[x]$. Let $f \in R[x]$ and assume $fu^n \in R[x]$ for all n. Write $u = u_t x^t + u_{t+1}x^{t+1} + \cdots + u_T x^T$, where $u_i \in K$, $t \geq 0$, and $u_t \neq 0$. Write $f = f_s x^s + f_{s+1}x^{s+1} + \cdots + f_S x^S$, where $f_i \in R$, $s \geq 0$, and $f_s \neq 0$. Since R is an integral domain, in fu^n, the coefficient of the lowest degree monomial is equal to $f_s u_t^n$. Therefore, u_t is almost integral over R, hence $u_t \in R$. By Lemma 11.1.2 (2) we see that $u - u_t x^t = u_{t+1}x^{t+1} + \cdots + u_T x^T$ is almost integral over $R[x]$. By a finite iteration, we can prove that every coefficient of u is in R.

(2): Mimic the proof of Part (1). The proof is left to the reader.

(3): It is enough to prove $R[x]$ is normal. Let Q be a prime ideal in $R[x]$. We need to show $R[x]_Q$ is a normal integral domain. Let $P = Q \cap R$. Then $R[x]_Q$ is a localization of $R_P[x]$. By assumption, R_P is a normal integral domain. By Proposition 6.1.9, it is enough to prove the result when R is a local normal integral domain. Let K be the quotient field of R. Let $u \in K(x)$ and assume u is integral over $R[x]$. Then u is integral over $K[x]$ and $K[x]$ is integrally closed, so $u \in K[x]$. We can write $u = u_r x^r + \cdots + u_1 x + u_0$ where each $u_i \in K$. Each u_i can be represented as a fraction $u_i = t_i/b_i$, for some $t_i, b_i \in R$. There is a monic polynomial $f(y) \in R[x][y]$ such that $f(u) = 0$. Write $f(y) = y^m + f_{m-1}y^{m-1} + \cdots + f_1 y + f_0$, where each $f_i \in R[x]$. Let S be the subring of R generated by $1, b_0, \dots, b_r, t_0, \dots, t_r$, together with all of the coefficients of all of the polynomials $f_0, \dots, f_{m-1}$. Since S is a finitely generated $\mathbb{Z}$-algebra, S is noetherian, by the Hilbert Basis Theorem (Theorem 6.2.1). Also, S is an integral domain and $S[x] \subseteq R[x]$. If F is the quotient field of S, then $F \subseteq K$ and $u \in F[x]$. Therefore, u is integral over $S[x]$. By the proof of Part (1), each coefficient of u is almost integral over S. By Lemma 11.1.2 (3), each coefficient of u is integral over S. Therefore, each coefficient of u is integral over R. Since R is integrally closed, this proves $u \in R[x]$. $\square$

Let R be a commutative ring and I an ideal of R such that the I-adic topology of R is separated. In this case, $\bigcap_n I^n = (0)$. As in Example 7.2.3, let $\operatorname{gr}_I(R) = \bigoplus_{n\geq 0} I^n/I^{n+1}$ be the graded ring associated to the I-adic filtration $R = I^0 \supset I^1 \supseteq I^2 \supset \dots$. For notational simplicity, set $\operatorname{gr}_n(R) = I^n/I^{n+1}$. Then $\operatorname{gr}_I(R) = \operatorname{gr}_0(R) \oplus \operatorname{gr}_1(R) \oplus \operatorname{gr}_2(R) \oplus \cdots$. Given $x \in R - (0)$, there exists a unique nonnegative integer n such that $x \in I^n$ and $x \notin I^{n+1}$. This integer n is called the *order of x with respect to I*, and is written $\operatorname{ord}(x)$. Define $\operatorname{ord}(0) = \infty$. The reader should verify that $\operatorname{ord}(xy) \geq \operatorname{ord}(x) + \operatorname{ord}(y)$ and $\operatorname{ord}(x+y) \geq \min(\operatorname{ord}(x), \operatorname{ord}(y))$.

If $x \neq 0$ and $n = \operatorname{ord}(x)$, then the image of x in $\operatorname{gr}_n(R) = I^n/I^{n+1}$ is denoted $\lambda(x)$. We call $\lambda(x)$ the *least form* of x. Define $\lambda(0) = 0$.

THEOREM 11.1.7. *Let R be a commutative ring and I an ideal of R such that the I-adic topology of R is separated.*

(1) *If $\operatorname{gr}_I(R)$ is an integral domain, then R is an integral domain and for any $x, y \in R$, $\operatorname{ord}(xy) = \operatorname{ord}(x) + \operatorname{ord}(y)$ and $\lambda(xy) = \lambda(x)\lambda(y)$.*
(2) *If R is noetherian, I is contained in the Jacobson radical of R, and $\operatorname{gr}_I(R)$ is a normal integral domain, then R is a normal integral domain.*

PROOF. (1): Let x and y be nonzero elements of R. Write $m = \operatorname{ord}(x)$ and $n = \operatorname{ord}(y)$. Then $\lambda(x) \in \operatorname{gr}_m(R)$ is nonzero and $\lambda(y) \in \operatorname{gr}_n(R)$ is nonzero. Since $\lambda(x)\lambda(y)$ is a nonzero element of $\operatorname{gr}_{m+n}(R)$, we have $xy \in I^{m+n}$ and $xy \notin I^{m+n+1}$. This proves $xy \neq 0$. This also proves $\operatorname{ord}(xy) = \operatorname{ord}(x) + \operatorname{ord}(y)$ and $\lambda(xy) = \lambda(x)\lambda(y)$.

(2): By Part (1), R is an integral domain. Let a/b be an element of the quotient field of R which is integral over R. We must prove that $a \in bR$. By Corollary 7.3.6, the I-adic topology of R/bR is separated. In other words, $bR = \cap_n(bR + I^n)$, and it suffices to prove $a \in bR + I^n$ for all $n \geq 0$. The $n = 0$ case is trivially true, since $I^0 = R$. Inductively assume $n > 0$ and that $a \in bR + I^{n-1}$. Write $a = bx + c$, for some $c \in I^{n-1}$ and $x \in R$. It is enough to prove $c \in bR + I^n$. Assume $c \neq 0$, otherwise the proof is trivial. Since $c/b = a/b + x$ is integral over R, c/b is almost integral over R, by Lemma 11.1.2. There exists $d \in R - (0)$ such that $d(c/b)^m \in R$ for all $m > 0$. Therefore, $dc^m \in b^m R$ for all $m > 0$. By Part (1), λ is multiplicative, so $\lambda(d)\lambda(c)^m \in \lambda(b)^m \operatorname{gr}_I(R)$, for all m. This implies $\lambda(c)/\lambda(b)$ is almost integral over $\operatorname{gr}_I(R)$. By Proposition 7.2.9, $\operatorname{gr}_I(R)$ is noetherian. By Lemma 11.1.2, $\lambda(c)/\lambda(b)$ is integral over $\operatorname{gr}_I(R)$. By hypothesis, $\operatorname{gr}_I(R)$ is integrally closed, hence $\lambda(c) \in \lambda(b)\operatorname{gr}_I(R)$. Since $\lambda(c)$ is homogeneous, there exists a homogeneous element $\lambda(e) \in \operatorname{gr}_I(R)$ such that $\lambda(c) = \lambda(b)\lambda(e)$. By Part (1), $\lambda(c) = \lambda(be)$. By definition of λ, this implies $\operatorname{ord}(c) < \operatorname{ord}(c - be)$. By choice of c we have $n - 1 < \operatorname{ord}(c) < \operatorname{ord}(c - be)$. Thus, $c - be \in I^n$, which proves $c \in bR + I^n$. □

1.2. Regular Local Rings. A generalization of Theorem 11.1.8 for the ideal generated by a regular sequence in a commutative noetherian ring is proved in Corollary 11.3.7.

THEOREM 11.1.8. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$, and residue field $k = R/\mathfrak{m}$. Then R is a regular local ring of Krull dimension n if and only if the graded ring $\operatorname{gr}_{\mathfrak{m}}(R)$ associated to the $\mathfrak{m}$-adic filtration is isomorphic as a graded k-algebra to a polynomial ring $k[t_1, \dots, t_n]$.*

PROOF. Assume that R is regular. By Definition 9.6.14, $\mathfrak{m}$ is generated by a regular system of parameters, say $\mathfrak{m} = x_1R + \cdots + x_nR$. By Example 7.2.3, $\operatorname{gr}_{\mathfrak{m}}(R) = R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \cdots$ is a $k = R/\mathfrak{m}$-algebra which is generated by $\lambda(x_1), \dots, \lambda(x_n)$. As in the proof of Proposition 9.6.7, let $S = k[t_1, \dots, t_n]$ and define $\theta : S \to \operatorname{gr}_{\mathfrak{m}}(R)$ by $\theta(t_i) = \lambda(x_i)$. Then θ is a graded homomorphism of graded k-algebras and θ is onto. Let I denote the kernel of θ. Then I is a graded ideal, hence is generated by homogeneous polynomials. If $I = (0)$, then we are done. For contradiction's sake, assume f is a homogeneous polynomial of degree N in I. The sequence of graded S-modules

$$0 \to S(-N) \xrightarrow{\ell_f} S \to S/fS \to 0$$

is exact, where $S(-N)$ is the twisted module. If $m > N$, the components of degree m give the sequence

$$0 \to S_{m-N} \xrightarrow{\ell_f} S_m \to (S/fS)_m \to 0$$

which is still exact. By Example 9.5.10,

$$\sum_{d=0}^{m} \ell(S_d) = \binom{n}{n} + \cdots + \binom{m-1+n}{n} = \binom{m+n}{n},$$

and

$$\sum_{d=0}^{m-N} \ell(S_d) = \binom{n}{n} + \cdots + \binom{m-N-1+n}{n} = \binom{m-N+n}{n}.$$

Since

$$(S/fS)_0 \oplus (S/fS)_1 \oplus \cdots \oplus (S/fS)_m \xrightarrow{\theta} R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \cdots \oplus \mathfrak{m}^m/\mathfrak{m}^{m+1}$$

is onto, applying the length function, we have

$$\binom{m+n}{n} - \binom{m-N+n}{n} \geq \ell\left(R/\mathfrak{m}^{m+1}\right).$$

The left hand side is a numerical polynomial in m of degree $n-1$, by Lemma 9.5.8. At the same time, Theorem 9.6.11 says the function $\ell(A/\mathfrak{m}^{m+1})$ is a polynomial in m of degree n. This contradiction implies $I = (0)$.

Conversely, assume $\operatorname{gr}_{\mathfrak{m}}(R)$ is isomorphic to a polynomial ring $k[t_1, \dots, t_n]$. The Hilbert function of R is therefore $\ell(R/\mathfrak{m}^{m+1}) = \binom{m+n}{n}$, a polynomial in m of degree n. Corollary 9.6.13 says R has Krull dimension n. Also, $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k(kt_1 + \cdots + kt_n) = n$. By Exercise 9.6.2, R is regular. □

COROLLARY 11.1.9. *If R is a commutative noetherian regular local ring, then R is a normal integral domain.*

PROOF. This follows from Theorem 11.1.7 and Theorem 11.1.8. □

COROLLARY 11.1.10. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. Let $\hat{R} = \varprojlim R/\mathfrak{m}^n$ be the completion of R with respect to the $\mathfrak{m}$-adic topology.*

(1) $\hat{R}$ is a noetherian local ring with maximal ideal $\hat{\mathfrak{m}} = \mathfrak{m}\hat{R}$.
(2) The Krull dimension of R is equal to the Krull dimension of $\hat{R}$.
(3) $R \to \hat{R}$ is faithfully flat.
(4) R is a regular local ring if and only if $\hat{R}$ is a regular local ring.

PROOF. (1): Follows from Corollary 7.1.12 and Corollary 7.3.12.
(2): This is Corollary 9.6.13 (4).
(3): Follows from Theorem 7.3.7.
(4): By Corollary 7.3.2, the associated graded rings $\operatorname{gr}_{\mathfrak{m}}(R)$ and $\operatorname{gr}_{\hat{\mathfrak{m}}}(\hat{R})$ are isomorphic as graded rings. Part (4) follows from Theorem 11.1.8. □

1.3. Exercises.

EXERCISE 11.1.1. Let k be an algebraically closed field of characteristic different from 2 and 3 and let x and y be indeterminates. Let $f = y^2 - x^2 + x^3$ and $R = k[x,y]/(f)$. Define $\alpha : k[x] \to R$ by $x \mapsto x$.

(1) Show that α is one-to-one.
(2) Show that R is a finitely generated $k[x]$-module.
(3) Show that R is not a separable $k[x]$-module.
(4) Show that R is an integral domain.
(5) Show that R is not a normal integral domain.

2. Valuations and Valuation Rings

As an introduction to the subject of valuations and valuation rings we consider an example. Let R be a unique factorization domain with quotient field K. Let p be an irreducible element of R and $P = Rp$ the prime ideal generated by p. By Corollary 9.6.12, P has height one. If R_P is the local ring of R at P, then every $\alpha \in R_P$ can be represented as a fraction $\alpha = x/y$, where $x \in R$ and $y \in R - Rp$. Since R is a unique factorization domain and y is not divisible by p, α has a unique representation in the form $\alpha = up^a$, where $a \geq 0$

and u is an invertible element of R_P. This implies R_P is a unique factorization domain. By Theorem 1.5.8, R_P is a principal ideal domain. By Exercise 3.1.17, every invertible element z in K^* has a unique representation in the form $z = vp^n$, where v is a unit in R_P^* and n is an integer in $\mathbb{Z}$. Using this unique representation, we define a function $\nu_P : K^* \to \mathbb{Z}$, the so-called P-adic valuation on K^*. It is routine to verify the following.

(1) For all $x, y \in K^*$, $\nu_P(xy) = \nu_P(x) + \nu_P(y)$ and if $x + y \neq 0$, then $\nu_P(x+y) \geq \min(\nu_P(x), \nu_P(y))$.
(2) $R_P = \{0\} \cup \{z \in K^* \mid \nu_P(z) \geq 0\}$.
(3) For all $z \in K^*$, either $z \in R_P$, or $z^{-1} \in R_P$.

The definitions and results that follow are motivated by this example. General references for the material in this section are [**4**] and [**12**].

2.1. Valuation Rings. In this section we employ the notation R^* to designate the group of invertible elements of a ring.

LEMMA 11.2.1. *Let R be an integral domain with quotient field K. The following are equivalent.*

(1) For all $x \in K^*$, either $x \in R$, or $x^{-1} \in R$.
(2) For all a, b in R, either $a \mid b$, or $b \mid a$.

PROOF. Is left to the reader. □

If R is an integral domain that satisfies the equivalent parts of Lemma 11.2.1, then we say R is a *valuation ring* of K.

Let G be an abelian group, written additively. We say G is an *ordered group*, if there is a partial order on G that preserves the binary operation. In other words, if $u \leq v$ and $x \leq y$, then $u + x \leq v + y$. We say G is a *totally ordered group*, if the partial order is a chain.

EXAMPLE 11.2.2. The set $\mathbb{R}$ is partially ordered by the usual "less than" relation. Under addition, $\mathbb{R}$ is a totally ordered group. The subgroup $\mathbb{Z}$ is also a totally ordered group.

A *valuation* on a field F is a function $\nu : F^* \to G$, for a totally ordered group G which satisfies

(1) $\nu(xy) = \nu(x) + \nu(y)$, and
(2) if $x + y \neq 0$, then $\nu(x+y) \geq \min(\nu(x), \nu(y))$.

The reader should verify that $\nu(1) = 0$.

LEMMA 11.2.3. *Suppose F is a field and $\nu : F^* \to G$ is a valuation on F. Let*

$$R = \{0\} \cup \{x \in F^* \mid \nu(x) \geq 0\}.$$

Then R is a valuation ring of F which we call the valuation ring associated to ν. Conversely, if R is a valuation ring of F, then there exists a valuation $v : F^* \to H$ for some totally ordered group H such that R is the valuation ring of v.

PROOF. Is left to the reader (see Exercise 11.2.1). □

Let F be a field and $R \subseteq S$ subrings of F. Assume R and S are local rings and that the inclusion homomorphism $R \to S$ is a local homomorphism of local rings (or, equivalently, the maximal ideal of S contains the maximal ideal of R). In this case, we say S *dominates* R. The reader should verify that this defines a partial order on the set of all local subrings of F.

LEMMA 11.2.4. *Let F be a field and $\nu : F^* \to G$ a valuation on F. Let R be the valuation ring of ν.*

1. *R is a local ring with maximal ideal $\mathfrak{m}_R = \{0\} \cup \{x \in F^* \mid \nu(x) > 0\}$.*
2. *If $R \subseteq A \subseteq F$ is a tower of local subrings of F such that A dominates R, then $R = A$. In other words, R is a maximal local subring with respect to the relation "dominates".*
3. *R is integrally closed in F.*

PROOF. (1) and (2): Are left to the reader.

(3): Let $x \in F$ and assume x is integral over R. We prove $x \in R$. Assume the contrary. By Lemma 11.2.1, $x^{-1} \in R$. Since x is integral over R, there are elements $r_0, \dots, r_{n-1}$ in R such that

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0$$

where $n > 0$. Multiply by x^{1-n} and solve for x. Then

$$\begin{aligned} x &= -(x^{-1})^{n-1}(r_{n-1}x^{n-1} + \cdots + r_1 x + r_0) \\ &= -(r_{n-1} + \cdots + r_1 x^{2-n} + r_0 x^{1-n}) \end{aligned}$$

is in R, a contradiction. □

Let F be a field and Ω an algebraically closed field. Consider the set

$$\mathscr{C}(\Omega) = \{(R, f) \mid R \text{ is a subring of } F \text{ and } f : R \to \Omega \text{ is a homomorphism of rings}\}.$$

If (R, F) and (S, g) are in $\mathscr{C}$, then we say (S, g) *extends* (R, f), in case $R \subseteq S$ and the diagram

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr] & & \Omega \\ & S \arrow[ur, "g"'] & \end{tikzcd}$$

commutes. The reader should verify that this defines a partial order on $\mathscr{C}(\Omega)$.

LEMMA 11.2.5. *Let F be a field, R a local subring of F which is maximal with respect to the relation "dominates". Let $\mathfrak{m}_R$ be the maximal ideal of R and $k_R = R/\mathfrak{m}$ the residue field. Let $\bar{k}$ be an algebraic closure of k_R and $\eta : R \to \bar{k}$ the natural map. Then (R, η) is a maximal element of $\mathscr{C}(\bar{k})$.*

PROOF. Assume $R \subseteq A \subseteq F$ is a tower of subrings of F and $h : A \to \bar{k}$ is a homomorphism that extends η. The diagram

$$\begin{tikzcd} R \arrow[rr, "\eta"] \arrow[dr] & & \bar{k} \\ & A \arrow[ur, "h"'] & \end{tikzcd}$$

commutes. If P denotes the kernel of h, then it is easy to see that $P \cap R = \mathfrak{m}_R$. Then $R \to A_P$ is a local homomorphism of local rings and A_P dominates R. By hypothesis, R is equal to A_P. We conclude that $R = A$. □

LEMMA 11.2.6. *Let F be a field, Ω an algebraically closed field, and (R, f) a maximal element of $\mathscr{C}(\Omega)$. Then R is a valuation ring of F.*

PROOF. Step 1: R is a local ring, with maximal ideal $\mathfrak{m} = \ker g$. Since the image of f is a subring of the field Ω, we know that $\mathfrak{m} = \ker g$ is a prime ideal of R. Consider the tower of subrings of F, $R \subseteq R_P \subseteq F$. By Theorem 3.1.6, f extends uniquely to $g : R_P \to \Omega$. By maximality of (R, f), we conclude that $R = R_P$. Therefore, R is local and $\mathfrak{m}$ is the maximal ideal.

Step 2: For any nonzero $\alpha \in F$, either $\mathfrak{m}R[\alpha] \neq R[\alpha]$, or $\mathfrak{m}R[\alpha^{-1}] \neq R[\alpha^{-1}]$. Assume the contrary. Then $\mathfrak{m}[\alpha] = R[\alpha]$ and $\mathfrak{m}[\alpha^{-1}] = R[\alpha]$. There exist elements $a_0, \dots, a_m \in \mathfrak{m}$ such that

$$1 = a_0 + a_1\alpha + \cdots + a_m\alpha^m. \tag{2.1}$$

Among all such relations, pick one such that m is minimal. Likewise, there is a relation

$$1 = b_0 + b_1\alpha^{-1} + \cdots + b_n\alpha^{-n} \tag{2.2}$$

where $b_0, \dots, b_n \in \mathfrak{m}$ and n is minimal. Without loss of generality assume $m \geq n$. Multiply (2.2) by α^n and rearrange to get

$$(1 - b_0)\alpha^n = b_1\alpha^{n-1} + \cdots + b_n.$$

By Step 1, R is a local ring, so $1 - b_0$ is invertible in R. Solve for α^n and we can write

$$\alpha^n = c_1\alpha^{n-1} + \cdots + c_n$$

for some $c_1, \dots, c_n \in \mathfrak{m}$. Multiply by α^{m-n} to get $\alpha^m = c_1\alpha^{m-1} + \cdots + c_n\alpha^{m-n}$. Substituting this in (2.1), we get a relation with degree less than m, a contradiction.

Step 3: Let $\alpha \in F^*$ and prove that either $\alpha \in R$, or $\alpha^{-1} \in R$. Without loss of generality we assume by Step 2 that $\mathfrak{m}R[\alpha] \neq R[\alpha]$. Let M be a maximal ideal of $R[\alpha]$ such that $\mathfrak{m}R[\alpha] \subseteq M$. Now $M \cap R$ is a prime ideal of R which contains the maximal ideal $\mathfrak{m}$. Hence $M \cap R = \mathfrak{m}$ and we can view $R[\alpha]/M$ as an extension field of $R/\mathfrak{m}$. The field $R[\alpha]/M$ is generated as an algebra over $R/\mathfrak{m}$ by the image of α. Therefore, $R[\alpha]/M$ is a finitely generated algebraic extension of $R/\mathfrak{m}$. By Corollary 1.8.3, there exists a homomorphism $R[\alpha] \to \Omega$ which extends $f : R \to \Omega$. Since (R, f) is maximal, we conclude that $R = R[\alpha]$. $\square$

THEOREM 11.2.7. *Let F be a field and R a subring of F.*

1. *Let Ω be an algebraically closed field and $f : R \to \Omega$ a homomorphism of rings. Then there exists a valuation ring A of F and a homomorphism $g : A \to \Omega$ such that (A, g) extends (R, f) and the kernel of g is equal to the maximal ideal of A.*
2. *If R is a local ring, then there exists a valuation ring A of F such that A dominates R.*
3. *The integral closure of R in F is equal to the intersection of the valuation rings of F that contain R.*
4. *If R is a local ring, then the integral closure of R in F is equal to the intersection of the valuation rings of F that dominate R.*

PROOF. (2): Take Ω to be an algebraic closure of the residue field of R and let $\eta : R \to \Omega$ be the natural map. Apply Part (1).

(1): Let $\mathfrak{C}$ be the subset of $\mathscr{C}(\Omega)$ consisting of those pairs (A, g) that extend (R, f). Then $\mathfrak{C}$ contains (R, f), hence is nonempty. Suppose $\{(A_i, f_i)\}$ is a chain in $\mathfrak{C}$. The reader should verify that the union $\cup f_i : \cup A_i \to \Omega$ is also in $\mathfrak{C}$. By Zorn's Lemma, Proposition 1.2.4, $\mathfrak{C}$ contains a maximal member, say (A, g). By Lemma 11.2.6, A is a valuation ring of F and the kernel of f is the maximal ideal of A.

(3): Let $\tilde{R}$ be the integral closure of R in F. Let A be a valuation ring of F which contains R. By Lemma 11.2.4 (3), A is integrally closed. Therefore $\tilde{R} \subseteq A$. Conversely, suppose $\alpha \in F - \tilde{R}$. The reader should verify that $\alpha \notin R[\alpha^{-1}]$, so α^{-1} is not invertible in $R[\alpha^{-1}]$. There exists a maximal ideal M of $R[\alpha^{-1}]$ such that $\alpha^{-1} \in M$. By Part (2), there exists a valuation ring A of F which dominates the local ring $R[\alpha^{-1}]_M$. Because α^{-1} is an element of the maximal ideal of A, A does not contain α.

(4): In the proof of Part (3), notice that the diagram

$$\begin{tikzcd} R \arrow[d] \arrow[dr, "\phi"] & \\ R[\alpha^{-1}] \arrow[r, "\eta"] & R[\alpha^{-1}]/M \end{tikzcd}$$

commutes. Since $\eta(\alpha^{-1}) = 0$, the image of ϕ is equal to the image of η. Therefore, ϕ is onto and the kernel of ϕ is a maximal ideal of R. If R is local with maximal ideal $\mathfrak{m}$, this proves $M \cap R = \mathfrak{m}$. The rest is left to the reader. $\square$

2.2. Exercise.

EXERCISE 11.2.1. This exercise outlines a proof to the last part of Lemma 11.2.3. Let F be a field and R a valuation ring of F. Define G to be the factor group F^*/R^*. There is a natural homomorphism of groups $\nu : F^* \to G$. The group G is an abelian group, written multiplicatively. If $x \in F^*$, the coset represented by x is denoted $\nu(x)$.

(1) Define a binary relation on G by the rule $\nu(x) \geq \nu(y)$ if and only if $xy^{-1} \in R$. Prove the following.
   (a) $\geq$ is a well defined binary relation on G.
   (b) $\geq$ is a partial order on G.
   (c) $\geq$ preserves the group law on G, hence G is an ordered group.
   (d) $\geq$ is a chain, hence G is a totally ordered group.
(2) $\nu : F^* \to G$ is a valuation on F.
(3) The valuation ring of ν is R.

2.3. Discrete Valuation Rings. If F is a field, a *discrete valuation* on F is a valuation $\nu : F^* \to \mathbb{Z}$ such that ν is onto. The valuation ring of ν is $R = \{0\} \cup \{x \in F^* \mid \nu(x) \geq 0\}$. Then R is a valuation ring of F. In particular, Lemma 11.2.4 implies that R is a local ring with maximal ideal $\mathfrak{m} = \{0\} \cup \{x \in F^* \mid \nu(x) > 0\}$, F is the field of fractions of R, and R is integrally closed in F. Since ν is onto, we see that $\mathfrak{m} \neq (0)$, so $\dim R \geq 1$. An integral domain A is called a *discrete valuation ring* (DVR for short), if there exists a discrete valuation on the field of fractions of A such that A is the associated valuation ring.

EXAMPLE 11.2.8. Let R be a unique factorization domain with quotient field K. Let p be an irreducible element of R and $P = Rp$ the principal prime ideal generated by p. As we saw in the opening paragraph of Section 11.2, the P-adic valuation is a discrete valuation on K and the local ring R_P is a discrete valuation ring.

LEMMA 11.2.9. *Let F be a field and ν a discrete valuation on F. Let R be the associated DVR, with maximal ideal* $\mathfrak{m}$.

(1) R is a PID.
(2) R is noetherian.
(3) For any element $\pi \in R$ such that $\nu(\pi) = 1$, $\mathfrak{m} = \pi R$. A complete list of the ideals of R is $(0), R\pi, R\pi^2, \ldots, R$.

(4) $\dim R = 1$.

PROOF. (1): Let I be a proper ideal in R. Then $I \subseteq \mathfrak{m}$. Consider the set $S = \{\nu(x) \mid x \in I - (0)\}$. This is a nonempty subset of $\mathbb{Z}$ which has a lower bound. By the Well Ordering Principle, there exists a least element, say $\nu(z)$. For any $x \in I$, we have $\nu(x/z) \geq 0$, so $x/z \in R$. Therefore, $x = z(x/z) \in Rz$. This proves that $I = Rz$ is principal.

(2): Follows from (1) and the fact that a principal ideal domain is noetherian (see Theorem 1.5.6).

(3): If $x, y \in R$, then x and y are associates if and only if $Rx = Ry$, if and only if $xy^{-1} \in R^*$, if and only if $\nu(x) = \nu(y)$. Since $\nu : F^* \to \mathbb{Z}$ is onto, there exists $\pi \in R$ such that $\nu(\pi) = 1$. Let I be a proper ideal of R. By Part (1), $I = Rz$ for some $z \in R$. Since I is proper, $\nu(z) = k > 0$. Then $\nu(z) = \nu(\pi^k)$, so $Rz = R\pi^k$. This proves every ideal of R is represented in the list. For $i \geq 0$, the ideals $R\pi^i$ are distinct, since π^i and π^j are associates if and only if $i = j$.

(4): See Example 9.6.1. $\square$

THEOREM 11.2.10. *Let R be a noetherian local integral domain with field of fractions K, maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. If $\dim(R) = 1$, the following are equivalent.*

(1) R is a DVR.
(2) R is a PID.
(3) R is regular.
(4) R is normal.
(5) $\mathfrak{m}$ is a principal ideal.
(6) There exists an element $\pi \in R$ such that every ideal of R is of the form $R\pi^n$, for some $n \geq 0$. We call π a local parameter *for R.*

PROOF. (1) implies (2): This is Lemma 11.2.9.

(2) implies (1): There exists $\pi \in R$ such that $\mathfrak{m} = R\pi$. The only prime ideals of R are $\mathfrak{m}$ and (0). By Exercise 3.1.17, any $x \in K^*$ can be factored uniquely as $x = u\pi^{\nu(x)}$ for some integer $\nu(x)$ and $u \in R^*$. The reader should verify that the function $\nu : K^* \to \mathbb{Z}$ is a discrete valuation on K, R is the valuation ring associated to ν, and the function ν does not depend on the choice of π.

(2) implies (3): There exists $\pi \in R$ such that $\mathfrak{m} = R\pi$. Then π is a regular system of parameters and R is regular, by Definition 9.6.14.

(3) implies (4): Corollary 11.1.9.

(4) implies (5): Let $x \in \mathfrak{m} - (0)$. Since $\dim(R) = 1$, the only prime ideal that contains Rx is $\mathfrak{m}$. Therefore, $\operatorname{Rad}(Rx) = \mathfrak{m}$. By Corollary 9.1.4, there exists $n > 0$ such that $\mathfrak{m}^n \subseteq Rx$. If $\mathfrak{m} = Rx$, then we are done. Otherwise pick n such that $\mathfrak{m}^{n-1} \not\subseteq Rx$. Let $y \in \mathfrak{m}^{n-1} - Rx$ and set $\pi = xy^{-1} \in K$. Then $y\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq Rx$ implies $\pi^{-1}\mathfrak{m} = yx^{-1}\mathfrak{m} \subseteq R$. Since $\pi^{-1}x = y \notin Rx$ it follows that $\pi^{-1} \notin R$. Since R is integrally closed in K, it follows that π^{-1} is not integral over R. If $\pi^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, then $\mathfrak{m}$ is a faithful $R[\pi^{-1}]$-module which is finitely generated as an R-module. Proposition 6.1.2 implies π^{-1} is integral over R, a contradiction. Therefore, $\pi^{-1}\mathfrak{m}$ is an ideal in R which is not contained in $\mathfrak{m}$. This means $\pi^{-1}\mathfrak{m} = R$, $\pi \in \mathfrak{m}$, and $\mathfrak{m} = R\pi$.

(5) implies (6): Let I be a proper ideal of R. Then $I \subseteq \mathfrak{m}$. Since $\dim(R) = 1$, R is not artinian. By Proposition 4.5.5, for all $n \geq 1$, $\mathfrak{m}^{n+1} \subsetneq \mathfrak{m}^n$. There exists $n \geq 1$ such that $I \subseteq \mathfrak{m}^n$ and $I \not\subseteq \mathfrak{m}^{n+1}$. Pick $y \in I$ such that $y \in \mathfrak{m}^n$ and $y \notin \mathfrak{m}^{n+1}$. There exists $\pi \in R$ such that $\mathfrak{m} = R\pi$. For some $u \in R$, we can write $y = u\pi^n$. Since $y \notin \mathfrak{m}^{n+1}$, we know that $u \in R - \mathfrak{m}$. That is, $u \in R^*$. It follows that $\pi^n = u^{-1}y \in I$, so $I = \mathfrak{m}^n$.

(6) implies (2): Is trivial. $\square$

2.3.1. *Completion of a Discrete Valuation Ring.*

THEOREM 11.2.11. *Let R be a DVR with field of fractions K and maximal ideal $\mathfrak{m} = \pi R$. Let $\hat{R} = \varprojlim R/\mathfrak{m}^n$ be the completion of R with respect to the $\mathfrak{m}$-adic topology.*

(1) *$\hat{R}$ is a DVR with maximal ideal $\hat{\mathfrak{m}} = \pi\hat{R}$.*
(2) *K is equal to the localization $R[\pi^{-1}]$.*
(3) *The quotient field of $\hat{R}$ is $\hat{K} = \hat{R} \otimes_R K$.*
(4) *$\hat{K}$ is equal to the localization $\hat{R}[\pi^{-1}]$.*
(5) *$\hat{R} \cap K = R$.*
(6) *Given $a \in \hat{R}$ and $p > 0$ there exists $b \in R$ such that $a - b \in \mathfrak{m}^p$.*
(7) *Given $a \in \hat{K}$ and $p > 0$ there exists $b \in K$ such that $a - b \in \hat{\mathfrak{m}}^p$.*

PROOF. (1) – (4): By Corollary 11.1.10, $\hat{R}$ is a DVR with maximal ideal $\hat{\mathfrak{m}} = \pi\hat{R}$ and $R \to \hat{R}$ is faithfully flat. It follows from Theorem 11.2.10 that K is generated as an R-algebra by π^{-1}. By the same argument, the field of fractions of $\hat{R}$ is generated by π^{-1}. Consider the exact sequence $R[x] \to K \to 0$ where $x \mapsto \pi^{-1}$. Tensor with $\hat{R}$ to get the exact sequence $\hat{R}[x] \to \hat{K} \to 0$. Therefore, $\hat{K}$ is generated as a $\hat{R}$-algebra by π^{-1}, so $\hat{K}$ is equal to the field of fractions of $\hat{R}$.

(5): Let $a \in \hat{R} \cap K$. Since $a \in \hat{R}$, $\nu(a) \geq 0$. Then a is in the valuation ring of K, which is equal to R.

(6): Since $\hat{R}$ is the completion of R with respect to the $\mathfrak{m}$-adic topology, the open set $a + \mathfrak{m}^p$ has a nontrivial intersection with R.

(7): Is left to the reader. □

3. Some Local Algebra

The central focus of this section are Cohen-Macaulay local rings. This class of rings is related to regular local rings. In Theorem 11.3.20 we show that a regular local ring is Cohen-Macaulay. The converse is not true, in fact a Cohen-Macaulay ring is not necessarily normal (see Corollary 11.4.9). The most intuitive way to see the connection between the definitions for Cohen-Macaulay local rings and regular local rings involves the notion of regular sequences. For this reason, the section begins with the definition of a regular sequence. Consider a noetherian local ring R with maximal ideal $\mathfrak{m}$. We show below that if a regular system of parameters exists for $\mathfrak{m}$, then it is also a regular sequence for R in $\mathfrak{m}$. If R is not a regular local ring, then of course a regular system of parameters does not exist. So the idea of a regular sequence is more general than a regular system of parameters. The length of a regular sequence for R in $\mathfrak{m}$ is bounded by the Krull dimension of R. The maximal length of all regular sequences for R in $\mathfrak{m}$ is called the depth of R. If the depth of R is equal to the Krull dimension of R, then R is called a Cohen-Macaulay local ring. General references for the material in this section are [**41**, Sections 15, 16, 17 and 18] and [**23**, § 17.3].

3.1. Regular Sequences. Let R be a commutative ring, M an R-module, and $a_1, \dots, a_n$ some elements of R. We denote by $(a_1, \dots, a_n) = Ra_1 + \cdots + Ra_n$ the ideal which they generate and in the same fashion $(a_1, \dots, a_n)M = Ra_1M + \cdots + Ra_nM$.

DEFINITION 11.3.1. Let $a_1, \dots, a_r$ be elements of R. We say $a_1, \dots, a_r$ is a *regular sequence for M* in case the following are satisfied.

(1) a_1 is not a zero divisor for M,
(2) for $k = 2, \dots, r$, a_k is not a zero divisor for $M/(a_1, \dots, a_{k-1})M$, and
(3) $M \neq (a_1, \dots, a_r)M$.

If this is true, and if I is an ideal of R such that $(a_1,\dots,a_r) \subseteq I$, then we say $a_1,\dots,a_r$ is a *regular sequence for M in I*. A regular sequence $a_1,\dots,a_r$ is *maximal* if there is no $b \in I$ such that $a_1,\dots,a_r,b$ is a regular sequence for M in I.

EXAMPLE 11.3.2. Let R be a regular local ring of dimension n and maximal ideal $\mathfrak{m}$. By Definition 9.6.14, $\mathfrak{m}$ is generated by a regular system of parameters, say $\mathfrak{m} = x_1R + \cdots + x_nR$. We will show in Theorem 11.3.20 (1) that $x_1,\dots,x_n$ is a regular sequence for R in $\mathfrak{m}$.

LEMMA 11.3.3. *Suppose $a_1,\dots,a_r$ is a regular sequence for M. If $\xi_1,\dots,\xi_r$ are elements of M and $\sum_{i=1}^r a_i\xi_i = 0$, then for all i, $\xi_i \in (a_1,\dots,a_r)M$.*

PROOF. If $r = 1$, then $a_1\xi_1 = 0$ implies $\xi_1 = 0$. Inductively assume $r > 1$ and that the result is true for a regular sequence of length $r-1$. We have $a_r\xi_r \in (a_1,\dots,a_{r-1})M$, which implies $\xi_r \in (a_1,\dots,a_{r-1})M$. Write $\xi_r = \sum_{i=1}^{r-1} a_i\zeta_i$, for some $\zeta_i \in M$. Hence $0 = \sum_{i=1}^{r-1} a_i\xi_i + a_r\sum_{i=1}^{r-1} a_i\zeta_i$. By the induction hypothesis, for each $1 \le i < r$, $\xi_i + a_r\zeta_i \in (a_1,\dots,a_{r-1})M$. Consequently each ξ_i is in $(a_1,\dots,a_r)M$. $\square$

Let $S = R[x_1,\dots,x_n]$ be the polynomial ring in n variables with coefficients in R. Give S the usual grading, where $S_0 = R$ and $\deg(x_i) = 1$, for each i. By $M[x_1,\dots,x_n]$ we denote the R-module $M \otimes_R R[x_1,\dots,x_n]$. An element f of $M[x_1,\dots,x_n]$ can be viewed as a polynomial $f(x_1,\dots,x_n)$ with coefficients in M. Give $T = M[x_1,\dots,x_n]$ the grading where $T_0 = M$ and $\deg(x_i) = 1$, for each i. If $(a_1,\dots,a_n) \in R^n$, then $f(a_1,\dots,a_n) \in (a_1,\dots,a_n)M$. Let $I = (a_1,\dots,a_n)$ and $\operatorname{gr}_I(M) = \bigoplus_{k=1}^{\infty} I^kM/I^{k+1}M$ the graded module associated to the I-adic filtration of M. Given a homogeneous polynomial $f \in T_k$, $f(a_1,\dots,a_n) \in I^kM$. There is an evaluation mapping

$$\phi_k : T_k \to I^kM/I^{k+1}M$$

which maps f to the coset of $f(a_1,\dots,a_n)$. The reader should verify that ϕ_k is onto. Sum over all k to get a graded homomorphism $\phi : T \to \operatorname{gr}_I(M)$. If $f \in IM[x_1,\dots,x_n]$ is homogeneous of degree k, then $f(a_1,\dots,a_n) \in I^{k+1}M$. So ϕ factors into

$$\phi : M/IM[x_1,\dots,x_n] \to \operatorname{gr}_I(M)$$

which is a surjective graded homomorphism. If ϕ is an isomorphism, then $a_1,\dots,a_n$ is called a *quasi-regular sequence for M*.

LEMMA 11.3.4. *Let R be a commutative ring, M an R-module, $a_1,\dots,a_n \in R$, $I = (a_1,\dots,a_n)$. The following are equivalent.*

(1) $a_1,\dots,a_n$ is a quasi-regular sequence for M.
(2) If $f \in M[x_1,\dots,x_n]$ is a homogeneous polynomial and $f(a_1,\dots,a_n) = 0$, then $f \in IM[x_1,\dots,x_n]$.

PROOF. (1) implies (2): Suppose f is homogeneous of degree k and $f(a_1,\dots,a_n) = 0$. Since ϕ is one-to-one, f is in $IM[x_1,\dots,x_n]$.

(2) implies (1): Suppose f is homogeneous of degree k and that $f(a_1,\dots,a_n) \in I^{k+1}M$. If $k = 0$, then this implies $f \in IM$ and we are done. Suppose $k \ge 1$. Since $I^{k+1}M = I^kIM$, there is a homogeneous polynomial $g \in IM[x_1,\dots,x_n]$ such that $f(a_1,\dots,a_n) = g(a_1,\dots,a_n)$. If $f = g$, then we can stop. Otherwise, $f - g$ is a homogeneous polynomial of degree k such that $(f-g)(a_1,\dots,a_n) = 0$. Then $f - g \in IM[x_1,\dots,x_n]$, hence $f \in IM[x_1,\dots,x_n]$. $\square$

DEFINITION 11.3.5. Let R be a commutative ring and M an R-module. If S is a submodule of M and I is an ideal of R, then the *module quotient* of S over I is defined to be $S : I = \{x \in M \mid Ix \subseteq S\}$. If M is R and S is an ideal of R, this definition agrees with the module quotient defined in Exercise 1.1.3. If A is a commutative ring containing R as a subring, then $R : A$ is called the conductor ideal from A to R (see Exercise 1.1.8).

THEOREM 11.3.6. *Let R be a commutative ring, M an R-module, $a_1,\dots,a_n \in R$, $I = (a_1,\dots,a_n)$.*

(1) Assume $a_1,\dots,a_n$ is a quasi-regular sequence for M and x is an element of R such that $IM : x = IM$. Then $I^kM : x = I^kM$ for all $k > 0$.

(2) If $a_1,\dots,a_n$ is a regular sequence for M, then $a_1,\dots,a_n$ is a quasi-regular sequence for M.

(3) Assume

(a) M, $M/(a_1)M$, $M/(a_1,a_2)M$, $\dots$, $M/(a_1,\dots,a_{n-1})M$ are separated for the I-adic topology, and

(b) $a_1,\dots,a_n$ is a quasi-regular sequence for M.

Then $a_1,\dots,a_n$ is a regular sequence for M.

PROOF. (1): Inductively assume $k > 1$ and that the result is true for $k-1$. Suppose $x\xi \in I^kM = II^{k-1}M \subseteq I^{k-1}M$. By the induction hypothesis, $\xi \in I^{k-1}M$. There exists a homogeneous polynomial $f(x_1,\dots,x_n)$ in $M[x_1,\dots,x_n]$ of degree $k-1$ such that $\xi = f(a_1,\dots,a_n)$. Thus $x\xi = xf(a_1,\dots,a_n)$ is in I^kM. By quasi-regularity, the polynomial xf is in $IM[x_1,\dots,x_n]$, which implies the coefficients of f are in $IM : x = IM$. So $\xi = f(a_1,\dots,a_n)$ is in I^kM.

(2): The proof is by induction on n. The basis step, $n = 1$, is left to the reader. Assume $n > 1$ and that the result is true for a regular sequence of length $n-1$. Let f in $M[x_1,\dots,x_n]$ be a homogeneous polynomial of degree k and assume $f(a_1,\dots,a_n) = 0$. By Lemma 11.3.4, it suffices to show f is in $IM[x_1,\dots,x_n]$. If $k = 0$ this is trivial. If $k = 1$, this is Lemma 11.3.3. Proceed by induction on k. Assume $k > 1$ and that for any such homogeneous polynomial of degree $k-1$, its coefficients are in IM. Write

$$f(x_1,\dots,x_n) = x_n g(x_1,\dots,x_n) + h(x_1,\dots,x_{n-1})$$

where g and h are homogeneous polynomials of degrees $k-1$ and k respectively. Then $f(a_1,\dots,a_n) = a_n g(a_1,\dots,a_n) + h(a_1,\dots,a_{n-1}) = 0$, which says $g(a_1,\dots,a_n)$ is in the set $(a_1,\dots,a_{n-1})^kM : a_n$. Because $a_1,\dots,a_n$ is a regular sequence, $(a_1,\dots,a_{n-1})M : a_n$ is equal to $(a_1,\dots,a_{n-1})M$. By our induction hypothesis, $a_1,\dots,a_{n-1}$ is quasi-regular. Part (1) implies that $g(a_1,\dots,a_n)$ is in $(a_1,\dots,a_{n-1})^kM \subseteq I^kM$. Now g is homogeneous of degree $k-1$ and by induction on k and the proof of Lemma 11.3.4, this implies $g(x_1,\dots,x_n)$ is in $IM[x_1,\dots,x_n]$. Because $g(a_1,\dots,a_n)$ is in $(a_1,\dots,a_{n-1})^kM$, there exists a homogeneous polynomial $p(x_1,\dots,x_{n-1})$ of degree k such that $g(a_1,\dots,a_n) = p(a_1,\dots,a_{n-1})$. Look at the polynomial

$$q(x_1,\dots,x_{n-1}) = h(x_1,\dots,x_{n-1}) + a_n p(x_1,\dots,x_{n-1})$$

which is either 0 or homogeneous of degree k in $n-1$ variables. Because $q(a_1,\dots,a_{n-1}) = f(a_1,\dots,a_n) = 0$, the induction hypothesis on n says $q(x_1,\dots,x_{n-1})$ is in $IM[x_1,\dots,x_{n-1}]$. This implies $q(a_1,\dots,a_{n-1})$ is in $I^{k+1}M$. Now $p(a_1,\dots,a_{n-1}) = g(a_1,\dots,a_n)$ is in I^kM, from which it follows that $a_n p(a_1,\dots,a_{n-1})$ is in $I^{k+1}M$. This shows $h(a_1,\dots,a_{n-1})$ is in $I^{k+1}M$. By induction on n and the proof of Lemma 11.3.4, this implies the coefficients of h are in IM. We conclude that the coefficients of f are in IM.

(3): We must show conditions (1), (2) and (3) of Definition 11.3.1 are satisfied. Since M is separated for the I-adic topology we have $\bigcap_{k>0} I^kM = (0)$. In particular, $M \neq IM$.

Step 1: Show that a_1 is not a zero divisor for M. Suppose $\xi \in M$ and $a_1\xi = 0$. Consider $f(x) = \xi x_1$, a homogeneous linear polynomial in $M[x_1,\dots,x_n]$. Since $f(a_1,\dots,a_n) = 0$, by quasi-regularity ξ is in IM. There exists a homogeneous linear polynomial $f_1 = \sum_{i=1}^n m_i x_i$ in $M[x_1,\dots,x_n]$ such that $f_1(a_1,\dots,a_n) = \xi$. In this case, $a_1 f_1(a_1,\dots,a_n)$ is equal to $f(a_1,\dots,a_n) = 0$, so the coefficients of the homogeneous quadratic $x_1 f_1(x_1,\dots,x_n)$ are in IM. That is, for each m_i there exists a homogeneous linear polynomial f_{i2} such that $m_i = f_{i2}(a_1,\dots,a_n)$. Consider the homogeneous quadratic polynomial

$$f_2 = \sum_{i=1}^n f_{i2} x_i.$$

Then $f_2(a_1,\dots,a_n) = \xi$ is in I^2M. Moreover, $a_1 f_2(a_1,\dots,a_n) = 0$, so the coefficients of f_2 are in IM. By an obvious iterative argument, we conclude that $\xi \in I^kM$ for all $k \geq 1$. Since M is separated in the I-adic topology, this proves $\xi = 0$.

Step 2: Show that $a_2,\dots,a_n$ is a quasi-regular sequence for M/a_1M. For this, apply Lemma 11.3.4 (2). Let f be a homogeneous polynomial of degree k in $M[x_2,\dots,x_n]$. Assume $f(a_2,\dots,a_n) \in a_1M$. For some $\xi \in M$, we can write $f(a_2,\dots,a_n) = a_1\xi$. Since $\bigcap I^iM = (0)$, there exists $i \geq 0$ such that $\xi \in I^iM - I^{i+1}M$. There is a homogeneous polynomial g in $M[x_1,\dots,x_n]$ with degree i such that $\xi = g(a_1,\dots,a_n)$. For contradiction's sake, suppose $i < k-1$. Then $I^kM \subseteq I^{i+2}M$. Notice that $x_1 g(x_1,\dots,x_n)$ is homogeneous of degree $i+1$ and under the evaluation map, $a_1 g(a_1,\dots,a_n)$ is in $I^{i+1}M/I^{i+2}M$. But $a_1 g(a_1,\dots,a_n) = f(a_2,\dots,a_n) \in I^kM$. Because $a_1,\dots,a_n$ is a quasi-regular sequence for M the coefficients of g are in IM. Then $\xi = g(a_1,\dots,a_n)$ is in $I^{i+1}M$, a contradiction. Consequently, we know $i = k-1$. Set

$$h(x_1,\dots,x_n) = f(x_2,\dots,x_n) - x_1 g(x_1,\dots,x_n),$$

a homogeneous polynomial of degree k. Since $h(a_1,\dots,a_n) = 0$, by quasi-regularity, the coefficients of h are in IM. $h(0,x_2,\dots,x_n) = f(x_2,\dots,x_n)$, each coefficient of f is in IM. Under the map $M[x_2,\dots,x_n] \to (M/a_1M)[x_2,\dots,x_n]$ the image of f is in the submodule $(a_2,\dots,a_n)(M/a_1M)[x_2,\dots,x_n]$. That completes Step 2.

Step 3: To complete Part (3), we must show that for all $k = 2,\dots,n$, a_k is not a zero divisor for $M/(a_1,\dots,a_{k-1})M$. We prove a stronger statement. For $n = 1$, Step 1 shows Part (3) is true. Therefore, assume $n \geq 2$ and that the statement of Part (3) is true for any sequence of length $n-1$. By Step 2, $a_2,\dots,a_n$ is a quasi-regular sequence for M/a_1M. By the induction hypothesis we conclude $a_2,\dots,a_n$ is a regular sequence for M/a_1M. From this it follows that a_k is not a zero divisor for $M/(a_1,\dots,a_{k-1})M$. □

COROLLARY 11.3.7. *Let R be a noetherian commutative ring, M a finitely generated R-module, and $a_1,\dots,a_n$ elements of the Jacobson radical of R. Then $a_1,\dots,a_n$ is a regular sequence for M if and only if $a_1,\dots,a_n$ is a quasi-regular sequence for M.*

PROOF. Is left to the reader. □

COROLLARY 11.3.8. *Let $R = \bigoplus_{n\geq 0} R_n$ be a commutative graded ring, $M = \bigoplus_{n\geq 0} M_n$ a graded R-module, and $a_1,\dots,a_n$ elements of R. Assume each a_i is homogeneous of positive degree. Then $a_1,\dots,a_n$ is a regular sequence for M if and only if $a_1,\dots,a_n$ is a quasi-regular sequence for M.*

PROOF. There exists a positive integer N such that $I^kM \subseteq \sum_{n\geq kN} M_n$. The rest is left to the reader. □

THEOREM 11.3.9. *Let R be a commutative noetherian ring and M a finitely generated R-module. Let I be an ideal of R such that $IM \neq M$ and n a positive integer. The following are equivalent.*

(1) *There exists a regular sequence $a_1, \dots, a_n$ for M in I.*
(2) *For all $i < n$ and for all finitely generated R-modules N such that $\operatorname{Supp}(N) \subseteq V(I)$, we have $\operatorname{Ext}^i_R(N,M) = (0)$.*
(3) *$\operatorname{Ext}^i_R(R/I,M) = (0)$ for all $i < n$.*
(4) *There exists a finitely generated R-module N such that $\operatorname{Supp}(N) = V(I)$ and $\operatorname{Ext}^i_R(N,M) = (0)$ for all $i < n$.*

PROOF. (2) implies (3): Is trivial. (3) implies (4): Is trivial.

(4) implies (1): Step 1: Show that there exists an element $a_1 \in R$ such that a_1 is not a zero divisor for M. There exists a finitely generated R-module N such that $\operatorname{Supp}(N) = V(I)$ and $\operatorname{Ext}^i_R(N,M) = (0)$ for all $i < n$. In particular, if $i = 0$, $\operatorname{Hom}_R(N,M) = (0)$. For contradiction's sake, assume every element of I is a zero divisor for M. Then I is a subset of the union of the associated primes of M. By Lemma 6.3.2, there exists $P \in \operatorname{Assoc}_R(M)$ such that $I \subseteq P$. By Lemma 9.2.1, M contains an element x such that

$$0 \to P \to R \xrightarrow{\rho_x} M$$

is exact, where $\rho_x(1) = x$. Localize at P. Let $\mathfrak{m}_P$ denote the maximal ideal PR_P and k_P the residue field $R_P/\mathfrak{m}_P$. Then $\rho_x : k_P \to M_P$ is one-to-one, where $1 \mapsto x$. Since $P \in V(I) = \operatorname{Supp}(N)$, $N_P \neq (0)$. By Corollary 2.2.2, $N_P \otimes_{R_P} k_P \neq (0)$. Since $N_P \otimes_{R_P} k_P$ is a nonzero finitely generated k_P-vector space, there exists a nonzero R_P-module homomorphism

$$N_P \to N_P \otimes_{R_P} k_P \to k_P \xrightarrow{\rho_x} M_P.$$

That is, $\operatorname{Hom}_R(N,M) \otimes_R R_P = \operatorname{Hom}_{R_P}(N_P, M_P) \neq (0)$, a contradiction.

Step 2: The induction step. By Step 1, let a_1 be an element of I which is not a zero divisor for M. If $n = 1$, then we are done. Otherwise, assume (4) implies (1) is true for $n-1$. Start with the short exact sequence of R-modules

$$0 \to M \xrightarrow{\ell_{a_1}} M \to M/a_1M \to 0. \tag{3.1}$$

By Proposition 8.3.9 (2) there is a long exact sequence

$$\cdots \to \operatorname{Ext}^i_R(N,M) \xrightarrow{\ell_{a_1}} \operatorname{Ext}^i_R(N,M) \to \operatorname{Ext}^i_R(N,M/a_1M) \xrightarrow{\delta^i} \operatorname{Ext}^{i+1}_R(N,M) \to \dots \tag{3.2}$$

from which it immediately follows $\operatorname{Ext}^i_R(N,M/a_1M) = (0)$ for $0 \le i < n-1$. By the induction hypothesis, there exists a regular sequence $a_2, \dots, a_n$ for M/a_1M in I.

(1) implies (2): Since a_1 is not a zero divisor for M, the sequence (3.1) is exact. Let N be a finitely generated R-module with $\operatorname{Supp}(N) \subseteq V(I)$. In degree zero, the long exact sequence (3.2) is

$$0 \to \operatorname{Ext}^0_R(N,M) \xrightarrow{\ell_{a_1}} \operatorname{Ext}^0_R(N,M).$$

For any $r > 0$, "left multiplication" by a_1^r is one-to-one on $\operatorname{Ext}^0_R(N,M)$. By Exercise 9.2.7, $\operatorname{Supp}(N) \subseteq V(I)$ implies there exists $r > 0$ such that $a_1^r \in \operatorname{annih}_R(N)$. That is, "left multiplication" by a_1^r is the zero map. Applying the functor $\operatorname{Ext}^0_R(\cdot,M)$ to $\ell_{a_1^r} : N \to N$, "left multiplication" by a_1^r is the zero map on $\operatorname{Ext}^0_R(N,M)$. Taken together, this implies $\operatorname{Ext}^0_R(N,M) = (0)$. Proceed by induction on n. Assume $n > 1$ and that (1) implies (2) is true for a regular sequence of length $n-1$. Then $a_2, \dots, a_n$ is a regular sequence for

M/a_1M in I and $\operatorname{Ext}^i_R(N, M/a_1M) = (0)$ for $i = 0, \dots, n-2$. The long exact sequence (3.2) reduces to the exact sequence

$$0 \to \operatorname{Ext}^i_R(N,M) \xrightarrow{\ell_{a_1}} \operatorname{Ext}^i_R(N,M)$$

for $i = 0, \dots, n-1$. The rest of the proof is left to the reader. □

DEFINITION 11.3.10. Let R be a noetherian commutative ring and M a finitely generated R-module. Let I be a proper ideal in R. The *I-depth* of M, denoted $\operatorname{depth}_I(M)$, is the least element of the set $\{i \mid \operatorname{Ext}^i_R(R/I, M) \neq (0)\}$. By Theorem 11.3.9, $\operatorname{depth}_I(M)$ is equal to the length of any maximal regular sequence for M in I. If R is a local ring with maximal ideal $\mathfrak{m}$, then we sometimes write $\operatorname{depth}(M)$ instead of $\operatorname{depth}_{\mathfrak{m}}(M)$.

On the subject of depth, the terminology and notation appearing in the literature is inconsistent. In [**23**] Grothendieck calls $\operatorname{depth}(M)$ the "profondeur de M" and writes $\operatorname{prof}(M)$. In [**6**] and [**8**] Auslander, Buchsbaum and Goldman call $\operatorname{depth}(M)$ the "codimension of M" and write $\operatorname{codim}(M)$. Our terminology and notation agree with that used by Matsumura (see [**41**, p. 102]).

LEMMA 11.3.11. *Let R be a noetherian commutative local ring with maximal ideal $\mathfrak{m}$. Let M and N be nonzero finitely generated R-modules. For all i less than* $\operatorname{depth}(M) - \dim(N)$, $\operatorname{Ext}^i_R(N,M) = (0)$.

PROOF. Set $n = \dim(N)$. By definition, $n = \dim(R/\operatorname{annih}_R(N))$. The proof is by induction on n. If $n = 0$, then $R/\operatorname{annih}_R(N))$ is a local artinian ring and $\operatorname{Supp}(N) = \{\mathfrak{m}\}$. By Part (1) implies (2) of Theorem 11.3.9, $\operatorname{Ext}^i_R(N,M) = (0)$ for all $i < \operatorname{depth}(M)$. Inductively assume $n > 0$ and that the lemma is true for any module L such that $0 \le \dim(L) < n$. By Theorem 9.2.10 there exists a filtration $0 = N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_t = N$ of N and a set of prime ideals $P_j \in \operatorname{Spec} R$ such that $N_j/N_{j-1} \cong R/P_j$ for $j = 1, \dots, t$. Moreover, for each j, $P_j \in \operatorname{Supp}(M)$, hence $\operatorname{annih}_R(M) \subseteq P_j$. Then $\dim(R/P_j) \le \dim(N)$. For each j we have a short exact sequence

$$0 \to N_{j-1} \to N_j \to R/P_j \to 0$$

and a long exact sequence

$$\cdots \to \operatorname{Ext}^i(N_{j-1}, M) \to \operatorname{Ext}^i(N_j, M) \to \operatorname{Ext}^i(R/P_j, M) \to \dots.$$

Therefore, it is enough to prove that $\operatorname{Ext}^i_R(R/P_j, M) = (0)$ for $1 \le j \le t$ and $i < \operatorname{depth}(M) - \dim(N)$. Assume $P \in \operatorname{Spec}(R)$ and $n = \dim(R/P)$. Then $P \neq \mathfrak{m}$ so there exists $a \in \mathfrak{m} - P$. Denote by S the quotient $R/(P + (a))$. In the integral domain R/P, a is not a zero divisor, so the sequence

$$0 \to R/P \xrightarrow{\ell_a} R/P \to S \to 0$$

is exact. By Corollary 9.6.13, $\dim(S) = n-1$. If $i < \operatorname{depth}(M) - n$, then $i+1 < \operatorname{depth}(M) - (n-1)$. By the induction hypothesis, $\operatorname{Ext}^{i+1}_R(S,M) = (0)$. From the long exact sequence of Ext groups, left multiplication by a is an isomorphism

$$0 \to \operatorname{Ext}^i(R/P,M) \xrightarrow{\ell_a} \operatorname{Ext}^i(R/P,M) \to 0$$

for all $i < \operatorname{depth}(M) - n$. Tensoring ℓ_a with $R/\mathfrak{m}$ it becomes the zero map. Therefore, by Corollary 2.2.2, $\operatorname{Ext}^i(R/P,M) = (0)$. □

COROLLARY 11.3.12. *Let R be a noetherian commutative local ring and M a nonzero finitely generated R-module.*

(1) $\operatorname{depth}(M) \le \dim(R/P)$ *for every associated prime ideal $P \in$* $\operatorname{Assoc}_R(M)$.
(2) $\operatorname{depth}(M) \le \dim(M)$.

PROOF. (1): If $P \in \operatorname{Assoc}_R(M)$, then $\operatorname{Hom}_R(R/P, M) \neq (0)$. By Lemma 11.3.11, $\operatorname{depth}(M) - \dim(R/P) \leq 0$.

(2): Is left to the reader. □

LEMMA 11.3.13. *Let R be a commutative noetherian local ring, $\mathfrak{m}$ the maximal ideal of R, M a nonzero finitely generated R-module, and $a_1, \ldots, a_r$ a regular sequence for M in $\mathfrak{m}$. Then* $\dim(M/(a_1, \ldots, a_r)M) = \dim(M) - r$.

PROOF. Let $t = \dim(M) = \dim(R/\operatorname{annih}_R(M))$. Then t is the supremum of the lengths of all prime chains $\operatorname{annih}_R(M) \subseteq Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_t \subsetneq R$. A minimal prime over-ideal Q_0 of $\operatorname{annih}_R(M)$ is in the support of M, hence by Theorem 9.2.7, Q_0 is an associated prime of M. Then every element of Q_0 is a zero divisor of M, hence $a_1 \notin Q_0$. By Exercise 11.3.6, $\operatorname{Supp}(M/a_1M) = \operatorname{Supp}(M) \cap \operatorname{Supp}(R/(a_1))$. Let $s = \dim(M/a_1M) = \dim(R/\operatorname{annih}_R(M/a_1M))$. Then s is the supremum of the lengths of all prime chains $\operatorname{annih}_R(M/a_1M) \subseteq P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_s \subsetneq R$. Since $a_1 \in P_0$, this proves $s < t$. Iterate this argument r times to see that $\dim(M/(a_1, \ldots, a_r)M) \leq \dim(M) - r$. For the reverse inequality, $\dim(M) \geq \dim(M/a_1M) \geq \dim(M) - 1$, by Lemma 9.6.10. Iterate r times to see that $\dim(M/(a_1, \ldots, a_r)M) \geq \dim(M) - r$. □

3.2. Exercises.

EXERCISE 11.3.1. Let R be a noetherian commutative ring, I a proper ideal of R, M an R module, and $a_1, \ldots, a_r$ a regular sequence for M in I.

(1) There exists $n \geq r$ and elements $a_{r+1}, \ldots, a_n$ such that $a_1, \ldots, a_n$ is a maximal regular sequence for M.
(2) $\operatorname{depth}_I(M/(a_1, \ldots, a_r)M) = \operatorname{depth}_I(M) - r$.

EXERCISE 11.3.2. Let R be a noetherian commutative local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. Then $\operatorname{depth}_{\mathfrak{m}}(M) = 0$ if and only if $\mathfrak{m}$ is an associated prime of M.

EXERCISE 11.3.3. Let R be a noetherian commutative ring and $P \in \operatorname{Spec}(R)$. Let M be a finitely generated R-module. Let $\mathfrak{m}_P = PR_P$ be the maximal ideal of R_P and let $M_P = M \otimes_R R_P$. The following are equivalent.

(1) $\operatorname{depth}_{\mathfrak{m}_P}(M_P) = 0$.
(2) $\mathfrak{m}_P \in \operatorname{Assoc}_{R_P}(M_P)$.
(3) $P \in \operatorname{Assoc}_R(M)$.

EXERCISE 11.3.4. Let R be a noetherian commutative ring and $P \in \operatorname{Spec}(R)$. Let M be a finitely generated R-module. Let $\mathfrak{m}_P = PR_P$ be the maximal ideal of R_P and let $M_P = M \otimes_R R_P$. Then $\operatorname{depth}_{\mathfrak{m}_P}(M_P) \geq \operatorname{depth}_P(M)$.

EXERCISE 11.3.5. Let R be a commutative local ring. Let M and N be nonzero finitely generated R-modules. Show that $M \otimes_R N$ is nonzero.

EXERCISE 11.3.6. Let R be a commutative ring. Let M and N be nonzero finitely generated R-modules. Show that $\operatorname{Supp}(M \otimes_R N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$.

3.3. Cohen-Macaulay Modules.

DEFINITION 11.3.14. Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. By Corollary 11.3.12, if M is nonzero, then $\operatorname{depth}_{\mathfrak{m}}(M) \leq \dim(M)$. We say that M is a *Cohen-Macaulay module* in case $M = (0)$, or $\operatorname{depth}_{\mathfrak{m}}(M) = \dim(M)$. If $\operatorname{depth}_{\mathfrak{m}}(R) = \dim(R)$, then we say R is a *Cohen-Macaulay local ring*.

THEOREM 11.3.15. *Let R be a noetherian commutative local ring with maximal ideal $\mathfrak{m}$, and M a finitely generated R-module. If $P \in \operatorname{Spec}(R)$, then we write $\mathfrak{m}_P$ for PR_P and M_P for $M \otimes_R R_P$.*

(1) *If M is a Cohen-Macaulay module and $P \in \operatorname{Assoc}_R(M)$, then $\operatorname{depth}(M)$ is equal to $\dim(R/P)$. The associated primes of M all have the same height, or in other words, M has no embedded prime ideals (see Definition 9.2.9).*
(2) *If $a_1, \dots, a_r$ is a regular sequence for M in $\mathfrak{m}$, then M is a Cohen-Macaulay module if and only if $M/(a_1, \dots, a_r)M$ is a Cohen-Macaulay module.*
(3) *If M is a Cohen-Macaulay module and $P \in \operatorname{Spec}(R)$, then M_P is a Cohen-Macaulay R_P-module. If $M_P \neq (0)$, then $\operatorname{depth}_{\mathfrak{m}_P}(M_P) = \operatorname{depth}_P(M)$.*

PROOF. (1): Since P is an associated prime of M, M is nonzero and $\operatorname{depth}(M) = \dim(M)$. By Corollary 11.3.12, $\operatorname{depth}(M) \le \dim(R/P)$. Since $\operatorname{Assoc}_R(M) \subseteq \operatorname{Supp}(M)$, $\operatorname{annih}_R(M) \subseteq P$. Then $\dim(M) = \dim(R/\operatorname{annih}_R(M)) \ge \dim(R/P)$.

(2): Since $(a_1, \dots, a_r) \subseteq \mathfrak{m}$, by Corollary 2.2.2, $M/(a_1, \dots, a_r)M$ is nonzero if and only if M is nonzero. Assume M is nonzero. Then $\dim(M/(a_1, \dots, a_r)M) = \dim(M) - r$, which follows from Lemma 11.3.13. Consequently, $\operatorname{depth}(M/(a_1, \dots, a_r)M) = \operatorname{depth}(M) - r$, by Exercise 11.3.1.

(3): Assume $M_P \neq (0)$, hence $\operatorname{annih}_R(M) \subseteq P$. By Exercise 11.3.4, $\operatorname{depth}_P(M) \le \operatorname{depth}_{\mathfrak{m}_P}(M_P)$. By Corollary 11.3.12, $\operatorname{depth}_{\mathfrak{m}_P}(M_P) \le \dim(M_P)$. To finish the proof, we show $\operatorname{depth}_P(M) = \dim(M_P)$. The proof is by induction on $n = \operatorname{depth}_P(M)$.

For the basis step, assume $\operatorname{depth}_P(M) = 0$. Then every element of P is a zero divisor of M. It follows from Proposition 9.2.2 and Lemma 6.3.2 that $P \subseteq Q$ for some $Q \in \operatorname{Assoc}_R(M)$. By Exercise 9.2.8 and Part (1), Q is a minimal prime over-ideal of $\operatorname{annih}_R(M)$. Because $\operatorname{annih}_R(M) \subseteq P \subseteq Q$, we conclude $P = Q$. Then $\mathfrak{m}_P$ is a minimal prime over-ideal for $\operatorname{annih}_{R_P}(M_P)$. By Lemma 9.6.4, $\dim(M_P) = 0$.

Inductively, assume $n = \operatorname{depth}_P(M) > 0$ and that the result holds for $n-1$. Let a be a nonzero divisor of M in P. The sequence

$$0 \to M \xrightarrow{\ell_a} M \to M/aM \to 0$$

is exact. Since R_P is a flat R-module, the sequence

$$0 \to M_P \xrightarrow{\ell_a} M_P \to (M/aM)_P \to 0$$

is also exact and a is a nonzero divisor of M_P in $\mathfrak{m}_P$. Also, $(M/aM)_P = M_P/(aM_P)$, so by Lemma 11.3.13, $\dim((M/aM)_P) = \dim(M_P) - 1$. By Exercise 11.3.1, $\operatorname{depth}_P(M/aM) = \operatorname{depth}_P(M) - 1$. By Part (2), M/aM is a Cohen-Macaulay R-module. By induction on n, $\dim((M/aM)_P) = \operatorname{depth}_P(M/aM)$ which completes the proof. □

THEOREM 11.3.16. *Let R be a noetherian commutative Cohen-Macaulay local ring. Let $\mathfrak{m}$ denote the maximal ideal of R.*

(1) *Let $a_1, \dots, a_r$ be a sequence of elements in $\mathfrak{m}$. The following are equivalent.*
    (a) *$a_1, \dots, a_r$ is a regular sequence for R in $\mathfrak{m}$.*
    (b) *$\operatorname{ht}(a_1, \dots, a_i) = i$ for all i such that $1 \le i \le r$.*
    (c) *$\operatorname{ht}(a_1, \dots, a_r) = r$.*
    (d) *If $n = \dim(R)$, then there exist $a_{r+1}, \dots, a_n$ in $\mathfrak{m}$ such that $a_1, \dots, a_n$ is a system of parameters for R.*
(2) *Let I be a proper ideal of R. Then $\operatorname{ht}(I) = \operatorname{depth}_I(R)$ and $\operatorname{ht}(I) + \dim(R/I) = \dim(R)$.*
(3) *If P and Q are in $\operatorname{Spec} R$ such that $P \supseteq Q$, then $\operatorname{ht}(P/Q) = \operatorname{ht}(P) - \operatorname{ht}(Q)$.*

PROOF. (1): The reader should verify that the proofs of the implications (a) implies (b) implies (c) implies (d) are all true without the Cohen-Macaulay hypothesis.

(a) implies (b): Since $a_1,\dots,a_r$ is a regular sequence, $\operatorname{ht}(a_1)=1$, by Corollary 9.6.12. Inductively, assume $i>1$ and that $\operatorname{ht}(a_1,\dots,a_{i-1})=i-1$. Let $I=(a_1,\dots,a_i)$ and $I_1=(a_1,\dots,a_{i-1})$. By Corollary 9.6.12, $\operatorname{ht}(I)\le i$. For contradiction's sake, assume there exists a prime ideal P containing I such that $\operatorname{ht}(P)=i-1$. Since $I_1\subseteq P$, it follows that P is a minimal prime over-ideal of I_1. Thus P is an associated prime of R/I_1, which implies a_i is a zero divisor of R/I_1, a contradiction.

(b) implies (c): is trivial.

(c) implies (d): Let $I=(a_1,\dots,a_r)$. We are given that $\operatorname{ht}(I)=r$. If $r=n=\dim(R)$, then $\operatorname{ht}(\mathfrak{m})=r$, which means $\mathfrak{m}$ is a minimal prime over-ideal of I. Therefore, I is $\mathfrak{m}$-primary and $a_1,\dots,a_r$ is a system of parameters for R. If $\dim(R)>r$, then by Exercise 9.6.4, there exists an element $a_{r+1}\in\mathfrak{m}$ such that $\operatorname{ht}(a_1,\dots,a_{r+1})=r+1$. Iterate this process to construct $a_1,\dots,a_n$ such that $\operatorname{ht}(a_1,\dots,a_n)=n=\dim(R)$.

(d) implies (a): Let R be a Cohen-Macaulay local ring and $x_1,\dots,x_n$ a system of parameters for R. We show that $x_1,\dots,x_n$ is a regular sequence for R. By Proposition 9.6.15, $\dim(R/(x_1))=n-1$. If P is an associated prime of (0), then $\dim(R/P)=n$, by Theorem 11.3.15 (1). This implies x_1 is not in P. By Proposition 9.2.2, x_1 is not a zero divisor of R. By Theorem 11.3.15 (2), $R/(x_1)$ is a Cohen-Macaulay local ring. Moreover, the images of $x_2,\dots,x_n$ make up a system of parameters for $R/(x_1)$. By induction on n, $x_2,\dots,x_n$ is a regular sequence for $R/(x_1)$ in $\mathfrak{m}$.

(2): Step 1: Show that $\operatorname{depth}_I(R)=\operatorname{ht}(I)$. Let $\operatorname{ht}(I)=h$. By Exercise 9.6.4, there exist elements $x_1,\dots,x_h$ in I such that $\operatorname{ht}(x_1,\dots,x_i)=i$ for $1\le i\le h$. By Part (1), $x_1,\dots,x_h$ is a regular sequence for R in I. This proves $\operatorname{ht}(I)\le\operatorname{depth}_I(R)$. On the other hand, if $a_1,\dots,a_r$ is a regular sequence for R in I, then by Part (1), $r=\operatorname{ht}(a_1,\dots,a_r)\le\operatorname{ht}(I)$, so $\operatorname{depth}_I(R)\le\operatorname{ht}(I)$.

Step 2: Show that $\operatorname{ht}(P)+\dim(R/P)=\dim(R)$ for all prime ideals P. Let $\operatorname{ht}(P)=r$. By Step 1, $\operatorname{depth}_P(R)=r$. Start with a maximal regular sequence $a_1,\dots,a_r$ for R in P and put $J=(a_1,\dots,a_r)$. By Theorem 11.3.15 (2), R/I is Cohen-Macaulay. Every element of P is a zero divisor for R/I, so P is an associated prime of R/I. By Theorem 11.3.15 (1), R/I has no embedded primes, so P is a minimal prime over-ideal of I. Therefore, $\dim(R/I)=\dim(R/P)$. By Lemma 11.3.13, $\dim(R/I)=\dim(R)-r$.

Step 3: $\operatorname{ht}(I)+\dim(R/I)=\dim(R)$. By definition, $\operatorname{ht}(I)=\inf\{\operatorname{ht}(P)\mid P\in V(I)\}$. By Step 2, this becomes

$$
\begin{aligned}
\operatorname{ht}(I)&=\inf\{\dim(R)-\dim(R/P)\mid P\in V(I)\}\\
&=\dim(R)-\sup\{\dim(R/P)\mid P\in V(I)\}.
\end{aligned}
$$

The reader should verify that $\dim(R/I)=\sup\{\dim(R/P)\mid P\in V(I)\}$, so we are done.

(3): By Theorem 11.3.15 (3), R_P is a Cohen-Macaulay ring. By Part (2), $\dim R_P=\operatorname{ht}(QR_P)+\dim(R_P/QR_P)$. By Lemma 9.6.2, and Exercise 3.3.9, $\operatorname{ht}(P)=\operatorname{ht}(Q)+\operatorname{ht}(P/Q)$. □

DEFINITION 11.3.17. A commutative ring R is said to be a *Cohen-Macaulay* ring if R is noetherian and R_P is a Cohen-Macaulay local ring, for every prime ideal P in R. By Theorem 11.3.15, a noetherian commutative ring R is Cohen-Macaulay if $R_{\mathfrak{m}}$ is Cohen-Macaulay for every maximal ideal $\mathfrak{m}$ of R.

THEOREM 11.3.18. *Let R be a noetherian commutative ring. The following are equivalent.*

(1) *R is a Cohen-Macaulay ring.*
(2) *For every $r \geq 0$, if $I = (a_1, \ldots, a_r)$ is an ideal generated by r elements in R such that $\operatorname{ht}(I) = r$, then R/I has no embedded primes.*
(3) *For every maximal ideal $\mathfrak{m}$ of R, and for every $r \geq 0$, if $J = (a_1, \ldots, a_r)$ is an ideal generated by r elements in $R_\mathfrak{m}$ such that $\operatorname{ht}(J) = r$, then $R_\mathfrak{m}/J$ has no embedded primes.*

PROOF. (2) implies (1): Let P be a prime ideal in R and assume $\operatorname{ht}(P) = r$. We must prove that R_P is Cohen-Macaulay. If $r = 0$, then R_P is a field and by Exercise 11.3.7, R_P is Cohen-Macaulay. Assume $r > 0$. By Exercise 9.6.4, there exist elements $a_1, \ldots, a_r$ in P such that $\operatorname{ht}(a_1, \ldots, a_i) = i$ for all $i = 1, \ldots, r$. By (2), the ideal (0) has no embedded primes. Since $\operatorname{ht}(a_1) = 1$, a_1 belongs to no associated prime of (0). So a_1 is not a zero divisor of R. For $1 \leq i < r$, $R/(a_1, \ldots, a_i)$ has no embedded primes. Since $\operatorname{ht}(a_1, \ldots, a_{i+1}) = i+1$, a_{i+1} belongs to no associated prime of $(a_1, \ldots, a_i)$. So a_{i+1} is not a zero divisor of $R/(a_1, \ldots, a_i)$. This shows $a_1, \ldots, a_r$ is a regular sequence for R in P. We have $r \leq \operatorname{depth}_P(R) \leq \operatorname{depth}_{PR_P}(R_P)$, by Exercise 11.3.4. By Corollary 11.3.12, $\operatorname{depth}_{PR_P}(R_P) \leq \dim R_P$, which is equal to $\operatorname{ht}(P) = r$, by Lemma 9.6.2. This proves R_P is Cohen-Macaulay.

(1) implies (3): Let $\mathfrak{m}$ be a maximal ideal of R. By definition, $R_\mathfrak{m}$ is a Cohen-Macaulay local ring. By Theorem 11.3.15, the zero ideal of $R_\mathfrak{m}$ has no embedded primes. Let $r > 0$ and $J = (a_1, \ldots, a_r)$ an ideal generated by r elements in $R_\mathfrak{m}$ such that $\operatorname{ht}(J) = r$. By Theorem 11.3.16, the sequence $a_1, \ldots, a_r$ is a regular sequence for $R_\mathfrak{m}$ in $\mathfrak{m}R_\mathfrak{m}$. By Theorem 11.3.15, $R_\mathfrak{m}/J$ is Cohen-Macaulay and has no embedded primes.

(3) implies (2): Let I be a nonunit ideal in R. Let P be an associated prime of R/I in $\operatorname{Spec} R$ and assume P is an embedded prime. Let $\mathfrak{m}$ be a maximal ideal of R containing P. By Lemma 9.2.5, $PR_\mathfrak{m}$ is an associated prime of $R_\mathfrak{m}/IR_\mathfrak{m}$ which is an embedded prime. $\square$

THEOREM 11.3.19. *If R is a Cohen-Macaulay ring, then so is $R[x]$ for an indeterminate x.*

PROOF. Let Q be a prime ideal in $S = R[x]$ and let $P = Q \cap R$. We must show that S_Q is a Cohen-Macaulay local ring. But R_P is a Cohen-Macaulay local ring, by Theorem 11.3.15. Since $(R - P) \subseteq (S - Q)$, S_Q is the localization of $S \otimes_R R_P = R_P[x]$ at the prime ideal $Q \otimes_R R_P$. From now on assume R is a Cohen-Macaulay local ring with maximal ideal P and residue field $k = R/P$. Moreover assume Q is a prime ideal of $S = R[x]$ and $Q \cap R = P$. Then $S/PS = k[x]$. The reader should verify that S is a flat R-module. Consequently, S_Q is a flat R-module. By Theorem 6.3.5, going down holds for $R \to S$.

Suppose $\dim(R) = r$ and $a_1, \ldots, a_r$ is a regular sequence for R in P. If $\ell_{a_1} : R \to R$ is left multiplication by a_1, then ℓ_{a_1} is one-to-one. Upon tensoring with the flat R-algebra S_Q, ℓ_{a_1} is still one-to-one. In the same way, upon tensoring $\ell_{a_i} : R/(a_1, \ldots, a_{i-1}) \to R/(a_1, \ldots, a_{i-1})$ with the flat R-algebra S_Q, ℓ_{a_i} is still one-to-one. Therefore, $a_1, \ldots, a_r$ is a regular sequence for S_Q in QS_Q. This proves $r \leq \operatorname{depth}(S_Q)$.

A prime ideal of $k[x]$ is principal and is either equal to the zero ideal, or is generated by a monic irreducible polynomial in $k[x]$. Since Q is a prime ideal of S containing PS, Q is equal to $PS + gS$, where g is either 0, or a monic polynomial in $S = R[x]$ which restricts to an irreducible polynomial in $k[x]$. There are two cases.

Case 1: $Q = PS$. Theorem 9.6.16 says $\dim(S_Q) = \dim(R) = r$. This implies S_Q is Cohen-Macaulay.

Case 2: $Q = PS + gS$. In this case, the fiber $S_Q \otimes_R k$ is equal to the localization of $k[x] = S \otimes_R k$ at the prime ideal Q/PS. The local ring $S_Q \otimes_R k$ is a PID, hence has Krull dimension one. By Theorem 9.6.16, $\dim(S_Q) = \dim(R) + 1 = r + 1$. But g is a monic polynomial in $R[x]$ so g is not a zero divisor for $R/(a_1,\dots,a_r)[x]$. Therefore, $\operatorname{depth}_Q(S) \geq r+1$. This implies S_Q is Cohen-Macaulay. □

3.4. Exercises.

EXERCISE 11.3.7. Let F be a field. If F is viewed as a local ring with maximal ideal (0), then F is a Cohen-Macaulay local ring.

EXERCISE 11.3.8. Let R be a local PID. Then R is a Cohen-Macaulay local ring.

EXERCISE 11.3.9. Let R be a Cohen-Macaulay local ring with maximal ideal $\mathfrak{m}$, and $x_1,\dots,x_r$ a set of elements of $\mathfrak{m}$. Then $x_1,\dots,x_r$ is a regular sequence for R in $\mathfrak{m}$ if and only if $\dim(R/(x_1,\dots,x_r) = \dim R - r$.

EXERCISE 11.3.10. Let k be a field. As in Exercises 9.1.6, 9.2.10, and 7.3.2, let $A = k[x,y]$ and $R = k[x^2,xy,y^2,x^3,x^2y,xy^2,y^3]$. Prove:

(1) R and A have the same quotient field, namely $k(x,y)$, and A is equal to the integral closure of R in $k(x,y)$.
(2) $\dim(R) = 2$.
(3) Let M be the maximal ideal in A generated by x and y. Let $\mathfrak{m} = M \cap R$. Then $\mathfrak{m}$ is generated by $x^2,xy,y^2,x^3,x^2y,xy^2,y^3$, and $\operatorname{ht}(\mathfrak{m}) = 2$.
(4) In R, $\operatorname{ht}(x^3) = 1$, and $\dim(R/(x^3)) = 1$.
(5) $\operatorname{depth}(R_{\mathfrak{m}}/(x^3) = 0$ and $R_{\mathfrak{m}}$ is not Cohen-Macaulay.

EXERCISE 11.3.11. Let k be a field and R the localization of $k[x,y]$ at the maximal ideal (x,y). Show that the rings R, $R/(xy)$, $R/(xy,x-y)$ are Cohen-Macaulay.

3.5. Cohomological Theory of Regular Local Rings.

THEOREM 11.3.20. *Let R be a regular local ring with maximal ideal $\mathfrak{m}$, residue field k, and regular system of parameters $x_1,\dots,x_r$. The following are true.*

(1) $x_1,\dots,x_r$ *is a regular sequence for R in $\mathfrak{m}$.*
(2) R is a Cohen-Macaulay local ring.
(3) For each i, $P_i = (x_1,\dots,x_r)$ is a prime ideal of R of height i, and R/P_i is a regular local ring of Krull dimension $r-i$.
(4) If P is a prime ideal of R such that R/P is a regular local ring of dimension $r-i$, then there exists a regular system of parameters $y_1,\dots,y_r$ for R such that $P = (y_1,\dots,y_i)$.
(5) $\dim(R) = r = \operatorname{coh.dim}(R)$.

PROOF. (1): By Theorem 11.1.8, $k[t_1,\dots,t_r] \cong \operatorname{gr}_{\mathfrak{m}}(R)$. The sequence $x_1,\dots,x_r$ is a quasi-regular sequence for R in $\mathfrak{m}$. By Corollary 11.3.7, $x_1,\dots,x_r$ is a regular sequence for R in $\mathfrak{m}$.

(2): By Part (1), $\operatorname{depth}(R) \geq r = \dim(R)$.

(3): By Proposition 9.6.15, $\dim(R/P_i) = r-i$. Since $\mathfrak{m}/P_i$ is generated by $x_{i+1},\dots,x_r$, R/P_i is a regular local ring. By Corollary 11.1.9, R/P_i is a normal integral domain. Thus P_i is a prime ideal.

(4): Let $\bar{\mathfrak{m}} = \mathfrak{m}/P$. By Exercise 9.6.2, $r = \dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ and $r-i = \dim(R/P) = \dim_k(\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2)$. But $\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 = \mathfrak{m}/(\mathfrak{m}^2+P)$. Consider the tower of ideals $\mathfrak{m}^2 \subseteq \mathfrak{m}^2+P \subseteq \mathfrak{m}$. Then $r-i = \dim_k(\mathfrak{m}/(\mathfrak{m}^2+P)) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) - \dim_k((\mathfrak{m}^2+P)/\mathfrak{m}^2)$, from which it follows that $\dim_k((\mathfrak{m}^2+P)/\mathfrak{m}^2) = i$. Choose i elements $y_1,\dots,y_i$ in P such that modulo $\mathfrak{m}^2$, $y_1,\dots,y_i$ are linearly independent over k. Choose $r-i$ elements $y_{i+1},\dots,y_r$ in $\mathfrak{m}$ such that modulo $\mathfrak{m}^2$, $y_1, \dots, y_r$ are linearly independent over k. Then $y_1, \dots, y_r$ is a regular system of parameters for R. By Part (3), $Q = (y_1, \dots, y_i)$ is a prime ideal of height i. By Theorem 11.3.16, $\operatorname{ht}(P) = \dim(R) - \dim(R/P) = i$. Since $Q \subseteq P$, this proves $Q = P$.

(5): Let $x_1, \dots, x_d$ be a regular system of parameters for R. By Proposition 8.4.10 applied recursively to $k = R/(x_1, \dots, x_d)$, $\operatorname{proj.dim}_R(k) = \operatorname{proj.dim}(R) + d = d$. By Theorem 8.4.15, $\operatorname{coh.dim}(R) = d$. $\square$

THEOREM 11.3.21. *Let R be a commutative regular ring. If x is an indeterminate, then $R[x]$ is a regular ring.*

PROOF. As in the proof of Theorem 11.3.19, we can reduce to the case where R is a regular local ring with maximal ideal P, $k = R/P$, Q is a prime ideal of $S = R[x]$ and $Q \cap R = P$. Moreover, $S/PS = k[x]$ and going down holds for $R \to S$. A prime ideal of $k[x]$ is principal and is either equal to the zero ideal, or is generated by a monic irreducible polynomial in $k[x]$. Since Q is a prime ideal of S containing PS, Q is equal to $PS + gS$, where g is either 0, or a monic polynomial in $S = R[x]$ which restricts to an irreducible polynomial in $k[x]$.

Suppose $\dim(R) = r$. Then P is generated by r elements. There are two cases. If $Q = PS$, then Q is generated by r elements. In this case, Theorem 9.6.16 says $\dim(S_Q) = \dim(R) = r$, hence S_Q is regular. For the second case, assume $Q = PS + gS$ and $g \neq 0$. Then Q is generated by $r+1$ elements. In this case, the fiber $S_Q \otimes_R k$ is equal to the localization of $k[x] = S \otimes_R k$ at the prime ideal Q/PS. The local ring $S_Q \otimes_R k$ is a PID, hence has Krull dimension one. By Theorem 9.6.16, $\dim(S_Q) = \dim(R) + 1 = r + 1$. Hence S_Q is regular in this case as well. $\square$

COROLLARY 11.3.22. *(Hilbert's Syzygy Theorem) Let k be a field and $x_1, \dots, x_n$ a set of indeterminates. Then $k[x_1, \dots, x_n]$ has cohomological dimension n.*

PROOF. By Theorem 10.3.1, $R = k[x_1, \dots, x_n]$ has dimension n. Let $\mathfrak{m}$ be a maximal ideal of R. By Theorem 11.3.21, $R_\mathfrak{m}$ is a regular local ring of dimension n. By Theorem 11.3.20, $\operatorname{coh.dim}(R_P) = n$. By Lemma 8.4.14 (2), $\operatorname{coh.dim}(R) = n$. $\square$

LEMMA 11.3.23. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. If every element of $\mathfrak{m} - \mathfrak{m}^2$ is a zero divisor of R, then $\mathfrak{m}$ an associated prime of R.*

PROOF. If $\mathfrak{m}^2 = \mathfrak{m}$, then by Nakayama's Lemma (Theorem 4.2.3), $\mathfrak{m} = 0$. In this case, R is a field and the result is trivially true. Assume $\mathfrak{m} - \mathfrak{m}^2$ is nonempty. Let $\{P_1, \dots, P_n\}$ be the set of associated primes of R. By Proposition 9.2.2,

$$\mathfrak{m} - \mathfrak{m}^2 \subseteq P_1 \cup \cdots \cup P_n.$$

Since $\mathfrak{m}$ is not a subset of $\mathfrak{m}^2$, it follows from Lemma 6.3.2 that $\mathfrak{m} \subseteq P_i$ for some i. Since $\mathfrak{m}$ is maximal, $\mathfrak{m}$ is equal to P_i. $\square$

LEMMA 11.3.24. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. Let a be an element of $\mathfrak{m} - \mathfrak{m}^2$. The natural map $\mathfrak{m}/a\mathfrak{m} \to \mathfrak{m}/aR$ splits.*

PROOF. Without loss of generality, assume $\mathfrak{m} \neq \mathfrak{m}^2$. In the $R/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$, the image of a is nonzero. Extend the image of a to a basis of $\mathfrak{m}/\mathfrak{m}^2$, and lift this basis to elements $a, b_1, \dots, b_n$ in $\mathfrak{m} - \mathfrak{m}^2$. Let $B = Rb_1 + \cdots + Rb_n$. Consider an element ax in the intersection $aR \cap B$, where $x \in R$. Then $ax = \sum r_i b_i$ for some $r_i \in R$. We have linear independence of $a, b_1, \dots, b_n$ modulo $\mathfrak{m}^2$, hence $ax \in \mathfrak{m}^2$. By choice of a, if $x \in R - \mathfrak{m}$, then $ax \notin \mathfrak{m}^2$. Therefore $x \in \mathfrak{m}$. This proves $aR \cap B \subseteq a\mathfrak{m}$, so the natural map $B \to \mathfrak{m}/a\mathfrak{m}$

factors through $B/(aR \cap B)$. Let α be the inverse of the natural isomorphism $B/(aR \cap B) \to (aR+B)/aR$. The reader should verify that the composition

$$\frac{\mathfrak{m}}{aR} \xrightarrow{=} \frac{aR+B}{aR} \xrightarrow{\alpha} \frac{B}{aR \cap B} \to \frac{\mathfrak{m}}{a\mathfrak{m}} \to \frac{\mathfrak{m}}{aR}$$

is the identity map. □

LEMMA 11.3.25. *Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module of finite projective dimension. If a is an element in $\mathfrak{m}$ which is both M-regular and R-regular, then*

(1) *M/aM is an R/aR-module of finite projective dimension, and*
(2) $\operatorname{proj.dim}_{R/aR}(M/aM) \le \operatorname{proj.dim}_R(M)$.

PROOF. Let $\operatorname{proj.dim}_R(M) = n$. If $n = 0$, then M is a projective R-module and M/aM is a projective R/aR-module. This implies $\operatorname{proj.dim}_{R/aR}(M/aM) = 0$. Inductively, suppose $n > 0$ and that the result holds for any finitely generated R-module of projective dimension less than n. By Exercise 8.3.3, there exists a projective resolution $P_\bullet \to M$ such that each P_i is finitely generated. Since R is a local ring, each P_j is free. Let K be the kernel of $\varepsilon : P_0 \to M$. Consider the exact sequence

$$0 \to K \to P_0 \to M \to 0.$$

The reader should verify that $\operatorname{proj.dim}_R(K) = \operatorname{proj.dim}_R(M) - 1$. Since R is noetherian, K is finitely generated. The diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] \arrow[d, "\alpha"] & P_0 \arrow[r] \arrow[d, "\beta"] & M \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & K \arrow[r] & P_0 \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

commutes, where the three vertical maps are "left multiplication" by a. Since a is R-regular and P_0 is free, β is one-to-one. Since a is M-regular, γ is one-to-one. The Snake Lemma (Theorem 2.5.2) implies α is one-to-one, and the sequence

$$0 \to K/aK \to P_0/aP_0 \to M/aM \to 0$$

is exact. Since P_0/aP_0 is a free R/aR-module, this proves

$$\operatorname{proj.dim}_{R/aR}(M/aM) \le \operatorname{proj.dim}_{R/aR}(K/aK) + 1.$$

Since α is one-to-one, a is K-regular. Applying the induction hypothesis to K, it follows that $\operatorname{proj.dim}_{R/aR}(K/aK) \le n$. In conclusion, $\operatorname{proj.dim}_{R/aR}(M/aM) \le n+1$. □

THEOREM 11.3.26. *(Hilbert-Serre) Let R be a commutative noetherian local ring. The following are equivalent*

(1) *R has finite cohomological dimension.*
(2) *R is regular.*

If either condition is satisfied, $\operatorname{coh.dim}(R) = \dim(R)$.

PROOF. Let $\mathfrak{m}$ denote the maximal ideal of R and $k = R/\mathfrak{m}$ the residue field.

(2) implies (1): This follows from Theorem 11.3.20. It also follows that the equation $\operatorname{coh.dim}(R) = \dim(R)$ is satisfied.

(1) implies (2): Let $n = \operatorname{coh.dim}(R)$.

Step 1: Prove that $\mathfrak{m} - \mathfrak{m}^2$ contains an R-regular element. For contradiction's sake, assume $\mathfrak{m} - \mathfrak{m}^2$ is nonempty and consists of zero divisors. By Lemma 11.3.23, $\mathfrak{m}$ is an associated prime of R. By Lemma 9.2.1, there exists $x \in R - (0)$ such that $x\mathfrak{m} = (0)$. In other words, $\mathfrak{m}$ is not faithful, hence not free. By Proposition 3.4.2, $\mathfrak{m}$ is not a projective R-module. By Definition 8.4.13, $\operatorname{coh.dim}(R) \geq \operatorname{proj.dim}_R(\mathfrak{m}) \geq 1$. By Theorem 8.4.15, $\operatorname{proj.dim}_R(k) = \operatorname{coh.dim}(R) \geq 1$. By Proposition 8.4.10, $\operatorname{Tor}^R_{n+1}(R/xR, k) = 0$. The exact sequence of R-modules

$$0 \to \mathfrak{m} \to R \xrightarrow{\ell_x} R \to R/xR \to 0$$

can be shortened to

$$0 \to k \to R \to R/xR \to 0.$$

Since $\operatorname{Tor}^R_i(R,k) = 0$ for $i \geq 1$, the associated long exact sequence of Lemma 8.3.2 (3) implies the boundary map $\partial : \operatorname{Tor}^R_{n+1}(R/xR, k) \to \operatorname{Tor}^R_n(k,k)$ is an isomorphism. This implies $\operatorname{Tor}^R_n(k,k) = 0$, which is a contradiction to Theorem 8.4.15.

Step 2: The proof is by induction on $d = \dim(R)$. If $d = 0$, then R is regular, by Definition 9.6.14. Assume $d > 0$ and that the result is true for a ring of dimension $d-1$. By Step 1 we can assume there exists an element $a \in \mathfrak{m} - \mathfrak{m}^2$ such that a is R-regular. Then a is also $\mathfrak{m}$-regular. Consider the local ring R/aR, which has maximal ideal $\mathfrak{m}/aR$. By Corollary 9.6.13 (3), $\dim(R/aR) = d-1$. By (1), $\operatorname{proj.dim}_R(\mathfrak{m}) \leq \operatorname{coh.dim}(R)$ is finite. By Lemma 11.3.25, $\mathfrak{m}/a\mathfrak{m}$ is an R/aR-module of finite projective dimension. By Lemma 11.3.24, $\mathfrak{m}/aR$ is an R/aR-module direct summand of $\mathfrak{m}/a\mathfrak{m}$. By Exercise 8.4.9, $\mathfrak{m}/aR$ is an R/aR-module of finite projective dimension. By the induction hypothesis, R/aR is a regular local ring. By Exercise 11.3.12, R is regular. $\square$

COROLLARY 11.3.27. *If R is a regular local ring and P a prime ideal of R, then R_P is a regular local ring.*

PROOF. Is left to the reader. $\square$

PROPOSITION 11.3.28. *If R is a regular local ring and M a nonzero finitely generated R-module, then the following are true.*

(1) $\operatorname{depth}(M) + \operatorname{proj.dim}(M) = \dim(R)$.
(2) M is a free R-module if and only if $\operatorname{depth}(M) = \dim(R)$.

PROOF. Let $n = \dim(R)$, $\mathfrak{m}$ the maximal ideal of R, and $k = R/\mathfrak{m}$ the residue field. Since R is regular, $\operatorname{coh.dim}(R) = n$ (Theorem 11.3.20 (5)). Therefore, $\operatorname{proj.dim}_R(M) \leq n$ (Definition 8.4.13) and $\operatorname{proj.dim}_R(k) = n$ (Theorem 8.4.15). The proof is by induction on $d = \operatorname{depth}(M)$. First assume $d = 0$. By Exercise 11.3.2, there is an R-submodule $N \subseteq M$ such that N is isomorphic to k. The short exact sequence $0 \to N \to M \to M/N \to 0$ yields

$$\cdots \to \operatorname{Tor}^R_{n+1}(M/N, k) \xrightarrow{\partial} \operatorname{Tor}^R_n(N,k) \to \operatorname{Tor}^R_n(M,k) \to \cdots$$

(Lemma 8.3.2). By Proposition 8.4.10 (2), $\operatorname{Tor}^R_{n+1}(M/N,k) = 0$ and by Theorem 8.4.15, $\operatorname{Tor}^R_n(N,k) \neq 0$. Since $\operatorname{Tor}^R_n(M,k) \neq 0$, Proposition 8.4.10 (2) implies $\operatorname{proj.dim}(M) \geq n$. We have shown that $\operatorname{proj.dim}(M) = n$.

Inductively, assume $d > 0$ and that the statement is true for any module of depth $d-1$. Let x be an M-regular element in $\mathfrak{m}$. Then $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1 = d - 1$ (Exercise 11.3.1) and $\operatorname{proj.dim}(M/xM) = \operatorname{proj.dim}(M) + 1$ (Proposition 8.4.10 (3)). By induction, we are done. $\square$

3.6. Exercises.

EXERCISE 11.3.12. Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and let a be an R-regular element in $\mathfrak{m}$. Prove that if R/aR is regular, then R is regular and $a \notin \mathfrak{m}^2$.

EXERCISE 11.3.13. Let S be a commutative faithfully flat R-algebra. Prove that if R and S are both noetherian, and S is regular, then R is regular.

EXERCISE 11.3.14. Let R be a commutative noetherian ring. Prove R is regular if and only if $R_{\mathfrak{m}}$ is a regular local ring for every $\mathfrak{m} \in \operatorname{Max} R$.

4. Noetherian Normal Integral Domains

This section has two main goals. The first is to define the class group of noetherian normal integral domain R in terms of the Weil divisors of R. The groundwork for this definition is done in Section 11.4.1 and the definition itself is in Section 11.4.3. The important theorem of Serre which states necessary and sufficient conditions for a commutative noetherian ring R to be normal is proved in Theorem 11.4.8. Lastly, in Theorem 11.4.17 we prove that in a certain sense, a divisor is "close to" a principal divisor. General references for this section are [**41**, §17], [**62**, Chapter VI], [**24**], [**28**, Chapter II], and [**21**].

4.1. A Noetherian Normal Integral Domain is a Krull Domain. Let R denote a noetherian integral domain and K the field of fractions. By $X_1(R)$ we denote the subset of $\operatorname{Spec}(R)$ consisting of primes of height one. The main results of this section are Theorem 11.4.3 and Corollary 11.4.4. If P is a prime ideal of R in $X_1(R)$, then R_P is a discrete valuation domain and the valuation associated to R_P on K^* is denoted ν_P. We show that there is a homomorphism of groups $K^* \to \bigoplus_{P \in X_1(R)} \mathbb{Z}P$ defined by $\alpha \mapsto \sum_{P \in X_1(R)} \nu_P(\alpha)P$ and the kernel is equal to R^*.

First we introduce some new notation. Given an ideal I of R, let

$$I^{-1} = \{x \in K \mid xI \subseteq R\}.$$

Then $R \subseteq I^{-1}$ and $I^{-1}$is an R-submodule of K. The reader should verify that $I \subseteq I^{-1}I \subseteq R$ and $I^{-1}I$ is an ideal of R.

LEMMA 11.4.1. *Let R be a noetherian integral domain, x a nonzero noninvertible element of R, and $P \in \operatorname{Assoc}_R(R/xR)$. Then $P^{-1} \neq R$.*

PROOF. By Lemma 9.2.1, there exists $y \in R - xR$ such that $P = (xR : y)$. Then $yP \subseteq xR$, or in other words, $yx^{-1}P \subseteq R$. This implies $yx^{-1} \in P^{-1}$ and $yx^{-1} \notin R$ because $y \notin xR$. $\square$

LEMMA 11.4.2. *Let R be a noetherian local integral domain with maximal ideal $\mathfrak{m}$. If $\mathfrak{m} \neq (0)$ and $\mathfrak{m}^{-1}\mathfrak{m} = R$, then $\mathfrak{m}$ is a principal ideal and R is a DVR.*

PROOF. By Exercise 4.1.6, R is not artinian. By Proposition 4.5.5, $\mathfrak{m} \neq \mathfrak{m}^2$. Pick $\pi \in \mathfrak{m} - \mathfrak{m}^2$. Then $\pi\mathfrak{m}^{-1} \subseteq R$. Hence $\pi\mathfrak{m}^{-1}$ is an ideal in R. If $\pi\mathfrak{m}^{-1} \subseteq \mathfrak{m}$, then $\pi R = \pi\mathfrak{m}^{-1}\mathfrak{m} \subseteq \mathfrak{m}^2$, which contradicts the choice of π. Since $\pi\mathfrak{m}^{-1}$ is an ideal of R which is not contained in $\mathfrak{m}$, we conclude that $\pi\mathfrak{m}^{-1} = R$. That is, $\pi R = \pi\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$, which proves that $\mathfrak{m}$ is principal. By Corollary 9.6.13, $\dim R = 1$. By Theorem 11.2.10, R is a DVR. $\square$

Let R be a noetherian normal integral domain with field of fractions K. Let $X_1(R)$ denote the subset of $\operatorname{Spec} R$ consisting of all prime ideals P such that $\operatorname{ht}(P) = 1$. If $P \in X_1(R)$, then R_P is a one-dimensional noetherian normal local integral domain. By Theorem 11.2.10, R_P is a DVR of K. Denote by $\mathfrak{m}_P$ the maximal ideal of R_P and by π_P a generator of $\mathfrak{m}_P$. Then π_P is unique up to associates in R_P. Let $\nu_P : K \to \mathbb{Z}$ be the valuation on K defined as in the proof of (2) implies (1) of Theorem 11.2.10.

THEOREM 11.4.3. *Let R be a noetherian normal integral domain with field of fractions K.*

(1) Let x be a nonzero, noninvertible element of R. If P is an associated prime of Rx, then the height of P is equal to one.
(2) Let P be a prime ideal of height one in R and I a P-primary ideal. Then there exists a unique $\nu > 0$ such that I is equal to $P^{(\nu)}$, the νth symbolic power of P.
(3) If $\dim(R) \le 2$, then R is Cohen-Macaulay.

PROOF. (1): Let $P \in \operatorname{Assoc}_R(R/xR)$. By Lemma 9.6.2, it suffices to prove $\dim(R_P) = 1$. By this observation and Lemma 9.2.5, we assume from now on that R is a local normal integral domain with maximal ideal P and that P is an associated prime of a nonzero principal ideal xR and x is noninvertible. By Lemma 11.4.1 we have $R \subsetneq P^{-1}$. For contradiction's sake, assume $\operatorname{ht}(P) > 1$. Lemma 11.4.2 says $P^{-1}P = P$. Given $\alpha \in P^{-1}$, we have $\alpha P \subseteq P$, and for all $n > 0$,

$$\alpha^n P = \alpha^{n-1}\alpha P \subseteq \alpha^{n-1} P \subseteq \cdots \subseteq \alpha P.$$

Therefore, $\alpha^n \in P^{-1}$ for all $n > 0$, and $R[\alpha] \subseteq P^{-1}$. Since $x \neq 0$, $P \neq (0)$, so there exists $x_1 \in P - (0)$. Then for all $y \in P^{-1}$, $x_1^{-1} y \in R$. So $y \in x_1^{-1}R$, which shows P^{-1} is a subset of the principal R-module $x_1^{-1}R$. Since R is noetherian, P^{-1} is finitely generated as an R-module. Since $R[\alpha] \subseteq P^{-1}$, it follows that $R[\alpha]$ is finitely generated as an R-module. By Proposition 6.1.2, α, and hence P^{-1}, is integral over R. Since R is integrally closed, it follows that $P^{-1} \subseteq R$, which is a contradiction.

(2): By Theorem 11.2.10, R_P is a DVR and every proper ideal is equal to $P^m R_P$, for some $m > 0$. By Exercise 9.1.3, there is a unique ν such that $I = P^\nu R_P \cap R$, which is equal to $P^{(\nu)}$, by Exercise 9.3.1.

(3): This follows from Part (1), and Theorem 11.3.18. □

In the terminology of [**21**], Corollary 11.4.4 says that R is a *Krull domain*.

COROLLARY 11.4.4. *Let R be a noetherian normal integral domain with field of fractions K. Let $\alpha \in K^*$.*

(1) $\nu_P(\alpha) = 0$ for all but finitely many $P \in X_1(R)$.
(2) $\alpha \in R$ if and only if $\nu_P(\alpha) \ge 0$ for all $P \in X_1(R)$.
(3) $\alpha \in R^*$ if and only if $\nu_P(\alpha) = 0$ for all $P \in X_1(R)$.
(4) $R = \bigcap_{P \in X_1(R)} R_P$.

PROOF. Step 1: Assume $\alpha \in R - (0)$. By Theorem 11.4.3, the reduced primary decomposition of $R\alpha$ is

$$\alpha R = P_1^{(n_1)} \cap \cdots \cap P_s^{(n_s)}$$

where $s \ge 0$, $P_1, \dots, P_s$ are height one primes of R, $n_i \ge 1$, and $s = 0$ if and only if α is invertible in R. The integers $s, n_1, \dots, n_s$ and the primes $P_1, \dots, P_s$ are unique. By Exercise 3.1.1,

$$\alpha R_P = \begin{cases} \mathfrak{m}_{P_i}^{n_i} & \text{if } P \in \{P_1, \dots, P_s\} \\ R_P & \text{if } P \notin \{P_1, \dots, P_s\}. \end{cases}$$

It follows that

$$\nu_P(\alpha) = \begin{cases} n_i & \text{if } P \in \{P_1, \dots, P_s\} \\ 0 & \text{if } P \notin \{P_1, \dots, P_s\}. \end{cases}$$

This proves that
$$\alpha R = \bigcap_{P \in X_1(R)} P^{(\nu_P(\alpha))}.$$

Step 2: Assume $\alpha = uv^{-1} \in K^*$, where $u, v \in R - (0)$. We can apply Step 1 to both u and v. That is, $uR = \bigcap_{P \in X_1(R)} P^{(\nu_P(u))}$ and $vR = \bigcap_{P \in X_1(R)} P^{(\nu_P(v))}$ where $\nu_P(u) \geq 0$ and $\nu_P(v) \geq 0$ for all $P \in X_1(R)$. For each $P \in X_1(R)$, $\nu_P(uv^{-1}) = \nu_P(u) - \nu_P(v)$ is zero for all but finitely many P. This proves Part (1). If $\nu_P(uv^{-1}) \geq 0$ for all P, then $uR \subseteq vR$, hence $uv^{-1}R \subseteq R$ which implies $uv^{-1} \in R$. This proves Part (2). Parts (3) and (4) are left to the reader. □

4.2. Serre's Criteria for Normality. We prove an important theorem of Serre (Theorem 11.4.8) which states necessary and sufficient conditions for a commutative noetherian ring R to be normal. Our proof is based on [**24**, Théorème (5.8.6)].

DEFINITION 11.4.5. Let R be a commutative noetherian ring and $i \in \mathbb{N}$. We say R *has property* (S_i), if for every prime ideal P in R $\operatorname{depth}(R_P) \geq \inf(i, \operatorname{ht}(P))$. We say R *has property* (R_i), if for every prime ideal P in R such that $\operatorname{ht}(P) \leq i$, R_P is a regular local ring.

EXAMPLE 11.4.6. Some important cases of properties (S_i) are listed here.

(1) Any commutative noetherian ring R has property (S_0).
(2) By Exercise 11.3.3, R has property (S_1) if and only if R has no embedded primes.
(3) The commutative noetherian ring R has properties (S_i) for all $i \geq 0$ if and only if for every $P \in \operatorname{Spec} R$, $\operatorname{depth}(R_P) = \dim(R_P) = \operatorname{ht}(P)$. This is true if and only if R is Cohen-Macaulay.

PROPOSITION 11.4.7. *Let R be a commutative noetherian ring. Then R has properties (S_1) and (R_0) if and only if* $\operatorname{Rad}_R(0) = (0)$. *The ring R is said to be* reduced.

PROOF. Assume R is reduced, that is, assume $\operatorname{Rad}_R(0) = (0)$. Let $P_1, \dots, P_n$ be the complete list of distinct minimal primes of the zero ideal. By Theorem 9.2.7, $\operatorname{Assoc}_R(R) \supseteq \{P_1, \dots, P_n\}$. By Exercise 9.2.9, the natural homomorphism of rings
$$R \xrightarrow{\phi} \bigoplus_{i=1}^{n} R/P_i$$
is one-to-one. By Corollary 9.2.3, we have $\operatorname{Assoc}_R\left(\bigoplus_{i=1}^n R/P_i\right) = \{P_1, \dots, P_n\}$. These results, together with Proposition 9.2.2 (4), prove $\operatorname{Assoc}_R(R) = \{P_1, \dots, P_n\}$. Therefore every associated prime of R is minimal. Given $P \in \operatorname{Spec}(R)$, if $\operatorname{ht}(P) \geq 1$, then $\operatorname{depth}(P) \geq 1$, by Exercise 11.3.3. Therefore, R has property (S_1). If $\operatorname{ht}(P) = 0$, then by Exercise 3.3.11, the nil radical of R_P is (0). Since R_P has dimension 0, by Lemma 4.5.2, R_P is artinian. Proposition 4.5.3 implies R_P is a field. This proves R has property (R_0).

Conversely, assume $\operatorname{Rad}_R(0) \neq (0)$ and R has property (S_1). We show R does not have property (R_0). By Proposition 9.2.2 (1), there exists a nonzero nilpotent element $x \in \operatorname{Rad}_R(0)$ and a prime ideal $P \in \operatorname{Spec}(R)$ such that $P = \operatorname{annih}_R(x)$. Then $P \in \operatorname{Assoc}_R(R)$ and by property (S_1), $\operatorname{ht}(P) = 0$. By Exercise 11.4.1, the image of x in R_P is a nonzero nilpotent. Therefore, R_P is not a field, so R does not have property (R_0). □

THEOREM 11.4.8. *(Serre's Criteria for Normality) Let R be a commutative noetherian ring. Then R is normal if and only if the following two properties are satisfied.*

(R_1) *For every prime ideal P in R such that* $\operatorname{ht}(P) \leq 1$, *$R_P$ is a regular local ring.*

(S_2) *For every prime ideal P in R,*

$$\operatorname{depth}(R_P) \geq \begin{cases} 1 & \textit{if } \operatorname{ht}(P) = 1 \\ 2 & \textit{if } \operatorname{ht}(P) \geq 2. \end{cases}$$

PROOF. Assume R is normal and $P \in \operatorname{Spec}(R)$. By definition, R_P is an integrally closed integral domain. If $\operatorname{ht}(P) = 1$, then Theorem 11.2.10 says R_P is a regular local ring. Suppose $\operatorname{ht}(P) \geq 2$. By Exercise 9.6.4, there exist elements a_1, a_2 in PR_P such that $\operatorname{ht}(a_1) = 1$ and $\operatorname{ht}(a_1, a_2) = 2$. Therefore, a_1 is not a zero divisor for R_P. By Theorem 11.4.3 (1), $R_P/(a_1)$ has no embedded primes, so a_2 is not a zero divisor for $R_P/(a_1)$. This proves a_1, a_2 is a regular sequence for R_P in PR_P, hence $\operatorname{depth}(R_P) \geq 2$.

The converse is a series of four steps. Assume R has properties (R_1) and (S_2).

Step 1: Show that the nil radical of R is trivial. If $P \in \operatorname{Spec} R$ and $\operatorname{ht}(P) \geq 1$, then by ($S_2$), $\operatorname{depth}(R_P) \geq 1$ and by Exercise 11.3.3, P is not an associated prime of R. That is, $\operatorname{Assoc}(R)$ contains no embedded primes. By Proposition 11.4.7 we know that $\operatorname{Rad}_R(0) = (0)$.

Step 2: Show that the localization of R with respect to the set of all nonzero divisors decomposes into a sum of fields. Let $P_1, \dots, P_n$ be the distinct minimal primes of R. Then R_{P_i} is a field, and by Exercise 3.1.6, R_{P_i} is the quotient field of R/P_i. Since $\operatorname{Assoc}(R) = \{P_1, \dots, P_n\}$, by Proposition 9.2.2, the set of nonzero divisors in R is equal to $W = R - \bigcup_{i=1}^n P_i$. Then W is a multiplicatively closed set and $\operatorname{Spec}(RW^{-1}) = \{P_1W^{-1}, \dots, P_nW^{-1}\}$. Since each prime ideal in RW^{-1} is maximal, RW^{-1} is artinian. By Exercise 3.3.11, $\operatorname{Rad}_{RW^{-1}}(0) = (0)$. By Proposition 4.5.3 and Theorem 4.3.3, RW^{-1} is semisimple. By Theorem 4.4.3 (2) RW^{-1} decomposes into a direct sum

$$RW^{-1} = \bigoplus_{i=1}^{n} \frac{RW^{-1}}{P_iW^{-1}} = \bigoplus_{i=1}^{n} (R/P_i)W^{-1}$$

where each ring $(R/P_i)W^{-1}$ is a field. Since $W \subseteq R - P_i$ for each i, there is a natural map $RW^{-1} \to \bigoplus_{i=1}^n R_{P_i}$. This gives a homomorphism

$$(R/P_i)W^{-1} = \frac{RW^{-1}}{P_iW^{-1}} \xrightarrow{\phi_i} R_{P_i}$$

for each i. For each i, the kernel of the natural map $R \to (R/P_i)W^{-1}$ is the prime ideal P_i. Hence $R/P_i \to (R/P_i)W^{-1}$ is one-to-one and factors through the quotient field R_{P_i},

$$R_{P_i} \xrightarrow{\psi_i} (R/P_i)W^{-1}$$

for each i. The maps ϕ_i and ψ_i are inverses of each other, so the natural map

$$RW^{-1} \cong \bigoplus_{i=1}^{n} R_{P_i}$$

is an isomorphism.

Step 3: Show that R is integrally closed in its total ring of quotients RW^{-1}. Suppose $rw^{-1} \in RW^{-1}$, $u \geq 1$, and $a_1, \dots, a_{u-1} \in R$ such that

$$(rw^{-1})^u + a_{u-1}(rw^{-1})^{u-1} + \cdots + a_1(rw^{-1}) + a_0 = 0 \tag{4.1}$$

in RW^{-1}. The objective is to show $r \in wR$, so assume w is not a unit in R. If Q is a prime ideal that contains w, then the image of w is a nonzero divisor of R_Q in $\mathfrak{m}_Q = QR_Q$. By Corollary 9.6.12, $\operatorname{ht}(Q) \geq 1$. If $\operatorname{ht}(Q) \geq 2$, then by ($S_2$), $\operatorname{depth}(R_Q) \geq 2$. By Exercise 11.3.1, $\operatorname{depth}(R_Q/wR_Q) \geq 1$ and by Exercise 11.3.3, Q is not an associated prime of R/wR. That is, $\operatorname{Assoc}(R/wR)$ consists only of minimal prime over-ideals of wR. Let $Q \in \operatorname{Assoc}(R/wR)$. By (R_1), R_Q is an integral domain which is integrally closed in its field of fractions. By (4.1), the image of rw^{-1} in the quotient field of R_Q is integral over R_Q. In other words, $rw^{-1} \in R_Q$, or $r \in wR_Q \cap R$. If I is a Q-primary ideal in R, then $IR_Q = \mathfrak{m}_Q^\nu$, for some $\nu > 0$. By Exercise 9.1.3, $I = Q^\nu R_Q \cap R = Q^{(\nu)}$, the ν-th symbolic power of Q. The reduced primary decomposition of wR can be written in the form $wR = Q_1^{(\nu_1)} \cap \cdots \cap Q_s^{(\nu_s)}$. In this case, $wR_{Q_i} = Q_i^{\nu_i} R_{Q_i}$ and we already showed that r is in $wR_{Q_i} \cap R = Q_i^{(\nu_i)}$. This proves $r \in wR$.

Step 4: Show that R is normal. Let $e_1, \dots, e_n$ be the orthogonal idempotents in RW^{-1} corresponding to the direct sum decomposition of Step 2. Each e_i satisfies the monic polynomial $x^2 - x$ over R, hence belongs to R, by Step 3. This proves the natural map

$$R \to R/P_1 \oplus \cdots \oplus R/P_n$$

is onto, hence it is an isomorphism. The ideals $P_1, \dots, P_n$ are pairwise co-maximal. Every prime ideal Q of R contains exactly one of the ideals $P_1, \dots, P_n$. Each of the integral domains R/P_i satisfies the two properties (R_1) and (S_2). By Step 3, R/P_i is integrally closed in its quotient field R_{P_i}. By Lemma 11.1.5, R is a normal ring. □

COROLLARY 11.4.9. *If R is a Cohen-Macaulay ring, then R is normal if and only if R_P is regular for all P such that* $\operatorname{ht}(P) \le 1$.

PROOF. For every prime ideal P in R, $\operatorname{depth}(R_P) = \dim(R_P) = \operatorname{ht}(P)$, so condition (S_2) of Theorem 11.4.8 is satisfied. Therefore, R is normal if and only condition (R_1) is satisfied. □

4.2.1. *Local Complete Intersection Criteria.*

PROPOSITION 11.4.10. *Let R be a commutative noetherian ring. Let $a_1, \dots, a_r$ be a sequence of elements of R such that $I = (a_1, \dots, a_r)$ is not the unit ideal in R. Assume for every maximal ideal M of R such that $I \subseteq M$ that R_M is a Cohen-Macaulay local ring and* $\operatorname{ht}(IR_M) = r$. *Then*

(1) R/I is Cohen-Macaulay, and
(2) R/I is normal if and only if $(R/I)_P$ is regular for all $P \in \operatorname{Spec}(R/I)$ such that $\operatorname{ht}(P) \le 1$.

PROOF. (1): Since R_M is Cohen-Macaulay and $\operatorname{ht}(a_1 R_M + \cdots + a_r R_M) = r$, by Theorem 11.3.16, $a_1, \dots, a_r$ is a regular sequence for R_M in MR_M. By Theorem 11.3.15, $R_M/IR_M = (R/I)_{M/I}$ is Cohen-Macaulay. By Definition 11.3.17, R/I is Cohen-Macaulay.

(2): Follows by Corollary 11.4.9 and Part (1). □

4.3. Divisor Classes of Integral Domains. The class group of a noetherian normal integral domain R with quotient field K is defined as the group of Weil divisors modulo the subgroup of principal Weil divisors. In Section 12.4 below, we show that the class group of R is isomorphic to the group of reflexive fractional ideals of R in K modulo the subgroup of principal fractional ideals. The first main result, Theorem 11.4.12 and its corollary, shows that R is a unique factorization domain if and only if the class group of R is trivial. We then prove Nagata's Theorem which is an important tool for computing class groups. This method is illustrated in a nontrivial example, Example 11.4.15.

DEFINITION 11.4.11. Let R be a noetherian normal integral domain with field of fractions K. Let $X_1(R)$ be the subset of $\operatorname{Spec} R$ consisting of those prime ideals of height one. The free $\mathbb{Z}$-module on $X_1(R)$,

$$\operatorname{Div} R = \bigoplus_{P \in X_1(R)} \mathbb{Z}P$$

is called the *group of Weil divisors* of R. According to Corollary 11.4.4, there is a homomorphism of groups $\operatorname{Div} : K^* \to \operatorname{Div}(R)$ defined by

$$\operatorname{Div}(\alpha) = \sum_{P \in X_1(R)} \nu_P(\alpha) P,$$

and the kernel of $\operatorname{Div}()$ is equal to the group R^*. The *class group* of R is defined to be the cokernel of $\operatorname{Div}()$, and is denoted $\operatorname{Cl}(R)$. The sequence

$$0 \to R^* \to K^* \xrightarrow{\operatorname{Div}} \operatorname{Div}(R) \to \operatorname{Cl}(R) \to 0$$

is exact. The image of $\operatorname{Div} : K^* \to \operatorname{Div} R$ is denoted $\operatorname{Prin} R$ and is called the group of *principal Weil divisors*. In other words, $\operatorname{Cl}(R)$ is the group of Weil divisors modulo the principal Weil divisors.

THEOREM 11.4.12. *Let R be a noetherian integral domain. Then R is a UFD if and only if every prime ideal of height one is principal.*

PROOF. Suppose R has the property that every height one prime is principal. Let p be an irreducible element of R. By Exercise 1.5.1, it suffices to show that p is a prime element of R. By Lemma 1.5.2, it is enough to show that the principal ideal (p) is a prime ideal. Let P be a minimal prime over-ideal of (p). By Corollary 9.6.12 (Krull's Hauptidealsatz), $\operatorname{ht}(P) = 1$. By hypothesis, $P = (\pi)$ is principal. Then π divides p and since p is irreducible, it follows that π and p are associates. This implies $P = (p)$. The converse follows from Exercise 1.5.2. □

COROLLARY 11.4.13. *Let R be a noetherian normal integral domain. Then R is a UFD if and only if* $\operatorname{Cl}(R) = (0)$.

PROOF. The proof is left to the reader. □

THEOREM 11.4.14. *(Nagata's Theorem) Let R denote a noetherian normal integral domain with field of fractions K. Let f be a nonzero noninvertible element of R with divisor* $\operatorname{Div}(f) = \nu_1 P_1 + \cdots + \nu_n P_n$. *The sequence of abelian groups*

$$1 \to R^* \to R[f^{-1}]^* \xrightarrow{\operatorname{Div}} \bigoplus_{i=1}^{n} \mathbb{Z}P_i \to \operatorname{Cl}(R) \to \operatorname{Cl}(R[f^{-1}]) \to 0$$

is exact.

PROOF. There is a tower of subgroups $R^* \subseteq R[f^{-1}]^* \subseteq K^*$. There exists a map α such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & R^* \arrow[r] \arrow[d, "\delta"] & K^* \arrow[r, "\operatorname{Div}"] \arrow[d, "\varepsilon"] & \operatorname{Prin} R \arrow[r] \arrow[d, "\alpha"] & 0 \\
1 \arrow[r] & R[f^{-1}]^* \arrow[r] & K^* \arrow[r, "\operatorname{Div}"] & \operatorname{Prin} R[f^{-1}] \arrow[r] & 0
\end{tikzcd}$$

is commutative, where δ is set inclusion and ε is set equality. Clearly, α is onto. By the Snake Lemma (Theorem 2.5.2), $\operatorname{coker}\delta \cong \ker\alpha$. Hence

$$1 \to R^* \to R[f^{-1}]^* \to \ker\alpha \to 0 \tag{4.2}$$

is exact. Using Exercise 3.3.9, $X_1(R[f^{-1}])$ is the subset of $X_1(R)$ consisting of those primes of height one in R that do not contain f. We can view $\operatorname{Div}(R[f^{-1}])$ as the free $\mathbb{Z}$-submodule of $\operatorname{Div}(R)$ generated by primes in $X_1(R[f^{-1}])$. Let β be the projection map onto this subgroup defined by $P_1 \mapsto 0, \dots, P_n \mapsto 0$. This diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Prin}(R) \arrow[r] \arrow[d, "\alpha"] & \operatorname{Div}(R) \arrow[r] \arrow[d, "\beta"] & \operatorname{Cl}(R) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & \operatorname{Prin}(R[f^{-1}]) \arrow[r] & \operatorname{Div}(R[f^{-1}]) \arrow[r] & \operatorname{Cl}(R[f^{-1}]) \arrow[r] & 0
\end{tikzcd}$$

commutes and the rows are exact. Since β is onto, so is γ. The group $\operatorname{Div} R$ is free on $X_1(R)$. The only height one primes that contain f are $P_1, \dots, P_n$. Therefore, the kernel of β is the free subgroup $\mathbb{Z}P_1 \oplus \cdots \oplus \mathbb{Z}P_n$. By the Snake Lemma (Theorem 2.5.2),

$$0 \to \ker\alpha \to \ker\beta \to \ker\gamma \to 0 \tag{4.3}$$

is exact. Combine (4.2) and (4.3) to complete the proof. □

EXAMPLE 11.4.15. Let k be a field with characteristic not equal to 3. Let

$$R = \frac{k[x,y,z]}{(z^3 - y(y-x)(x+1))}.$$

The reader should verify that R is an integrally closed noetherian integral domain. This can be done using the method outlined in Exercise 11.4.2. Let K be the quotient field of R. In this example we compute the class group $\operatorname{Cl}(R)$ and the group of invertible elements, R^*. To compute the class group $\operatorname{Cl}(R)$, we first show that there exists a localization of R which is factorial. The transformation we use is based on the blowing-up of the maximal ideal (x,y,z). The reader is referred to [**28**, pp. 28–29] for more details. Start with the equation

$$z^3 - y(y-x)(x+1)) = 0 \tag{4.4}$$

in K. Divide both sides of (4.4) by x^3 and substitute $v = y/x$ and $w = z/x$ to get

$$w^3 - v(v-1)(1+x^{-1}) = 0. \tag{4.5}$$

Solve (4.5) for x to get

$$x = \frac{v^2 - v}{w^3 - v^2 + v}. \tag{4.6}$$

Now treat v, w as indeterminates and define

$$R = \frac{k[x,y,z]}{(z^3 - y(y-x)(x+1))} \xrightarrow{\phi} k[v,w][(w^3 - v^2 + v)^{-1}] \tag{4.7}$$

by $\phi(x) = (v^2 - v)(w^3 - v^2 + v)^{-1}$, $\phi(y) = v\phi(x)$, and $\phi(z) = w\phi(x)$. The reader should verify that ϕ is a well-defined k-algebra homomorphism and that if we adjoin $(xy(y-x))^{-1}$ to R and $(v^2 - v)^{-1}$ to the ring on the right hand side of (4.7), then

$$R[x^{-1}, y^{-1}, (y-x)^{-1}] \xrightarrow{\phi} k[v,w][v^{-1}, (v-1)^{-1}, (w^3 - v^2 + v)^{-1}] \tag{4.8}$$

is a k-algebra homomorphism which is onto. Since the domain and range of ϕ are both noetherian integral domains with Krull dimension two, ϕ is an isomorphism (Corollary 10.3.4). Since $k[v,w]$ is a unique factorization domain, it follows from Theorem 11.4.14 that the group of units in the ring on the right hand side of (4.8) decomposes into the internal direct product

$$k^* \times \langle v \rangle \times \langle v-1 \rangle \times \langle w^3 - v^2 + v \rangle. \tag{4.9}$$

Using the isomorphism (4.8) we see that the group of units in $R[x^{-1}, y^{-1}, (y-x)^{-1}]$ is generated by k^*, x, y, $y-x$. Since $z^3 - y^2$ is irreducible, $R/(x) \cong k[y,z]/(z^3-y^2)$ is an integral domain of Krull dimension one. Also, $R/(y,z) \cong k[x]$ and $R/(y-x,z) \cong k[x]$. From this it follows that

$$\begin{aligned} \mathfrak{p}_0 &= (x) \\ \mathfrak{p}_1 &= (y,z) \\ \mathfrak{p}_2 &= (y-x,z) \end{aligned} \tag{4.10}$$

are each height one prime ideals of R. Using the identity (4.4) we see that z is a local parameter for each of the two local rings: $R_{\mathfrak{p}_1}$ and $R_{\mathfrak{p}_2}$. From this we compute the divisors:

$$\begin{aligned} \operatorname{Div}(x) &= \mathfrak{p}_0 \\ \operatorname{Div}(y) &= 3\mathfrak{p}_1 \\ \operatorname{Div}(y-x) &= 3\mathfrak{p}_2. \end{aligned} \tag{4.11}$$

Since $R[x^{-1}, y^{-1}, (y-x)^{-1}]$ is factorial, the exact sequence of Nagata (Theorem 11.4.14) is

$$1 \to R^* \to R[(xy(y-x))^{-1}]^* \xrightarrow{\operatorname{Div}} \bigoplus_{i=0}^{2} \mathbb{Z}\mathfrak{p}_i \to \operatorname{Cl}(R) \to 0. \tag{4.12}$$

From (4.12) and (4.11), it follows that $\operatorname{Cl}(R) \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3$ and is generated by the prime divisors $\mathfrak{p}_1$ and $\mathfrak{p}_2$. We remark that from (4.9) and (4.12) it follows that $R^* = k^*$.

4.4. The Approximation Theorem. Let R be a noetherian integrally closed integral domain with quotient field K. If $D = \sum_{P \in X_1(R)} n_P P$ is a divisor in $\operatorname{Div} R$, the *support of* D is the set of primes P in $X_1(R)$ such that the coefficient n_P is nonzero. If $n_P \geq 0$ for all P, then we say D is an *effective divisor*. In the terminology of Section 11.4.3, if $\alpha \in K^*$, then $\operatorname{Div}(\alpha)$ is called a principal divisor. It follows from Corollary 11.4.4 that the set of all principal divisors is a subgroup of $\operatorname{Div} R$. The Approximation Theorem shows that in a certain sense D is "close to" a principal divisor. Specifically, there exists $\alpha \in K^*$ such that $\operatorname{Div}(\alpha) - D$ is an effective divisor, and the support of $\operatorname{Div}(\alpha) - D$ is disjoint from the support of D.

LEMMA 11.4.16. *Let R be a noetherian integrally closed integral domain. Let $r \geq 1$ and $\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_r$ a set of $r+1$ distinct primes in $X_1(R)$. Then there exists $t \in R$ such that $\nu_{\mathfrak{p}}(t) = 1$ and for $1 \leq i \leq r$, $\nu_{\mathfrak{p}_i}(t) = 0$.*

PROOF. Let $\pi_{\mathfrak{p}}$ be an element in R which maps to a local parameter for $R_{\mathfrak{p}}$. If $\pi_{\mathfrak{p}} \notin \bigcup_{i=1}^r \mathfrak{p}_i$, then set $t = \pi_{\mathfrak{p}}$ and stop. Otherwise rearrange the list $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and assume that $\pi_{\mathfrak{p}} \in \bigcap_{i=1}^s \mathfrak{p}_i$ and $\pi_{\mathfrak{p}} \notin \bigcup_{j=1}^{r-s} \mathfrak{p}_{s+j}$ for some $s \geq 1$. Applying Lemma 6.3.2, since $\mathfrak{p}^2 \not\subseteq \bigcup_{i=1}^s \mathfrak{p}_i$, pick $f_0 \in \mathfrak{p}^2 - \bigcup_{i=1}^s \mathfrak{p}_i$. Likewise, for $1 \leq j \leq r-s$, since $\mathfrak{p}_{s+j} \not\subseteq \bigcup_{i=1}^s \mathfrak{p}_i$, pick $f_j \in \mathfrak{p}_{s+j} - \bigcup_{i=1}^s \mathfrak{p}_i$. Set $t = \pi_{\mathfrak{p}} - f_0 f_1 \cdots f_{r-s}$. Then $t \in \mathfrak{p} - \bigcup_{i=1}^r \mathfrak{p}_i$. Thus $\nu_{\mathfrak{p}_i}(t) = 0$ for $1 \leq i \leq r$. Now $f_0 f_1 \cdots f_{r-s} \in \mathfrak{p}^2 R_{\mathfrak{p}}$ and since $\pi_{\mathfrak{p}}$ is a local parameter for $R_{\mathfrak{p}}$, $t \in \mathfrak{p} R_{\mathfrak{p}} - \mathfrak{p}^2 R_{\mathfrak{p}}$. Thus $\nu_{\mathfrak{p}}(t) = 1$. $\square$

THEOREM 11.4.17. *(The Approximation Theorem) Let R be a noetherian integrally closed integral domain with field of fractions K. Let $r \geq 1$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ a set of distinct primes in $X_1(R)$. Let $n_1, \dots, n_r \in \mathbb{Z}$. Then there exists $\alpha \in K$ such that*

$$\nu_{\mathfrak{p}}(\alpha) = \begin{cases} n_i & \text{if } \mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \\ \geq 0 & \text{otherwise.} \end{cases}$$

PROOF. Using Lemma 11.4.16, pick $t_1, \dots, t_r$ in R such that $\nu_{\mathfrak{p}_i}(t_j) = \delta_{i,j}$ (Kronecker delta). In K^*, let $\beta = t_1^{n_1} \cdots t_r^{n_r}$. If there is no height one prime $\mathfrak{p}$ in $X_1(R) - \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ such that $\nu_{\mathfrak{p}}(\beta) < 0$, then we take $\alpha = \beta$ and stop. Otherwise, let $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ be those height one primes in $X_1(R) - \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ such that $\nu_{\mathfrak{q}_j}(\beta) < 0$ for $1 \leq j \leq s$. Using Lemma 11.4.16, pick $u_1, \dots, u_s$ in R such that

$$\nu_{\mathfrak{p}}(u_j) = \begin{cases} 1 & \text{if } \mathfrak{p} = \mathfrak{q}_j, \\ 0 & \text{if } \mathfrak{p} = \mathfrak{q}_i, \text{ for some } i \neq j, \\ 0 & \text{if } \mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}. \end{cases}$$

Let $m_j = \nu_{\mathfrak{q}_j}(\beta)$ for $1 \leq j \leq s$. Then $\alpha = t_1^{n_1} \cdots t_r^{n_r} u_1^{-m_1} \cdots u_s^{-m_s}$ satisfies the conclusion of the theorem. □

COROLLARY 11.4.18. *Let R be a noetherian integrally closed integral domain with field of fractions K. If D is a divisor in* $\operatorname{Div} R$*, then there exists an effective divisor E in* $\operatorname{Div} R$ *such that the support of E is disjoint from the support of D and modulo* $\operatorname{Prin} R$ *the divisors E and D are congruent to each other.*

PROOF. By applying Theorem 11.4.17 to $-D$, there exists $\alpha \in K^*$ such that $\operatorname{Div}(\alpha) + D$ is an effective divisor with support that is disjoint from the support of D. □

4.5. Exercises.

EXERCISE 11.4.1. Let R be a commutative ring and assume $\operatorname{Rad}_R(0)$ is nonzero. Let x be a nonzero nilpotent element in R and let P be a prime ideal of R containing $\operatorname{annih}_R(x)$. Show that the image of x in the local ring R_P is nonzero and nilpotent.

EXERCISE 11.4.2. Let k be a field and $n \geq 2$ an integer which is invertible in k. Let $f \in k[x,y,z]$ be the polynomial $z^n - xy$ and let R be the quotient $k[x,y,z]/(f)$. In R we prefer not to use special adornment for cosets. That is, write simply x, or z for the coset represented by that element.

(1) Show that R is a noetherian integral domain and $\dim(R) = 2$.
(2) Let $P = (x,z)$ be the ideal in R generated by x and z. Show that P is a prime ideal of height one.
(3) Let $I = (x)$ be the principal ideal generated by x in R. Show that $\operatorname{Rad}(I) = P$.
(4) Show that R_P is a DVR and z generates the maximal ideal $\mathfrak{m}_P$.
(5) Show that $\nu_P(x) = n$ and $\operatorname{Div}(x) = nP$.
(6) Show that $R[x^{-1}] \cong k[x,z][x^{-1}]$ and $R[y^{-1}] \cong k[y,z][y^{-1}]$. Show that $R_{\mathfrak{p}}$ is regular if $\mathfrak{p} \in U(x) \cup U(y)$.
(7) Show that the only prime ideal containing both x and y is the maximal ideal $\mathfrak{m} = (x,y,z)$, which has height 2. Show that $\operatorname{depth}(R_{\mathfrak{m}}) = 2$. Apply Theorem 11.4.8 to show that R is integrally closed.
(8) Show that $\operatorname{Cl}(R[x^{-1}]) = 0$. (Hint: $R[x^{-1}]$ is a UFD.)
(9) $\operatorname{Cl}(R)$ is cyclic of order n.

EXERCISE 11.4.3. Let $S = \mathbb{R}[x,y]/(f)$, where $f = x^2 + y^2 - 1$. By Exercise 2.2.3, S is not a UFD. This exercise is an outline of a proof that $\mathrm{Cl}(S)$, the class group of S, is cyclic of order two.

(1) Let R be the $\mathbb{R}$-subalgebra of $S[x^{-1}]$ generated by yx^{-1} and x^{-1}. Show that $R = \mathbb{R}[yx^{-1}, x^{-1}]/(1 + (yx^{-1})^2 - (x^{-1})^2)$ is a PID.
(2) Show that $R[x] = S[1/x]$ is a PID.
(3) Let $P_1 = (x, y-1)$ and $P_2 = (x, y+1)$. Show that S_{P_1} and S_{P_2} are local principal ideal domains. Conclude that S is normal.
(4) Show that $\mathrm{Div}(x) = P_1 + P_2$ and $\mathrm{Div}(y-1) = 2P_1$.
(5) Use Theorem 11.4.14 to prove that that $\mathrm{Cl}(S)$ is generated by P_1 and has order two.

EXERCISE 11.4.4. (Nagata's Theorem) Let R be a noetherian normal integral domain with field of fractions K. Let $W \subseteq R - \{0\}$ be a multiplicative set. Modify the proof of Theorem 11.4.14 to show that there is an epimorphism of groups $\gamma : \mathrm{Cl}(R) \to \mathrm{Cl}(W^{-1}R)$ and that the kernel of γ is generated by the classes of those prime divisors $P \in X_1(R) - X_1(W^{-1}R)$.

EXERCISE 11.4.5. This exercise is a continuation of Exercise 11.4.2. Let k be a field and $n \geq 2$ an integer which is invertible in k. Let $f \in k[x,y,z]$ be the polynomial $z^n - xy$ and let R be the quotient $k[x,y,z]/(f)$. Let $\mathfrak{m}$ be the maximal ideal (x,y,z) in R, and $\hat{R}$ the $\mathfrak{m}$-adic completion of R.

(1) Show that $\hat{R} \cong k[[x,y]][z]/(f)$.
(2) Follow the procedure outlined in Exercise 11.4.2 to show that $\hat{R}$ is a noetherian normal integral domain and $\mathrm{Cl}(\hat{R})$ is a cyclic group of order n generated by the class of the prime ideal $P = (x,z)$.

In Algebraic Geometry, the ring R is the affine coordinate ring of the surface $X = Z(z^n - xy)$ in $\mathbb{A}^3_k$ and the point $p = (0,0,0)$ is called a singular point of X. It follows from [**17**, A5] and [**39**] that p is a rational double point of type A_{n-1}.

EXERCISE 11.4.6. Let k be a field such that $\operatorname{char} k \neq 2$. For the ring

$$R = \frac{k[x,y,z]}{(z^2 - (y^2 - x^2)(x+1))}$$

follow the method of Example 11.4.15 to prove the following:

(1) $R[x^{-1}, (y^2 - x^2)^{-1}]$ is a UFD.
(2) The group of invertible elements in $R[x^{-1}, (y^2 - x^2)^{-1}]$ is generated by $x, y - x, y + x$.
(3) $\mathfrak{q}_1 = (x, z - y)$, $\mathfrak{q}_2 = (x, z + y)$, $\mathfrak{p}_1 = (y - x, z)$, $\mathfrak{p}_2 = (y + x, z)$, are height one prime ideals in R.
(4) $\mathrm{Div}(x) = \mathfrak{q}_1 + \mathfrak{q}_2$, $\mathrm{Div}(y - x) = 2\mathfrak{p}_1$, $\mathrm{Div}(y + x) = 2\mathfrak{p}_2$.
(5) $\mathrm{Cl}(R) \cong \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

EXERCISE 11.4.7. Let k be a field and $n > 1$ an integer that is invertible in k. Assume moreover that k contains a primitive nth root of unity, say ζ. Let $a_1, \dots, a_n$ be distinct elements of k. For $1 \leq i \leq n$, define linear polynomials $\ell_i(x,y) = y - a_i x$ in $k[x,y]$, and set $f(x,y) = \ell_1(x,y) \cdots \ell_n(x,y)$. For the ring

$$R = \frac{k[x,y,z]}{(z^n - f(x,y)(x+1))}$$

follow the method of Example 11.4.15 to prove the following:

(1) $R[x^{-1}, f(x,y)^{-1}]$ is a UFD.
(2) The group of invertible elements in $R[x^{-1}, f(x,y)^{-1}]$ is generated by $x, \ell_1, \dots, \ell_n$.
(3) Let $\mathfrak{q}_i = (x, z - \zeta^i y)$, for $i = 0, \dots, n-1$. Let $\mathfrak{p}_j = (\ell_j, z)$, for $j = 1, \dots, n$. Then $\mathfrak{q}_0, \dots, \mathfrak{q}_{n-1}$, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are height one prime ideals in R.
(4) $\operatorname{Div}(x) = \mathfrak{q}_0 + \cdots + \mathfrak{q}_{n-1}$, and $\operatorname{Div}(\ell_j) = n\mathfrak{p}_j$, for $j = 1, \dots, n$.
(5) $\operatorname{Cl}(R) \cong (\mathbb{Z})^{(n-1)} \oplus (\mathbb{Z}/n)^{(n)}$.

Notice that for $n = 2$, this agrees with computation carried out in Exercise 11.4.6. The ring R was the focus of the article [**20**] where many other interesting properties of R were studied.

EXERCISE 11.4.8. Let k be a field and $n > 2$ an integer that is invertible in k. Let $a_1, \dots, a_{n-1}$ be distinct elements of k. For $1 \le i \le n-1$, define linear polynomials $\ell_i(x,y) = y - a_i x$ in $k[x,y]$, and set $f(x,y) = \ell_1(x,y) \cdots \ell_{n-1}(x,y)$. For the ring

$$R = \frac{k[x,y,z]}{(z^n - f(x,y)(x+1))}$$

follow the method of Example 11.4.15 to prove the following:

(1) $R[x^{-1}, f(x,y)^{-1}]$ is a UFD.
(2) The group of invertible elements in $R[x^{-1}, f(x,y)^{-1}]$ is generated by $x, \ell_1, \dots, \ell_{n-1}$.
(3) Let $\mathfrak{p}_0 = (x)$, and for $i = 1, \dots, n-1$, let $\mathfrak{p}_i = (\ell_i, z)$. Then $\mathfrak{p}_0, \dots, \mathfrak{p}_{n-1}$, are height one prime ideals in R.
(4) $\operatorname{Div}(x) = \mathfrak{p}_0$, and $\operatorname{Div}(\ell_j) = n\mathfrak{p}_j$, for $j = 1, \dots, n-1$.
(5) $\operatorname{Cl}(R) \cong (\mathbb{Z}/n)^{(n-1)}$.

Notice that for $n = 3$, this agrees with computation carried out in Example 11.4.15.

5. Fibers of a Faithfully Flat Morphism

This section is divided into three parts each with its own somewhat different context. First we consider a faithfully flat extension $f : R \to S$ of commutative noetherian rings. The point of view we take is to determine which properties of R are inherited by S, and conversely. The second main result is a proof of [**22**, Proposition 10.3.1] which states the following. Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Then we show that if K/k is an extension of fields, then there exists a noetherian local ring S and a faithfully flat local homomorphism $\theta : R \to S$ such that $S/\mathfrak{m}S = K$. In the last part, our context is an extension of commutative rings defined by adjoining the nth root of an element. Specifically, let R be a commutative ring, $n \ge 2$, $a \in R$, and $S = R[x]/(x^n - a)$. Among other results, we derive sufficient conditions on n and a such that if R is a noetherian normal integral domain, then so is S. General references for this section are [**41**, §21], [**22**] and [**18**, Section 9.4].

Throughout this section R and S will be commutative rings. Usually R and S will be noetherian. Let $f : R \to S$ be a homomorphism of rings, and $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 3.3.3. Let $P \in \operatorname{Spec} R$. The residue field at P is $k(P) = R_P/PR_P$. The fiber over P of the map $f^\sharp$ is $\operatorname{Spec}(S \otimes_R k(P))$, which is homeomorphic to $(f^\sharp)^{-1}(P)$, by Exercise 3.4.3. By Exercise 3.4.2, if Q is a prime ideal of S lying over P, then the corresponding prime ideal of $S \otimes_R k(P)$ is $Q \otimes_R k(P)$ and the local ring is $S_Q \otimes_R k(P) = S_Q/PS_Q$.

5.1. Flat Algebras and Depth.

THEOREM 11.5.1. *Assume all of the following are satisfied.*

(1) R is a noetherian local ring with maximal ideal $\mathfrak{m}$.
(2) S is a noetherian local ring with maximal ideal $\mathfrak{n}$.
(3) $f : R \to S$ is a local homomorphism of local rings.
(4) A is a finitely generated R-module and B is a finitely generated S-module which is a flat R-module.

Then

$$\begin{aligned}\operatorname{depth}_S(A \otimes_R B) &= \operatorname{depth}_R(A) + \operatorname{depth}_{S \otimes_R R/\mathfrak{m}}(B \otimes_R R/\mathfrak{m}) \\ &= \operatorname{depth}_R(A) + \operatorname{depth}_{S/\mathfrak{m}S}(B/\mathfrak{m}B).\end{aligned}$$

PROOF. The proof is by induction on $n = \operatorname{depth}_R(A) + \operatorname{depth}_S(B/\mathfrak{m}B)$. If $n = 0$, then by Exercise 11.3.2 we have $\mathfrak{m} \in \operatorname{Assoc}_R(A)$ and $\mathfrak{n} \in \operatorname{Assoc}_S(B/\mathfrak{m}B)$. By Theorem 9.3.10,

$$\operatorname{Assoc}_S(A \otimes_R B) = \bigcup_{P \in \operatorname{Assoc}_R(A)} \operatorname{Assoc}_S(B \otimes_R R/P).$$

We have $\mathfrak{n}$ in the right hand side, hence $\mathfrak{n}$ is in $\operatorname{Assoc}_S(A \otimes_R B)$. By Exercise 11.3.2, $\operatorname{depth}_S(A \otimes_R B) = 0$. Now assume $n > 0$ and that the equation holds for modules A', B' such that $\operatorname{depth}_R(A') + \operatorname{depth}_S(B'/\mathfrak{m}B') < n$.

Case 1: Suppose $\operatorname{depth}_R(A) > 0$. Let α be a regular element for A in $\mathfrak{m}$. Since B is R-flat, $f(\alpha)$ is a regular element for $A \otimes_R B$ in $\mathfrak{n}$. By our Induction Hypothesis, the equation $\operatorname{depth}_S(A/\alpha A \otimes_R B) = \operatorname{depth}_R(A/\alpha A) + \operatorname{depth}_{S/\mathfrak{m}S}(B/\mathfrak{m}B)$ holds for $A/\alpha A$ and B. Adding 1 to both sides shows the equation holds for A and B.

Case 2: Assume $\operatorname{depth}_R(A) = 0$ and $\operatorname{depth}_S(B/\mathfrak{m}B) > 0$. Let β be a regular element for $B/\mathfrak{m}B = B \otimes_R R/\mathfrak{m}$ in $\mathfrak{n}$. Start with the sequence of S-modules

$$0 \to B \xrightarrow{\ell_\beta} B \to B/\beta B \to 0 \tag{5.1}$$

where ℓ_β is the "left multiplication by β" homomorphism. Applying the functor $(\ ) \otimes_R R/\mathfrak{m}$ to (5.1), we get the sequence

$$0 \to B \otimes_R R/\mathfrak{m} \xrightarrow{\ell_\beta \otimes 1} B \otimes_R R/\mathfrak{m} \to (B/\beta B) \otimes_R R/\mathfrak{m} \to 0. \tag{5.2}$$

By choice of β, (5.2) is exact. By Proposition 10.4.14, (5.1) is exact and $B/\beta B$ is a flat R-module. Upon tensoring (5.1) with $A \otimes_R (\ )$ we get

$$0 \to A \otimes_R B \xrightarrow{1 \otimes \ell_\beta} A \otimes_R B \to A \otimes_R (B/\beta B) \to 0 \tag{5.3}$$

which is an exact sequence, by Lemma 8.3.2. This means β is a regular element for $A \otimes_R B$ in $\mathfrak{n}$. Therefore $\operatorname{depth}_S(A \otimes_R (B/\beta B)) = \operatorname{depth}_S(A \otimes_R B) - 1$. Since (5.2) is an exact sequence of $S/\mathfrak{m}S$-modules, β is a regular element for $B/\mathfrak{m}B$ in $\mathfrak{n}S/\mathfrak{m}S$. Therefore $\operatorname{depth}_{S/\mathfrak{m}S}((B/\beta B) \otimes_R R/\mathfrak{m}) = \operatorname{depth}_{S/\mathfrak{m}S}(B \otimes_R R/\mathfrak{m}) - 1$. By our Induction Hypothesis, the equation

$$\operatorname{depth}_S(A \otimes_R (B/\beta B)) = \operatorname{depth}_R(A) + \operatorname{depth}_{S/\mathfrak{m}S}((B/\beta B) \otimes_R R/\mathfrak{m})$$

holds for A and $B/\beta B$. Adding 1 to both sides shows the equation holds for A and B. $\square$

COROLLARY 11.5.2. *Assume $f : R \to S$ is a local homomorphism of noetherian local rings making S into a flat R-algebra. If the maximal ideal of R is $\mathfrak{m}$, then the following are true.*

(1) $\operatorname{depth}(S) = \operatorname{depth}(R) + \operatorname{depth}(S/\mathfrak{m}S)$.
(2) S is Cohen-Macaulay if and only if R and $S/\mathfrak{m}S$ are both Cohen-Macaulay.

PROOF. (1): Follows straight from Theorem 11.5.1.

(2): By Theorems 6.3.5 and 9.6.16, $\dim(S) = \dim(R) + \dim(S/\mathfrak{m}S)$. By Corollary 11.3.12, the depth of a noetherian local ring is always less than or equal to its Krull dimension. Part (2) follows from these facts and Part (1). □

COROLLARY 11.5.3. *Assume $f : R \to S$ is a faithfully flat homomorphism of commutative noetherian rings. Let i be a positive integer. Then the following are true.*

(1) If S satisfies property (S_i) of Definition 11.4.5, then so does R.
(2) If R satisfies property (S_i) and for each $P \in \operatorname{Spec} R$, $S \otimes_R k(P)$ satisfies (S_i), then S satisfies property (S_i).

PROOF. (1): Let $P \in \operatorname{Spec} R$. By Lemma 3.5.4, $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is onto. By Exercise 3.3.8 there exists $Q \in \operatorname{Spec} S$ which is a minimal prime over-ideal of PS and $f^\sharp(Q) = P$. Then $\dim(S_Q \otimes_R k(P)) = \operatorname{depth}(S_Q \otimes_R k(P)) = 0$. By Theorem 11.5.1, $\operatorname{depth}(S_Q) = \operatorname{depth}(R_P)$. It follows that

$$\begin{aligned}\operatorname{depth}(R_P) &= \operatorname{depth}(S_Q) \\ &\geq \inf(i, \dim(S_Q)) \\ &= \inf(i, \dim(R_P))\end{aligned}$$

which shows R has property (S_i).

(2): Let $Q \in \operatorname{Spec} S$ and set $P = Q \cap R$. Applying Theorems 11.5.1 and 9.6.16, we get

$$\begin{aligned}\operatorname{depth}(S_Q) &= \operatorname{depth}(R_P) + \operatorname{depth}(S_Q \otimes_R k(P)) \\ &\geq \inf(i, \dim(R_P)) + \inf(i, \dim(S_Q \otimes_R k(P))) \\ &\geq \inf(i, \dim(R_P) + \dim(S_Q \otimes_R k(P))) \\ &= \inf(i, \dim(S_Q))\end{aligned}$$

which shows S has property (S_i). □

THEOREM 11.5.4. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$, S a noetherian local ring with maximal ideal $\mathfrak{n}$, and $f : R \to S$ a local homomorphism of local rings. Then the following are true.*

(1) If S is a flat R-algebra and regular, then R is regular.
(2) If
  (a) $\dim(S) = \dim(R) + \dim(S/\mathfrak{m}S)$,
  (b) R is regular, and
  (c) $S/\mathfrak{m}S$ is regular,

  then S is a flat R-algebra and S is regular.

PROOF. (1): This is Exercise 11.3.13. To prove it, apply Proposition 8.4.16 and Theorem 11.3.26.

(2): By (b), there exists $\{a_1, \dots, a_m\} \subseteq \mathfrak{m}$ which is a regular system of parameters for R. By (c), there exists $\{b_1, \dots, b_n\} \subseteq \mathfrak{n}$ which maps onto a regular system of parameters for $S/\mathfrak{m}S$. Then $\{f(a_1), \dots, f(a_m), b_1, \dots, b_n\}$ generate the ideal $\mathfrak{n}$. By (a), $\dim(S) = m + n$. Therefore, S is regular.

To prove that S is a flat R-algebra, we utilize (5) implies (1) of Theorem 10.4.13. It suffices to show that $\operatorname{gr}_{\mathfrak{m}}(R) \otimes_{R/\mathfrak{m}} S/\mathfrak{m}S \cong \operatorname{gr}_{\mathfrak{m}S}(S)$. In the notation from above, there is a regular system of parameters $\{a_1, \dots, a_m\} \subseteq \mathfrak{m}$ for R such that $\{f(a_1), \dots, f(a_m)\}$ is a regular sequence for S in $\mathfrak{n}$. By Theorem 11.3.6 (2),

$$\operatorname{gr}_{\mathfrak{m}S}(S) = (S/\mathfrak{m}S)[t_1, \dots, t_m] = (R/\mathfrak{m})[t_1, \dots, t_m] \otimes_{R/\mathfrak{m}} S/\mathfrak{m}S = \operatorname{gr}_{\mathfrak{m}}(R) \otimes_{R/\mathfrak{m}} S/\mathfrak{m}S$$

which completes the proof. □

COROLLARY 11.5.5. *Assume $f : R \to S$ is a faithfully flat homomorphism of commutative noetherian rings. Let $i \geq 0$ be a natural number. Then the following are true.*

1. *If S satisfies property (R_i) of Definition 11.4.5, then so does R.*
2. *If R satisfies property (R_i) and for each $P \in \operatorname{Spec} R$, $S \otimes_R k(P)$ satisfies (R_i), then S satisfies property (R_i).*

COROLLARY 11.5.6. *Assume $f : R \to S$ is a faithfully flat homomorphism of commutative noetherian rings.*

1. *If S is a normal ring, then R is a normal ring. Conversely, if R is a normal ring and for each $P \in \operatorname{Spec} R$, $S \otimes_R k(P)$ is a normal ring, then S is a normal ring.*
2. *Part (1) is true if "normal ring" is replaced with "Cohen-Macaulay ring".*
3. *Part (1) is true if "normal ring" is replaced with "reduced ring".*

PROOF. (1): If S is a normal ring, then R is a normal ring, by Exercise 6.1.4 (3). Notice that this is true without the hypothesis that the rings R and S are noetherian. By Theorem 11.4.8, a commutative noetherian ring is normal if and only if the properties (R_1) and (S_2) are satisfied. Therefore, the "conversely" statement in (1) follows from Corollaries 11.5.5 and 11.5.3.

(2): By Example 11.4.6 (3), a commutative noetherian ring is Cohen-Macaulay if and only if the properties (S_i) are satisfied for all $i \geq 1$. Therefore, (2) follows from Corollary 11.5.3.

(3): By Proposition 11.4.7, a commutative noetherian ring is reduced if and only if the properties (R_0) and (S_1) are satisfied. Therefore, (3) follows from Corollaries 11.5.5 and 11.5.3. □

5.2. Existence of a Flat Extension. Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let K/k be an extension of fields. The purpose of this section is to prove that there exists a noetherian local ring S and a faithfully flat local homomorphism $\theta : R \to S$ such that $S/\mathfrak{m}S = K$. This result appears as Theorem 11.5.7 below. All of the results in this section are based on [**22**, Proposition 10.3.1] and its proof.

THEOREM 11.5.7. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let K/k be an extension of fields. Then there exists a noetherian local ring S and a local homomorphism of local rings $\theta : R \to S$ such that $S/\mathfrak{m}S = K$ and S is a faithfully flat R-algebra.*

PROOF. The method of proof is to reduce to the case where K is a simple extension of k. To accomplish this, we write K as a direct limit of subfields over a well ordered index set.

Step 1: Assume $K = k(t)$ is a transcendental extension of k of degree one. Let Q be the kernel of the natural map $R[t] \to R[t] \otimes_R k = k[t]$. Then Q is equal to the ideal $\mathfrak{m}[t]$. Let S be the local ring of $R[t]$ at the prime ideal Q. By Exercise 3.1.6, the residue field S/QS is equal to the quotient field of $R[t]/Q$, which we identify with $K = k(t)$. Since Q is generated by $\mathfrak{m}$, we have $R \to S$ is a local homomorphism of local rings and $\mathfrak{m}S = QS$. Since S is flat over $R[t]$ and $R[t]$ is flat over R, we have S is faithfully flat over R. Since R is noetherian, by Theorem 6.2.1 and Corollary 4.1.13, the ring S is noetherian.

Step 2: Assume $K = k(t)$ is a finite dimensional algebraic extension of k generated by the primitive element t. Let $f = \operatorname{min.poly}_k(t)$ be the minimal polynomial of t in $k[x]$. Let $F \in R[x]$ be a monic polynomial which maps onto f under the natural map $R[x] \to R[x] \otimes_R k$.

Let $S = R[x]/(F)$. By Corollary 5.6.3, S is a local ring with maximal ideal $\mathfrak{m}S$, residue field $S/\mathfrak{m}S = K$, and S is finitely generated and free as an R-module. Therefore, S is a faithfully flat R-algebra. Since R is noetherian, by Theorem 6.2.1, the ring S is noetherian.

Step 3: We will omit the details, but the reader should verify that the proof of Proposition 4.1.23 can be modified to show that there exists a well ordered set I and a family $\{K_\xi \mid \xi \in I\}$ of subfields of K indexed by I satisfying the following.

(1) If 1 is the least element of I, then $K_1 = k$.
(2) If α and β are in I and $\alpha \le \beta$, then $k \subseteq K_\alpha \subseteq K_\beta \subseteq K$.
(3) For each $\beta \in I$, if β has an immediate predecessor, say α, then there exists $x_\beta \in K_\beta$ such that $K_\beta = K_\alpha(x_\beta)$ is a simple extension. If β has no immediate predecessor, then $K_\beta = \bigcup_{\xi \in (-\infty,\beta)} K_\xi$.
(4) $K = \bigcup_{\xi \in I} K_\xi$.

By Transfinite Induction, Proposition 1.2.3, we define a direct limit system of local rings $\{S_\xi \mid \xi \in I\}$ over the index set I. First we set $S_1 = R$. Inductively, assume $\delta \in I$, $1 < \delta$. Assume for the well ordered set $(-\infty,\delta)$ that there is a direct limit system $\{S_\xi, \phi^\alpha_\beta\}$ where

(A) $S_1 = R$.
(B) Each S_ξ is a noetherian local ring with maximal ideal $\mathfrak{m}_\xi$ and residue field $S_\xi/\mathfrak{m}_\xi = K_\xi$.
(C) If $\alpha \le \beta < \delta$, then $\phi^\alpha_\beta : S_\alpha \to S_\beta$ is a local homomorphism of local rings, $\mathfrak{m}_\beta = \mathfrak{m}_\alpha S_\beta$, and S_β is a faithfully flat S_α-algebra.

To define S_δ there are two cases. If δ has an immediate predecessor, say β, then K_δ is a simple extension of K_β. By Step 1 or Step 2 there exists a noetherian local ring S_δ which is a faithfully flat S_α-algebra with maximal ideal $\mathfrak{m}_\delta$ and residue field K_δ. For any $\alpha \le \beta$ the homomorphism ϕ^α_δ is taken to be $\phi^\beta_\delta \circ \phi^\alpha_\beta$. If δ has no immediate predecessor, then $K_\delta = \bigcup_{\xi \in (-\infty,\delta)} K_\xi$. In this case we define S_δ to be the direct limit over the well ordered index set $(-\infty,\delta)$. By Exercise 2.7.8 and Corollary 10.5.4, $S_\delta = \varinjlim_{\xi \in (-\infty,\delta)} S_\xi$ is a noetherian local ring which is a faithfully flat R-algebra with maximal ideal $\mathfrak{m}_\delta = \varinjlim_\xi \mathfrak{m}_\xi = \mathfrak{m}_\xi S_\delta$, and residue field K_δ. Definition 2.7.2, the natural homomorphisms $\phi^\alpha_\delta : S_\alpha \to S_\delta$ exist and we have $\phi^\alpha_\delta = \phi^\beta_\delta \circ \phi^\alpha_\beta$ whenever $\alpha \le \beta < \delta$. By Transfinite Induction, the direct limit system $\{S_\xi, \phi^\alpha_\beta\}$ exists over the index set I. By Exercise 2.7.8 and Corollary 10.5.4, if we define S to be the limit $S_\delta = \varinjlim_{\xi \in I} S_\xi$, then S is a noetherian local ring which is a faithfully flat R-algebra with maximal ideal $\mathfrak{m}_\delta = \varinjlim_\xi \mathfrak{m}_\xi = \mathfrak{m}_\xi S$, and residue field $K = \bigcup_{\xi \in I} K_\xi$. □

COROLLARY 11.5.8. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let $\mathfrak{C}$ be the category whose objects are the noetherian local faithfully flat R-algebras S such that $S \otimes_R R/\mathfrak{m}$ is a field. The morphisms of $\mathfrak{C}$ are R-algebra homomorphisms. Let $\mathfrak{D}$ be the category whose objects are field extensions of k and whose morphisms are k-algebra homomorphisms. Then the functor $(\,) \otimes_R k : \mathfrak{C} \to \mathfrak{D}$ is essentially surjective.*

PROOF. This is a restatement of Theorem 11.5.7. □

COROLLARY 11.5.9. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let K/k be a finite dimensional extension of fields. Then there exists a noetherian local ring S and a local homomorphism of local rings $\theta : R \to S$ such that $S/\mathfrak{m}S = K$ and S is a finitely generated faithfully flat R-module.*

PROOF. In Step 3 of the proof of Theorem 11.5.7, the index set I can be taken to be finite. For the induction step, Step 2 is applied to get the ring S_δ, hence S_δ is a finitely generated free R-module. □

COROLLARY 11.5.10. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let K/k be an extension of fields. Then there exists a local ring S and a local homomorphism of local rings $\theta : R \to S$ such that $S/\mathfrak{m}S = K$ and S is a faithfully flat R-algebra.*

PROOF. Notice that in Steps 1 and 2 of Theorem 11.5.7 the hypothesis that R is noetherian was only used to prove that S is noetherian. In Step 3 the hypothesis that each S_ξ is noetherian was only used when Corollary 10.5.4 was applied to prove that the direct limit is noetherian. □

5.3. Ramified Radical Extensions. As another application of Theorem 11.5.1, we study the important class of finite extensions of commutative rings defined by adjoining an nth root of an element. Let R be a commutative ring, $n \geq 2$, $a \in R$, and set $S = R[x]/(x^n - a)$. We say S/R is a *radical extension of degree n*. In this section, the emphasis is on radical extensions which are not separable over R. Such an extension is also said to be a *ramified extension*. Our goal is to derive necessary and sufficient conditions on n and a such that if R is a noetherian normal integral domain, then so is S. Necessary conditions are provided by Lemma 11.5.12 (2). Sufficient conditions are stated in Lemma 11.5.13 and Theorem 11.5.14. For reference, we state sufficient conditions for S to be a separable R-algebra. The results of this section are based on [**18**, Section 9.4].

LEMMA 11.5.11. *Let R be a commutative ring, $n \geq 2$, and $a \in R$. Then the following are true for the radical extension $S = R[x]/(x^n - a)$.*

(1) S is an R-algebra which is a finitely generated free R-module of rank n with basis $1, x, \dots, x^{n-1}$.
(2) S is separable over R if and only if a and n are both invertible in R.
(3) Let $\theta : R \to S$ be the structure homomorphism. Then $\theta^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ is onto and the closed set $V(x) \subseteq \operatorname{Spec} S$ is mapped homeomorphically onto the closed set $V(a) \subseteq \operatorname{Spec} R$.
(4) If $Q \in \operatorname{Spec} S$ and $P = Q \cap R$, then
  (a) $\operatorname{ht}(Q) = \operatorname{ht}(P)$,
  (b) $\dim(S_Q/PS_Q) = 0$, and
  (c) $\operatorname{depth}(S_Q) = \operatorname{depth}(R_P)$.
(5) For $i \geq 1$, S satisfies property (S_i) of Definition 11.4.5 if and only if R does.

PROOF. (1) and (2): These follow from Example 1.6.10 (2) and Exercise 5.5.5, respectively.

(3): By (1), S is faithfully flat and integral over R. By Lemma 3.5.4, $\theta^\sharp$ is onto. Let $\eta : S \to S/(x)$ be the natural map. Then $\eta\theta(a) = 0$, so there is a commutative diagram

$$\begin{tikzcd} R \arrow[r, "\theta"] \arrow[d] & S = R[x]/(x^n - a) \arrow[d, "\eta"] \\ R/(a) \arrow[r, "\bar{\theta}"] & S/(x) \end{tikzcd}$$

and the reader should verify that $\bar{\theta}$ is an isomorphism. By Exercise 3.3.5, there is a commutative diagram

$$\begin{tikzcd} V(x) \arrow[r, "\bar{\theta}^\sharp"] \arrow[d, "\subseteq"] & V(a) \arrow[d, "\subseteq"] \\ \operatorname{Spec} S \arrow[r, "\theta^\sharp"] & \operatorname{Spec} R \end{tikzcd}$$

and $\bar{\theta}^\sharp$ is a homeomorphism.

(4) and (5): Part (4) follows from Theorems 6.3.5, 9.6.17, and Corollary 11.5.2. Part (5) follows from Part (4). □

LEMMA 11.5.12. *Let R be a commutative ring and a an element of R that is not a zero divisor. If $n \geq 2$ and $e \geq 1$, then the following are true for the radical extension $S = R[x]/(x^n - a^e)$.*

(1) a and x are not zero divisors in S.
(2) If a is not a unit in R and $e \geq 2$, then S is not integrally closed in $Q(S)$, the total ring of quotients of S.

PROOF. (1): Since S is a free R-module (Lemma 11.5.11), a is not a zero divisor of S. Suppose $a_0, \dots, a_{n-1}$ are elements of R and $(a_0 + a_1x + \cdots + a_{n-1}x^{n-1})x = 0$. Then $a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}a = 0$ implies $0 = a_0 = \cdots = a_{n-1}$. Therefore, x is not a zero divisor in S.

(2): Let $w = ax^{-1}$ and $v = xa^{-1}$, which are elements of $Q(S)$. If $n \geq e$, then $w^n = a^n(x^n)^{-1} = a^{n-e} \in S$. Therefore, w is integral over S. For contradiction's sake, assume $w \in S$. Then there are elements a_i of R such that $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = ax^{-1}$. Then $a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n = a$, which implies $0 = a_0 = \cdots = a_{n-2}$, and $a_{n-1}a^e = a$. This is a contradiction, since a is not a zero divisor and not invertible. If $n < e$, then a similar argument shows v is integral over S, and $v \notin S$. □

Now we derive sufficient conditions for a radical extension of a noetherian normal integral domain R to be a noetherian normal integral domain. Let a be a nonzero element of R and assume the divisor of a is

$$\operatorname{Div}(a) = n_1P_1 + \cdots + n_vP_v$$

(Definition 11.4.11). If $P_1, \dots, P_v$ are distinct height one primes in $X_1(R)$ and $n_1 = n_2 = \cdots = n_v = 1$, then we say that $\operatorname{Div}(a)$ is a *reduced effective divisor*.

LEMMA 11.5.13. *Let R be a DVR with maximal ideal $\mathfrak{m} = (\pi)$. Let $S = R[x]/(x^n - \pi)$, where $n \geq 2$. Then S is a DVR with maximal ideal $M = (x)$.*

PROOF. Since R is a UFD, so is $R[x]$. By Eisenstein's Criterion, $x^n - \pi$ is irreducible in $R[x]$. Therefore, S is an integral domain. By the Hilbert Basis Theorem (Theorem 6.2.1), S is noetherian. Since $S/(x) = R/(\pi)$ is a field, $M = (x)$ is a maximal ideal in S. By Theorem 6.3.6 (4) every maximal ideal of S contains π. Since $x^n = \pi$, this implies M is the unique maximal ideal, so S is a local ring. By Krull's Hauptidealsatz (Corollary 9.6.12 (2)), $\operatorname{ht}(M) = 1$. Therefore, $\dim(S) = 1$ and by Theorem 11.2.10, S is a DVR. □

THEOREM 11.5.14. *Let R be a noetherian normal integral domain with quotient field K. Let a be a nonzero element of R and assume* $\operatorname{Div}(a)$ *is a reduced effective divisor and $n \geq 2$ is invertible in R. If $S = R[x]/(x^n - a)$ and $L = K[x]/(x^n - a)$, then the following are true.*

(1) *L is a field.*
(2) *S is a noetherian integral domain.*
(3) *L is the quotient field of S.*
(4) *Let $Q \in \operatorname{Spec} S$, $P = Q \cap R$, and assume that $a \notin P$. Then R_P is regular if and only if S_Q is regular.*
(5) *S is a noetherian normal integral domain.*
(6) *S is the integral closure of R in L.*

PROOF. (1): By Section 11.4.1, for each $P \in X_1(R)$, R_P is a DVR with valuation ν_P. Let $\operatorname{Div}(a) = P_1 + \cdots + P_v$, where $P_1, \ldots, P_v$ are the distinct minimal primes of a in $X_1(R)$. For each i, $\nu_{P_i}(a) = 1$, so a is a local parameter for R_{P_i}. By Lemma 11.5.13, $x^n - a$ is irreducible in $R_{P_i}[x]$. By Gauss' Lemma (Lemma 6.1.10), $x^n - a$ is irreducible in $K[x]$, which implies L is a field.

(2): By Lemma 11.5.11, S is a free R-module of rank n and $1, x, \ldots, x^{n-1}$ is a basis. The natural mapping $S = S \otimes_R R \to S \otimes_R K = L$ is one-to-one since S is a flat R-module. Hence S is a subring of L and consequently an integral domain. By Theorem 6.2.1, S is noetherian.

(3): Let $Q(S)$ denote the quotient field of S. By Theorem 3.1.6, there is a homomorphism $Q(S) \to L$ which is onto since the natural mapping $S \to L$ is a localization of S.

(4): Since $a \notin P$, the image of a in $k(P)$ is invertible. By Lemma 11.5.11, $S \otimes_R R_P$ is separable over R_P. By Exercise 5.4.1, S_Q is separable over R_P. By Exercise 5.5.4, if $k(P)$ is the residue field of R_P, then $S_Q \otimes_R k(P)$ is a separable field extension of $k(P)$. By Theorem 11.5.4, R_P is regular if and only if S_Q is regular.

(5): We apply the Serre Criteria, Theorem 11.4.8. By Lemma 11.5.11 (5) it suffices to show S has property (R_1). Let $Q \in \operatorname{Spec} S$. Assume $\operatorname{ht}(Q) = 1$ and set $P = Q \cap R$. By Part (4) we can assume $a \in P$. By Lemma 11.5.11 (3), the prime ideals of S containing x correspond bijectively with the prime ideals of R containing a. Under this correspondence, a prime ideal $Q \in \operatorname{Spec} S$ corresponds to $P = Q \cap R$. A prime ideal $P \in \operatorname{Spec} R$ corresponds to $Q = PS + (x)$. The prime ideals of height one in R that contain a are $P_1, \ldots, P_v$. For $1 \le i \le v$, the height one prime of S lying over P_i is $Q_i = P_i S + (x)$. We have $S_{Q_i} = S \otimes_R R_{P_i} = R_{P_i}[x]/(x^n - 1)$. Since a is a local parameter for R_{P_i}, Lemma 11.5.13 shows that S_{Q_i} is a DVR with local parameter x. We have shown that S is regular in codimension one.

(6): S is integral over R and S is integrally closed in L. $\square$

For more results related to ramified radical extensions, see Corollaries 12.5.11 and 12.5.16, and Example 11.6.6.

6. Tests for Regularity

In this section, all rings are commutative. Suppose R is a local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. If R is noetherian and has Krull dimension $\dim(R) = d$, then R is regular if and only if $\mathfrak{m} = Rx_1 + \cdots + Rx_d$ for a regular system of parameters $x_1, \ldots, x_d$. By Exercise 9.6.2, R is a regular local ring if and only if $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$. In two important cases, we derive sets of necessary and sufficient conditions such that R is a regular local ring. In both cases, R is a localization of a finitely generated algebra over a field. The first criterion for regularity is based on the module of Kähler differentials, the second is in terms of the jacobian matrix associated to a set of generators and relations for R. A general reference for this section is [**28**, Sections I.5 and II.8].

6.1. A Differential Criterion for Regularity. As above, let R be a local ring with maximal ideal $\mathfrak{m}$. A *coefficient field* of R is a subfield k of R which is mapped onto $R/\mathfrak{m}$ under the natural map $R \to R/\mathfrak{m}$. In this case, R is a k-algebra, and $k \to R/\mathfrak{m}$ is a k-algebra isomorphism. The reader should verify that if k is a coefficient field of R, then every $x \in R$ has a unique representation in the form $x = y + z$, where $y \in k$ and $z \in \mathfrak{m}$.

PROPOSITION 11.6.1. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and assume R contains a coefficient field k. Then the k-linear map*

$$\mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\gamma} \Omega_{R/k} \otimes_R k$$

of Theorem 10.2.4 is an isomorphism.

PROOF. The cokernel of γ is $\Omega_{k/k}$ which is 0, so γ is onto. To show γ is one-to-one, it is enough to apply the exact functor $\operatorname{Hom}_k(\cdot, k)$ and show that

$$\operatorname{Hom}_k(\Omega_{R/k} \otimes_R k, k) \xrightarrow{\mathrm{H}_\gamma} \operatorname{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k)$$

is onto. As in the proof of Theorem 10.2.4, the map H_γ is isomorphic to

$$\operatorname{Der}_k(R, k) \xrightarrow{\rho} \operatorname{Hom}_R(\mathfrak{m}, k)$$

where ρ is defined by $\partial \mapsto \partial|_{\mathfrak{m}}$. It suffices to show ρ is onto. Let $h \in \operatorname{Hom}_R(\mathfrak{m}, k)$. Given $x \in R$, write $x = y + z$, where $y \in k$ and $z \in \mathfrak{m}$. This representation is unique. Define $\partial : R \to k$ by $\partial(x) = h(z)$. It is easy to see that ∂ is a well defined function that extends h, and $\partial(k) = 0$. The reader should verify that ∂ is a k-derivation on R. $\square$

THEOREM 11.6.2. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and assume R contains a coefficient field k which is a perfect field. Assume R is a localization of a finitely generated k-algebra. The following are equivalent.*

(1) R is regular.
(2) $\Omega_{R/k}$ is a free R-module of rank $d = \dim(R)$.

PROOF. By Theorem 6.2.1 and Corollary 4.1.13, R is noetherian. By Theorem 10.3.1 and Lemma 9.6.2, R is of finite Krull dimension.

(2) implies (1): By Proposition 11.6.1, $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$ and R is regular.

(1) implies (2): Assume $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$. By Proposition 11.6.1, it follows that $\dim_k(\Omega_{R/k} \otimes_R k) = d$. By Corollary 11.1.9, R is a normal integral domain. Let K be the quotient field of R. By Exercise 10.2.3, $\Omega_{R/k} \otimes_R K = \Omega_{K/k}$. By Theorem 10.3.9 and Theorem 10.3.6, $\dim_K(\Omega_{K/k}) = \operatorname{tr.deg}_k(K)$. By Noether's Normalization Lemma (Corollary 10.3.3), $d = \operatorname{tr.deg}_k(K)$. By Proposition 10.2.2 and Exercise 10.2.3, $\Omega_{R/k}$ is a finitely generated R-module. By Corollary 3.6.3, $\Omega_{R/k}$ is a free R-module of rank d. $\square$

COROLLARY 11.6.3. *Let k be an algebraically closed field and R an integral domain that is a finitely generated k-algebra. Let $n = \dim(R)$. The following are equivalent.*

(1) R is regular.
(2) $R_{\mathfrak{m}}$ is a regular local ring for every $\mathfrak{m} \in \operatorname{Max} R$.
(3) $\Omega_{R_{\mathfrak{m}}/k}$ is a free $R_{\mathfrak{m}}$-module of rank n for every $\mathfrak{m} \in \operatorname{Max} R$.
(4) $\Omega_{R/k}$ is a finitely generated projective R-module of rank n.

PROOF. By Theorem 6.2.1, R is noetherian. By Proposition 10.2.2, $\Omega_{R/k}$ is a finitely generated R-module. By Exercise 10.2.3, $\Omega_{R_{\mathfrak{m}}/k} = \Omega_{R/k} \otimes_R R_{\mathfrak{m}}$. (1) and (2) are equivalent by Exercise 11.3.14. (2) and (3) are equivalent by Theorem 11.6.2. (3) and (4) are equivalent, by Proposition 3.6.2. $\square$

COROLLARY 11.6.4. *Let k be an algebraically closed field and R an integral domain that is a finitely generated k-algebra. If*

$$\operatorname{Reg} R = \{\mathfrak{p} \in \operatorname{Spec} R \mid R_{\mathfrak{p}} \text{ is a regular local ring}\}$$

is the subset of $\operatorname{Spec} R$ *consisting of all prime ideals* $\mathfrak{p}$ *for which the local ring* $R_{\mathfrak{p}}$ *is regular, then*

(1) $\operatorname{Reg} R \cap \operatorname{Max} R \neq \emptyset$, *and*
(2) *for every* $\mathfrak{m} \in \operatorname{Reg} R \cap \operatorname{Max} R$, *there exists an open dense* $U \subseteq \operatorname{Spec} R$ *such that* $\mathfrak{m} \in U \subseteq \operatorname{Reg} R$.

PROOF. Let K be the quotient field of R. By Theorem 10.3.9, K is separably generated over k. By Corollary 10.3.3, if $n = \dim R$, then $n = \operatorname{tr.deg}_k(K)$. By Theorem 10.3.6, $\dim_K \Omega_{K/k} = n$. By Exercise 10.2.3, $\Omega_{K/k} = \Omega_{R/k} \otimes_R K$. By Proposition 10.2.2, $\Omega_{R/k}$ is a finitely generated R-module and by Lemma 3.1.14, there exists $\alpha \in R - (0)$ such that $\Omega_{R/k} \otimes_R R_\alpha$ is a free R_α-module. By Corollary 11.6.3, R_α is regular and the basic open set $U(\alpha)$ is a subset of $\operatorname{Reg} R$. It follows from Hilbert's Nullstellensatz that the Jacobson radical of R is (0) (see Corollary 6.2.16). Consequently, there exists $\mathfrak{m} \in \operatorname{Max} R$ such that α is not in $\mathfrak{m}$. Thus $\mathfrak{m} \in U(\alpha) \cap \operatorname{Max} R$, which proves (1).

To prove (2), let $\mathfrak{m}$ be a maximal ideal of R and assume $R_{\mathfrak{m}}$ is a regular local ring. Then $\Omega_{R_{\mathfrak{m}}/k} = \Omega_{R/k} \otimes_R R_{\mathfrak{m}}$ is free of rank n, by Theorem 11.6.2. By Lemma 3.1.14, there exists $\beta \in R - \mathfrak{m}$ such that $\Omega_{R/k} \otimes_R R_\beta$ is a free R_β-module. By Corollary 11.6.3, R_β is regular and the basic open set $U(\beta)$ is a subset of $\operatorname{Reg} R$. The open set $U(\beta)$ is dense in $\operatorname{Spec} R$ since it contains the generic point (0). $\square$

6.2. A Jacobian Criterion for Regularity. Throughout this section, k is an algebraically closed field, and all rings are commutative. From a utilitarian point of view, the jacobian criterion of Theorem 11.6.5 is one of the most useful and powerful methods for showing that a finitely generated k-algebra R is regular.

First we review some terminology and notation from Section 6.2.2. Affine n-space over k is denoted $\mathbb{A}_k^n$ and is equal to the set $\{(a_1, \dots, a_n) \mid a_i \in k\}$. For any subset $Y \subseteq \mathbb{A}_k^n$, the ideal of Y in $A = k[x_1, \dots, x_n]$ is defined by

$$I(Y) = \{f \in A \mid f(P) = 0, \text{ for all } P \in Y\}.$$

If $T \subseteq A$ is a set of polynomials, then the set of zeros of T

$$Z(T) = \{P \in \mathbb{A}_k^n \mid f(P) = 0, \text{ for all } f \in T\}$$

is an affine algebraic set. By Hilbert's Nullstellensatz (Corollary 6.2.11), there is a one-to-one correspondence between the algebraic sets in $\mathbb{A}_k^n$ and the radical ideals in A defined by the assignments $Y \mapsto I(Y)$ and $I \mapsto Z(I)$.

If $Y \subseteq \mathbb{A}_k^n$ is a affine algebraic set, then the *affine coordinate ring* of Y is $\mathscr{O}(Y) = A/I(Y)$. Now assume I is a radical ideal in A, and $Y = Z(I)$ is the associated affine algebraic set. Then $I = I(Y)$ and $\mathscr{O}(Y) = A/I$. By Hilbert's Nullstellensatz (see Example 6.2.15), the maximal ideals in $\mathscr{O}(Y) = A/I$ are in one-to-one correspondence with the points $P \in Y$. A point $P = (a_1, \dots, a_n) \in Y$, corresponds to the maximal ideal $\mathfrak{m}$ in $\mathscr{O}(Y)$ generated by $x_1 - a_1, \dots, x_n - a_n$. The localization of $\mathscr{O}(Y)$ at the maximal ideal $\mathfrak{m}$ is called the *local ring* at P on Y and is denoted $\mathscr{O}_{P,Y}$. Theorem 11.6.5 is a jacobian criterion for $\mathscr{O}_{P,Y}$ to be a regular local ring.

THEOREM 11.6.5. *Let k be an algebraically closed field, $Y \subseteq \mathbb{A}_k^n$ an affine algebraic set and $f_1, \dots, f_t$ a set of generators for $I(Y)$. Let $P \in Y$ and assume the Krull dimension* *of the local ring $\mathscr{O}_{P,Y}$ is r. Then the jacobian matrix*

$$J = \left(\frac{\partial f_i}{\partial x_j}(P) \right)$$

has rank $n-r$ if and only if $\mathscr{O}_{P,Y}$ is a regular local ring.

PROOF. Let $A = k[x_1,\dots,x_n]$, $I = I(Y) = (f_1,\dots,f_t)$, and $R = \mathscr{O}(Y) = A/I$. Let $\mathfrak{p}$ denote the maximal ideal of R corresponding to the point $P \in Y$. Then $\mathscr{O}_{P,Y} = R_{\mathfrak{p}}$. Let $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$ be the maximal ideal of $R_{\mathfrak{p}}$. Since k is algebraically closed, the residue field $R_{\mathfrak{p}}/\mathfrak{m}$ is equal to k. Start with the exact sequence

$$I/I^2 \xrightarrow{\gamma} \Omega_{A/k} \otimes_A R \xrightarrow{a} \Omega_{R/k} \to 0$$

of Theorem 10.2.4. Tensoring with the residue field, $(\,) \otimes_R k$, the sequence

$$I/I^2 \otimes_R k \xrightarrow{\gamma} \Omega_{A/k} \otimes_A k \xrightarrow{a} \Omega_{R_{\mathfrak{p}}/k} \otimes_{R_{\mathfrak{p}}} k \to 0$$

is exact. As in the proof of Proposition 10.2.7, the image of γ is the column space of the jacobian matrix J and $\Omega_{A/k} \otimes_A k \cong k^{(n)}$. From the exact sequence, the dimension of $\Omega_{R/k} \otimes_R k$ over k is equal to $n - \operatorname{Rank}(J)$. By Proposition 11.6.1, $\mathfrak{m}/\mathfrak{m}^2 \cong \Omega_{R_{\mathfrak{p}}/k} \otimes_{R_{\mathfrak{p}}} k$. Therefore, $R_{\mathfrak{p}}$ is a regular local ring if and only if $\operatorname{Rank}(J) = n - r$. □

EXAMPLE 11.6.6. In the above context, let $F = Z(f)$ be an algebraic set in $\mathbb{A}^n_k$ defined by a square free polynomial f in $A = k[x_1,\dots,x_n]$. Using Corollaries 9.6.12 and 10.3.4 we see that $\dim(\mathscr{O}(F)) = n-1$. Let $d \geq 2$ be an integer that is invertible in k. Consider the algebraic set $Y = Z(z^d - f)$ in $\mathbb{A}^{n+1}_k$. The affine coordinate ring of Y, $\mathscr{O}(Y) = A[z]/(z^d - f)$, is a ramified radical extension of A. We are in the context of Theorem 11.5.14. Then Y is irreducible, $\mathscr{O}(Y)$ is a normal integral domain, the quotient field of $\mathscr{O}(Y)$ is a finite algebraic extension of $k(x_1,\dots,x_n)$, and the Krull dimension of $\mathscr{O}(Y)$ is equal to n. If $\pi : \mathbb{A}^{n+1}_k \to \mathbb{A}^n_k$ is the projection along the z-axis defined by $(a_1,\dots,a_n,b) \mapsto (a_1,\dots,a_n)$, then $\pi^{-1}(F)$ is the algebraic subset of Y equal to $Y \cap Z(z)$. Let $\operatorname{Sing}(Y)$ denote the set of points in Y where the local ring $\mathscr{O}_{P,Y}$ is not a regular local ring. The set $\operatorname{Sing}(Y)$ is called the *singular locus* of Y. For any point $Q \in Y$ such that $\pi(Q)$ is not in F, it follows from Theorem 11.5.14 (4) that $\mathscr{O}_{Q,Y}$ is a regular local ring. This implies $\operatorname{Sing}(Y) \subseteq \pi^{-1}(F)$. Applying Theorem 11.6.5, we can say more. The jacobian of $z^d - f$ is $\left(f_{x_1},\dots,f_{x_n}, dz^{d-1}\right)$. From Theorem 11.6.5, we see at once that $P \in \operatorname{Sing}(Y)$ if and only if $P = (a_1,\dots,a_n,0)$ and $\pi(P) = (a_1,\dots,a_n)$ is in $\operatorname{Sing}(F)$. In other words, the singular locus of Y corresponds under π to the singular locus of F. By Exercise 11.3.14, $\mathscr{O}(Y)$ is a regular integral domain if and only if $\mathscr{O}(F)$ is a regular ring.

EXAMPLE 11.6.7. Although the field in Theorem 11.6.5 is required to be algebraically closed, it is sometimes possible to work around this obstacle. In this paragraph, one such method is presented. Let k be a field and in this example do not assume k is algebraically closed. Let $\bar{k}$ be an algebraic closure of k. Let I be an ideal in $k[x_1,\dots,x_n]$ and $T = k[x_1,\dots,x_n]/I$. If $\bar{T} = T \otimes_k \bar{k}$, then the natural map $T \to \bar{T}$ is faithfully flat (Exercise 3.5.3). By Exercise 11.3.13, if $\bar{T}$ is regular, then T is regular. By Exercise 6.1.4 (2), if $\bar{T}$ is an integrally closed integral domain, then T is an integrally closed integral domain. By Exercise 6.1.4 (3), if $\bar{T}$ is a normal ring, then T is a normal ring.

COROLLARY 11.6.8. *Let k be an algebraically closed field and Y an irreducible algebraic subset of $\mathbb{A}^n_k$. Then the singular locus of Y,* $\operatorname{Sing}(Y)$*, is a proper closed subset of Y.*

PROOF. As in Example 11.6.6, $\operatorname{Sing}(Y)$ consists of those points P in Y such that $\mathscr{O}_{P,Y}$ is not a regular local ring. There is a one-to-one correspondence between the points P in Y and the maximal ideals $\mathfrak{m}$ in $\operatorname{Max}\mathscr{O}(Y)$ (Example 6.2.15). The finitely generated k-algebra $\mathscr{O}(Y)$ is an integral domain since Y is irreducible. Therefore, this follows from Corollary 11.6.4. $\square$

CHAPTER 12

Divisor Class Groups

This subject of this chapter is ideal theory, in the classical sense. Let R be an integral domain with field of fractions K and V a finite dimensional K-vector space. Throughout this chapter, for sake of completeness and also for brevity, we will frequently assume the ring R is noetherian or integrally closed, or both. The chapter begins with a section on R-lattices. An R-lattice is an R-submodule M of V such that M contains a generating set for V as a K-vector space, and M is a submodule of a finitely generated R-submodule of V. When $\dim_K(V) = 1$, we assume $V = K$. In this case, an R-lattice is called a fractional ideal of R in K. Since any nonzero ideal I of R is a fractional ideal of R in K, this generalizes the usual notion of ideal. In Definition 3.6.6 we defined $\operatorname{Pic}(R)$, the Picard group of R. In Section 12.2 we construct the Picard group in terms of fractional ideals of R in K that are projective R-modules. Dedekind domains are the subject of Section 12.3. These are noetherian integrally closed integral domains with Krull dimension one. We show that for a Dedekind domain R, the set of all fractional ideals is an abelian group under multiplication. In Definition 11.4.11, we defined $\operatorname{Cl}(R)$, the class group of a noetherian integrally closed integral domain R, in terms of Weil divisors. In Section 12.4, we construct the class group in terms of those fractional ideals of R that are reflexive R-modules. In Section 12.5 some important functorial properties of the class group are derived. Section 12.6 contains some fundamental results on lattices over noetherian regular integral domains. For instance, we show that for such a ring R, the groups $\operatorname{Pic}(R)$ and $\operatorname{Cl}(R)$ are equal. There is a short section, Section 12.7, on the class group of a graded noetherian integrally closed integral domain. As an application of the results in the previous sections, Section 12.8 contains an introduction to classical Algebraic Number Theory. If R is the ring of integers in a global field, we prove that the class group of R is finite. We also prove the first half of the Dirichlet Units Theorem which says that if R is the integral closure of $\mathbb{Z}$ in a finite algebraic extension of $\mathbb{Q}$, then the group of units in R is a finitely generated abelian group.

1. Lattices

Let R be an integral domain with field of fractions K. If V is a finite dimensional K-vector space, and M is an R-submodule of V, then the K-subspace of V spanned by M is denoted KM. Notice that KM is finite dimensional over K, but M is not necessarily finitely generated as an R-module. If M is any finitely generated torsion free R-module, the natural mapping $R \otimes_R M \to K \otimes_R M$ is one-to-one (Lemma 3.1.4). In this case we can identify M with the R-submodule $1 \otimes M$ of $K \otimes_R M$. In this case, we write KM instead of $K \otimes_R M$. The primary sources for the material in this section are [**21**] and [**12**].

1.1. Definition and First Properties. Let R be an integral domain with field of fractions K and V a finite dimensional K-vector space. The definition of an R-lattice in V follows Proposition 12.1.1. If M is an R-submodule of V, then the proposition establishes five equivalent conditions, any one of which can be taken as the definition for an R-lattice in V. Of the five, the one with a particularly straightforward interpretation is Property (1). It states that to be an R-lattice it is necessary and sufficient that M has two key properties. The first is that M contains a spanning set for V as a K-vector space and the second is that M is either finitely generated as an R-module, or is contained in a finitely generated R-submodule of V.

PROPOSITION 12.1.1. *Let R be an integral domain with field of fractions K and V a finite dimensional K-vector space. The following are equivalent for an R-submodule M of V.*

1. *There is a finitely generated R-submodule N of V such that $M \subseteq N$, and $KM = V$, where KM denotes the K-subspace of V spanned by M.*
2. *There is a free R-submodule F in V with $\operatorname{Rank}_R(F) = \dim_K(V)$ and a nonzero element $r \in R$ such that $rF \subseteq M \subseteq F$.*
3. *There are free R-submodules F_1, F_2 in V with $F_1 \subseteq M \subseteq F_2$ and $\operatorname{Rank}_R(F_1) = \operatorname{Rank}_R(F_2) = \dim_K(V)$.*
4. *There is a chain of R-submodules $L \subseteq M \subseteq N$ where $KL = V$ and N is finitely generated.*
5. *Given any free R-submodule F of V with $\operatorname{Rank}_R(F) = \dim_K(V)$, there are nonzero elements $r, s \in R$ such that $rF \subseteq M \subseteq s^{-1}F$.*

PROOF. Assume $\dim_K(V) = n$. We prove that (4) implies (5). The rest is left to the reader. Assume we are given $F = Ru_1 \oplus \cdots \oplus Ru_n$ a free R-submodule of V. Also, let $L \subseteq M \subseteq N$, where $KL = V$ and N is a finitely generated R-submodule of V. Since $KL = V$ we can pick a K-basis for V in L, say $\{\lambda_1, \dots, \lambda_n\}$ (Theorem 1.6.13). For each j there are $k_{j,i} \in K$ such that $u_j = \sum_{i=1}^n k_{j,i}\lambda_i$. Pick a nonzero $r \in R$ such that $rk_{j,i} \in R$ for all pairs j,i. Then $ru_j = \sum_{i=1}^n rk_{j,i}\lambda_i \in \sum_i R\lambda_i \subseteq L$, hence $rF = \sum_j Rru_j \subseteq L \subseteq M$. Let $v_1, \dots, v_t$ be a generating set for N. For each j there are $\kappa_{j,i} \in K$ such that $v_j = \sum_{i=1}^n \kappa_{j,i}u_i$. Pick a nonzero $s \in R$ such that $s\kappa_{j,i} \in R$ for all pairs j,i. Then $sv_j = \sum_{i=1}^n s\kappa_{j,i}u_i \in \sum_{i=1}^n Ru_i = F$. Therefore, $M \subseteq N = \sum_{j=1}^t Rv_j \subseteq s^{-1}F$. □

DEFINITION 12.1.2. Let R be an integral domain, K the field of fractions of R, and V a finite dimensional K-vector space. An R-submodule M of V that satisfies any of the equivalent conditions of Proposition 12.1.1 is said to be an *R-lattice in V*. The *rank* of an R-lattice M in V is defined to be $\dim_K V$.

EXAMPLE 12.1.3. Let R be an integral domain with field of fractions K.

1. If M is a finitely generated R-module, then the image of $M \to K \otimes_R M$ is a finitely generated R-lattice.
2. Let R be a noetherian integral domain and M and N finitely generated R-modules such that N is torsion free. Then $\operatorname{Hom}_R(M,N)$ is a finitely generated torsion free R-module (Exercises 4.1.8 and 9.2.15). By Proposition 3.5.8, $\operatorname{Hom}_R(M,N)$ embeds as an R-lattice in $K \otimes_R \operatorname{Hom}_R(M,N) = \operatorname{Hom}_K(K \otimes_R M, KN)$. This is a special case of Proposition 12.1.6 (3).
3. Assume R is integrally closed in K, L/K is a finite separable field extension, and S is the integral closure of R in L. By Theorem 6.1.13, S is an R-lattice in L.

PROPOSITION 12.1.4. *Let R be an integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V.*

1. *If R is noetherian, then M is a finitely presented R-module.*
2. *If R is a principal ideal domain, then M is a finitely generated free R-module and $\operatorname{Rank}_R(M) = \dim_K(V)$.*

PROOF. (1): Apply Proposition 12.1.1 and Corollary 4.1.12.

(2): Apply (1) and Theorem 1.7.14. By Theorem 2.3.23, an R-basis for M is also a K-basis for V, so the rank of M is equal to the dimension of V. $\square$

PROPOSITION 12.1.5. *Let R be an integral domain and K the field of fractions of R. In the following, U, V, $V_1,\dots,V_r$, W denote finite dimensional K-vector spaces.*

(1) If M and N are R-lattices in V, then $M+N$ and $M\cap N$ are R-lattices in V.
(2) If U is a K-subspace of V, and M is an R-lattice in V, then $M\cap U$ is an R-lattice in U.
(3) Let $M_1,\dots,M_m$ be R-lattices in $V_1,\dots,V_m$ respectively. If $\phi : V_1\times\cdots\times V_m \to U$ is a multilinear form, then the R-module generated by $\phi(M_1\times\cdots\times M_m)$ is an R-lattice in the subspace spanned by $\phi(V_1\times\cdots\times V_m)$.
(4) Let L/K be an extension of fields. Let S be an R-subalgebra of L such that L is the field of fractions of S. If M is an R-lattice in V, then the image of $S\otimes_R M \to L\otimes_K V$ is an S-lattice in $L\otimes_K V$.

PROOF. (1): We apply Proposition 12.1.1 (5). Let F be a free R-submodule of V with rank $n=\dim_K(V)$. There exist nonzero elements a,b,c,d in R such that $aF\subseteq M$, $bF\subseteq N$, $M\subseteq c^{-1}F$, $N\subseteq d^{-1}F$. Then $(ab)F\subseteq M\cap N\subseteq M+N\subseteq (cd)^{-1}F$.

(2): Start with a K-basis, say $u_1,\dots,u_m$, for U. Extend to a K-basis $u_1,\dots,u_m,\dots,u_r$ for V. Let $E=Ru_1\oplus\cdots\oplus Ru_m$ and $F=Ru_1\oplus\cdots\oplus Ru_n$. Then $E=F\cap U$. Also, for any $\alpha\in K$, $(\alpha F)\cap U=(\sum_{i=1}^n R\alpha u_i)\cap U=\sum_{i=1}^m R\alpha u_i=\alpha E$. We apply Proposition 12.1.1 (5). Let r,s be nonzero elements in R such that $rF\subseteq M\subseteq s^{-1}F$. Then $rE\subseteq M\cap U\subseteq s^{-1}E$.

(3): For each j, M_j contains a K-spanning set for V_j. From this is follows that $\phi(M_1\times\cdots\times M_m)$ contains a spanning set for the subspace of U spanned by $\phi(V_1\times\cdots\times V_m)$. For each j, let N_j be a finitely generated R-submodule of V_j containing M_j. Then $\phi(N_1\times\cdots\times N_m)$ is contained in a finitely generated R-submodule of U.

(4): Since $K\otimes_R M=K\otimes_R V=V$, we have $L\otimes_S S\otimes_R M=L\otimes_K K\otimes_R M=L\otimes_K V$. If $M\subseteq N\subseteq V$ with N a finitely generated R-module, then the diagram of S-module homomorphisms

$$\begin{tikzcd} S\otimes_R M \arrow[rr] \arrow[dr] & & L\otimes_K V \\ & S\otimes_R N \arrow[ur] & \end{tikzcd}$$

commutes. Therefore, the image of $S\otimes_R M$ in $L\otimes_K V$ is contained in the image of $S\otimes_R N$ which is a finitely generated S-module. $\square$

PROPOSITION 12.1.6. *Let R be an integral domain and K the field of fractions of R. Let V and W be finite dimensional K-vector spaces. In the following, M_0,M_1,M denote R-lattices in V and N_0,N_1,N denote R-lattices in W. Using the module quotient notation, $N:M$ is defined to be*

$$N:M=\{f\in \operatorname{Hom}_K(V,W)\mid f(M)\subseteq N\}.$$

Then

(1) If $M_0\subseteq M_1$, and $N_0\subseteq N_1$, then $N_0:M_1\subseteq N_1:M_0$.
(2) The restriction mapping $\rho:(N:M)\to \operatorname{Hom}_R(M,N)$ is an isomorphism of R-modules.
(3) $N:M$ is an R-lattice in $\operatorname{Hom}_K(V,W)$.

(4) *Let $Z \subseteq R - \{0\}$ be a multiplicative set and $Z^{-1}R$ the localization of R in K. Then $Z^{-1}(N : M) = Z^{-1}N : Z^{-1}M$.*

PROOF. (1): Is left to the reader.

(2): The reader should verify that restriction defines an R-module homomorphism $\rho : (N : M) \to \operatorname{Hom}_R(M,N)$. Because M contains a K-basis for V, ρ is one-to-one. Because M and N are torsion free R-modules, the maps $M \to K \otimes_R M = KM$ and $N \to K \otimes_R N = KN$ are one-to-one. If $\theta \in \operatorname{Hom}_R(M,N)$, then the diagram

$$\begin{tikzcd} M \arrow[r, "\theta"] \arrow[d] & N \arrow[d] \\ K \otimes_R M = V \arrow[r, "1\otimes\theta"] & K \otimes_R N = W \end{tikzcd}$$

commutes. Therefore, $1 \otimes \theta : V \to W$ is an extension of θ and belongs to $N : M$. In other words, θ is in the image of ρ.

(3): Let $E_0 \subseteq M \subseteq E_1$ be R-lattices in V with E_0 and E_1 free. Let $F_0 \subseteq N \subseteq F_1$ be R-lattices in W with F_0 and F_1 free. By (1), $F_0 : E_1 \subseteq N : M \subseteq F_1 : E_0$. By Proposition 12.1.1 (4), it suffices to prove (4) when M and N are free R-lattices. In this case, $\operatorname{Hom}_R(M,N)$ is free over R and $\operatorname{Hom}_R(M,N) \to K \otimes_R \operatorname{Hom}_R(M,N)$ is one-to-one. By Corollary 2.4.13, the assignment $\theta \mapsto 1 \otimes \theta$ embeds $\operatorname{Hom}_R(M,N)$ as an R-submodule of $\operatorname{Hom}_K(KM,KN) = \operatorname{Hom}_K(V,W)$. By (2), the image of $\operatorname{Hom}_R(M,N)$ under this embedding is equal to $N : M$. This proves $N : M$ is an R-lattice in $\operatorname{Hom}_K(V,W)$, when M and N are free R-lattices.

(4): If $f \in (N : M)$ and $z \in Z$, then $f(z^{-1}x) = z^{-1}f(x) \in z^{-1}N$ for all $x \in M$. Conversely, suppose $f \in Z^{-1}N : Z^{-1}M$. Let $y_1, \dots, y_n$ be a generating set for M. There exists $z \in Z$ such that $f(x_i) \in z^{-1}N$ for $1 \le i \le n$. Therefore, $zf \in N : M$. $\square$

1.2. Reflexive Lattices. Most of the material in this section appears in [**18**, Section 6.3.2]. In the context of Proposition 12.1.6, we identify $R : M$ with the dual module $M^* = \operatorname{Hom}_R(M,R)$. By Exercise 2.4.5 the assignment $m \mapsto \varphi_m$ is an R-module homomorphism $M \to M^{**} = R : (R : M)$, where φ_m is the "evaluation at m" homomorphism. That is, $\varphi_m(f) = f(m)$. The diagram

$$\begin{tikzcd} M \arrow[r] \arrow[d] & M^{**} = R : (R : M) \arrow[d] \\ V \arrow[r] & V^{**} \end{tikzcd} \tag{1.1}$$

commutes and the bottom horizontal arrow is an isomorphism (Exercise 2.4.6). Since the vertical maps are one-to-one, the top horizontal arrow is one-to-one. We say M is a *reflexive R-lattice* in case $M \to R : (R : M)$ is onto. For instance, a finitely generated projective R-lattice is reflexive (Exercise 2.4.6). If M is an R-lattice, then Lemma 12.1.7 shows that $R : M$, the dual of M, is reflexive.

LEMMA 12.1.7. *Let R be an integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V. Then $R : M = R : (R : (R : M))$, or equivalently, $R : M$ is a reflexive R-lattice in V^*.*

PROOF. By Proposition 12.1.6 (1) applied to $M \subseteq R : (R : M)$, we get the set inclusion $R : M \supseteq R : (R : (R : M))$. The reverse inclusion follows from the commutative diagram (1.1). $\square$

PROPOSITION 12.1.8. *Let R be an integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V. Let $M \subseteq F \subseteq V$, where F is a free R-lattice (Proposition 12.1.1). Then M is a reflexive R-lattice if and only if*

$$M = \bigcap_{\alpha \in (R:M)} \left(\alpha^{-1}(R) \cap F\right).$$

PROOF. It suffices to prove

$$R:(R:M) = \bigcap_{\alpha \in (R:M)} \left(\alpha^{-1}(R) \cap F\right). \tag{1.2}$$

Let $v \in V$ and assume v is in the right hand side of (1.2). Then $v \in R:(R:M)$ if and only if $\alpha(v) \in R$, for all $\alpha \in R:M$. Notice that if $\alpha \in R:M$, then $\alpha \in R:(\alpha^{-1}(R) \cap F)$. Therefore, $\alpha(v) \in R$, which shows $v \in R:(R:M)$.

For the reverse inclusion, let $\alpha \in R:M$. Then $\alpha(M) \subseteq R$, hence $M \subseteq \alpha^{-1}(R) \cap F \subseteq F$. By Proposition 12.1.1 (4), this implies $\alpha^{-1}(R) \cap F$ is an R-lattice in V. Let $v \in R:(R:(\alpha^{-1}(R) \cap F))$. Under the identification $V = V^{**}$, we identify v with a vector in V. As mentioned above, $\alpha \in R:(\alpha^{-1}(R) \cap F)$, $\alpha(v) \in R$, hence $v \in \alpha^{-1}(R)$. Since F is free, F is reflexive (Exercise 2.4.6) and we see that $R:(R:(\alpha^{-1}(R) \cap F)) \subseteq R:(R:F) = F$. Combined, this shows $R:(R:(\alpha^{-1}(R) \cap F)) \subseteq \alpha^{-1}(R) \cap F$. That is, $\alpha^{-1}(R) \cap F$ is reflexive. This shows $R:(R:M) \subseteq \alpha^{-1}(R) \cap F$ for each α. In (1.2), the left hand side is a subset of the right hand side. $\square$

Let R be an integral domain with field of fractions K. Let U, V, W be finite dimensional K-vector spaces. Let

$$\operatorname{Hom}_K(V,W) \otimes_K U \xrightarrow{\alpha} \operatorname{Hom}_K(\operatorname{Hom}_K(U,V),W)$$

be the isomorphism of Lemma 2.4.11 which is defined by $\alpha(f \otimes a)(h) = f(h(a))$. Let

$$\operatorname{Hom}_K(U \otimes_K V, W) \xrightarrow{\phi} \operatorname{Hom}_K(U, \operatorname{Hom}_K(V,W))$$

be the Adjoint Isomorphism (Theorem 2.4.10) which is defined by $\phi(\theta)(u) = \theta(u \otimes \cdot)$.

LEMMA 12.1.9. *In the above context, let L, M, N be R-lattices in U, V, W respectively.*

(1) Let $(N:M)L$ denote the image of $(N:M) \otimes_R L \to \operatorname{Hom}_K(V,W) \otimes_K U$. Then $\alpha\left((N:M)L\right) \subseteq N:(M:L)$.
(2) Let LM denote the image of $L \otimes_R M \to U \otimes_K V$. Then $\phi\left(N:LM\right) \subseteq (N:M):L$, and $\phi^{-1}\left((N:M):L\right) \subseteq N:LM$.

PROOF. (1): Let $f \in N:M$, $\ell \in L$, $h \in M:L$. Then $\alpha(f \otimes \ell)(h) = f(h(\ell)) \in N$.

(2): Assume $\theta \in \operatorname{Hom}_K(U \otimes_K V, W)$ and $\theta(LM) \subseteq N$. For all $m \in M$ and $\ell \in L$, $\phi(\theta)(\ell)(m) = \theta(\ell \otimes m) \in N$. Therefore, $\phi(\theta)(L) \subseteq N:M$, hence $\phi(\theta) \in (N:M):L$. For the second part, suppose $\phi(\theta)(\ell) \in N:M$ for all $\ell \in L$. Then $\phi(\theta)(\ell)(m) = \theta(\ell \otimes m) \in N$, and $\theta \in N:LM$. $\square$

PROPOSITION 12.1.10. *Let R be an integral domain with field of fractions K. Let N be an R-lattice in the finite dimensional K-vector space W. Let M be a reflexive R-lattice in the finite dimensional K-vector space V. Then $M:N$ is a reflexive R-lattice in* $\operatorname{Hom}_K(W,V)$.

PROOF. In this context,

$$\operatorname{Hom}_K(W,V) \xrightarrow{\alpha^*} \operatorname{Hom}_K(W \otimes_K V^*, K) \xrightarrow{\phi} \operatorname{Hom}_K(W,V)$$

is the identity map. Under this identification, ϕ is the inverse of the dual of α. By Lemma 12.1.9 (2),

$$\phi(R:(R:M)N) \subseteq (R:(R:M)):N = M:N$$

where the last equality is because M is reflexive. By Lemma 12.1.9 (1),

$$\alpha((R:M)N) \subseteq R:(M:N)$$

taking duals,

$$R:(R:(M:N)) \subseteq R:\alpha((R:M)N).$$

By the identification mentioned above, $R:(R:(M:N)) \subseteq M:N$. □

THEOREM 12.1.11. *Let R be a noetherian integrally closed integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V.*

(1) If L is another R-lattice in V, then $L_{\mathfrak{p}} = M_{\mathfrak{p}}$ for all but finitely many $\mathfrak{p} \in X_1(R)$.

(2) Suppose for each $\mathfrak{p} \in X_1(R)$ that $N(\mathfrak{p})$ is an $R_{\mathfrak{p}}$-lattice in V such that $N(\mathfrak{p}) = M_{\mathfrak{p}}$ for all but finitely many $\mathfrak{p} \in X_1(R)$. For $N = \bigcap_{\mathfrak{p}\in X_1(R)} N(\mathfrak{p})$, the following are true.

(a) N is an R-lattice in V.

(b) $N_{\mathfrak{p}} = N(\mathfrak{p})$ for all $\mathfrak{p} \in X_1(R)$.

(c) If N' is an R-lattice in V such that $N'_{\mathfrak{p}} = N(\mathfrak{p})$ for all $\mathfrak{p} \in X_1(R)$, then $N' \subseteq N$.

PROOF. (1): Using Proposition 12.1.1, the reader should verify that there exist $r, s \in R$ such that $rM \subseteq L \subseteq s^{-1}M$. Let $\mathfrak{p} \in X_1(R)$ such that $\nu_{\mathfrak{p}}(r) = \nu_{\mathfrak{p}}(s) = 0$. Then $rM \otimes_R R_{\mathfrak{p}} = s^{-1}M \otimes_R R_{\mathfrak{p}}$. By Corollary 11.4.4, this proves (1).

(2): For each $\mathfrak{p} \in X_1(R)$, $R_{\mathfrak{p}}$ is a discrete valuation ring. By Proposition 12.1.4, $N(\mathfrak{p})$ is a finitely generated free $R_{\mathfrak{p}}$-module.

(a): Let F be a free R-lattice in V. By (1), $M_{\mathfrak{p}} = F_{\mathfrak{p}}$ for all but finitely many $\mathfrak{p} \in X_1(R)$. Assume $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ are those height one primes in $X_1(R)$ where $F_{\mathfrak{q}_j} \neq N(\mathfrak{q}_j)$. Let $u_1, \dots, u_n$ be a free R-basis for F. Let $\{v_{j,1}, \dots, v_{j,n}\}$ be a free $R_{\mathfrak{q}_j}$-basis for $N(\mathfrak{q}_j)$. There are elements $\kappa_{k,j,i}$ in K such that $u_k = \sum_{i=1}^n \kappa_{k,j,i} v_{j,i}$. For some $r \in R-(0)$, $ru_k \in \sum_{i=1}^n R v_{j,i} \subseteq N(\mathfrak{q}_j)$ for all k, j. For $1 \le j \le t$ this implies $rF \subseteq N(\mathfrak{q}_j)$. Also, if $F_{\mathfrak{p}} = N(\mathfrak{p})$, then $rF \subseteq rF_{\mathfrak{p}} = rN(\mathfrak{p}) \subseteq N(\mathfrak{p})$. Therefore, $rF \subseteq N = \bigcap_{\mathfrak{p}\in X_1(R)} N(\mathfrak{p})$.

There are elements $\lambda_{k,j,i}$ in K such that $v_{j,i} = \sum_{k=1}^n \lambda_{k,j,i} u_k$. For some $s \in R-(0)$, $sv_{j,i} \in \sum_{k=1}^n Ru_k = F$ for all j, i. This implies $sN(\mathfrak{q}_j) \subseteq F_{\mathfrak{q}_j}$, hence $N(\mathfrak{q}_j) \subseteq (s^{-1}F)_{\mathfrak{q}_j}$ for all j. Also, if $N(\mathfrak{p}) = F_{\mathfrak{p}}$, then $sN(\mathfrak{p}) \subseteq N(\mathfrak{p}) = F_{\mathfrak{p}}$, hence $N(\mathfrak{p}) \subseteq (s^{-1}F)_{\mathfrak{p}}$. If necessary, replace F with $s^{-1}F$, and assume $N(\mathfrak{p}) \subseteq F_{\mathfrak{p}}$ for all $\mathfrak{p} \in X_1(R)$. By taking direct sums in Corollary 11.4.4 (4) we see that $F = \bigcap_{\mathfrak{p}\in X_1(R)} F_{\mathfrak{p}}$. Then $N = \bigcap_{\mathfrak{p}\in X_1(R)} N(\mathfrak{p}) \subseteq F$. By Proposition 12.1.1, N is an R-lattice in V.

(b): By the last part of the proof of Part (a), $N(\mathfrak{p}) \subseteq F_{\mathfrak{p}}$ for all $\mathfrak{p} \in X_1(R)$ with equality for all but finitely many $\mathfrak{p} \in X_1(R)$. Assume $\mathfrak{p}_1, \dots, \mathfrak{p}_w$ are those height one primes in $X_1(R)$ where $F_{\mathfrak{p}_i} \neq N(\mathfrak{p}_i)$. (Note: we do not assume this list is equal to $\mathfrak{q}_1, \dots, \mathfrak{q}_t$.) Then

$$\begin{aligned} N &= \bigcap_{\mathfrak{p}\in X_1(R)} N(\mathfrak{p}) \\ &= N(\mathfrak{p}_1) \cap \cdots \cap N(\mathfrak{p}_w) \cap \left(\bigcap_{\mathfrak{p}\in X_1(R)} F_{\mathfrak{p}} \right) \\ &= N(\mathfrak{p}_1) \cap \cdots \cap N(\mathfrak{p}_w) \cap F. \end{aligned}$$

It follows from the definition of localization that

$$N_{\mathfrak{p}} = N(\mathfrak{p}_1)_{\mathfrak{p}} \cap \cdots \cap N(\mathfrak{p}_w)_{\mathfrak{p}} \cap F_{\mathfrak{p}}.$$

If $\mathfrak{p}$ is not one of $\mathfrak{p}_1,\dots,\mathfrak{p}_w$, then by Lemma 12.1.12, $N(\mathfrak{p}_j)_{\mathfrak{p}} = KN(\mathfrak{p}_j) = V$, for $1 \le j \le w$. In this case, $N_{\mathfrak{p}} = F_{\mathfrak{p}} = N(\mathfrak{p})$. On the other hand, if $i \neq j$, then $N(\mathfrak{p}_i)_{\mathfrak{p}_j} = KN(\mathfrak{p}_i) = V$. Thus $N_{\mathfrak{p}_j} = N(\mathfrak{p}_j)_{\mathfrak{p}_j} \cap F_{\mathfrak{p}_j}$. But $N(\mathfrak{p}_j)_{\mathfrak{p}_j} = N(\mathfrak{p}_j) \subseteq F_{\mathfrak{p}_j}$, so $N_{\mathfrak{p}_j} = N(\mathfrak{p}_j)$ for $1 \le j \le w$.

(c): Suppose N' is an R-lattice in V such that $N'_{\mathfrak{p}} = N(\mathfrak{p})$ for all $\mathfrak{p} \in X_1(R)$. Then $N' \subseteq \bigcap_{\mathfrak{p}\in X_1(R)} N'_{\mathfrak{p}} = \bigcap_{\mathfrak{p}\in X_1(R)} N(\mathfrak{p}) = N$. □

LEMMA 12.1.12. *Let R be an integral domain with field of fractions K. Let $\mathfrak{p}$, $\mathfrak{q}$ be prime ideals in R with $\mathfrak{p} \not\subseteq \mathfrak{q}$. Assume $R_{\mathfrak{p}}$ is a discrete valuation ring. Then*

1. *(1) $(R_{\mathfrak{p}})_{\mathfrak{q}} = K$.*
2. *(2) If M is an $R_{\mathfrak{p}}$-module, then $M_{\mathfrak{q}} = M \otimes_R R_{\mathfrak{q}} = M \otimes_{R_{\mathfrak{p}}} K$.*

PROOF. Let $a \in \mathfrak{p} - \mathfrak{q}$. Then $a \in \mathfrak{p}R_{\mathfrak{p}}$ and $a^{-1} \in R_{\mathfrak{q}}$, so the only maximal ideal in $(R_{\mathfrak{p}})_{\mathfrak{q}}$ is the zero ideal. □

LEMMA 12.1.13. *Let R be an integrally closed integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V. Then the following are true.*

1. *(1) $R : M = \bigcap_{\mathfrak{p}\in X_1(R)} R_{\mathfrak{p}} : M_{\mathfrak{p}}$.*
2. *(2) For any $\mathfrak{p} \in X_1(R)$, $(R : M)_{\mathfrak{p}} = R_{\mathfrak{p}} : M_{\mathfrak{p}}$.*

PROOF. Let $F \subseteq M$ be a free R-lattice. For every $\mathfrak{p} \in X_1(R)$, the diagram

$$\begin{tikzcd} (R:M)_{\mathfrak{p}} \arrow[r, "\alpha"] \arrow[d, "\beta"'] & (R:F)_{\mathfrak{p}} \arrow[d, "\gamma"] \\ R_{\mathfrak{p}} : M_{\mathfrak{p}} \arrow[r, "\delta"] & R_{\mathfrak{p}} : F_{\mathfrak{p}} \end{tikzcd}$$

commutes where β and γ are the natural maps induced by change of base. Since F is free, γ is an isomorphism (Corollary 2.4.13). By Proposition 12.1.6 (1), α and δ are one-to-one. We have

$$R : M \subseteq \bigcap_{\mathfrak{p}\in X_1(R)} (R:M)_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{p}\in X_1(R)} R_{\mathfrak{p}} : M_{\mathfrak{p}}$$

where the intersection takes place in $V^* = K : V$. Let $f \in \bigcap_{\mathfrak{p}\in X_1(R)} R_{\mathfrak{p}} : M_{\mathfrak{p}}$. Then for every $\mathfrak{p} \in X_1(R)$, $f(M) \subseteq f(M_{\mathfrak{p}}) \subseteq R_{\mathfrak{p}}$. Then $f(M) \subseteq R = \bigcap_{\mathfrak{p}\in X_1(R)} R_{\mathfrak{p}}$, hence $f \in R : M$. This proves (1). Part (2) follows from Theorem 12.1.11 (2) and Part (1). □

THEOREM 12.1.14. *Let R be a noetherian integrally closed integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V. If we set $\tilde{M} = \bigcap_{\mathfrak{p}\in X_1(R)} M_{\mathfrak{p}}$, then the following are true.*

1. *(1) $R : (R : M) = \tilde{M}$.*
2. *(2) M is a reflexive R-lattice if and only if $M = \tilde{M}$.*
3. *(3) For each $\mathfrak{p} \in X_1(R)$, $\tilde{M}_{\mathfrak{p}} = M_{\mathfrak{p}}$.*
4. *(4) $\tilde{M}$ is a reflexive R-lattice in V containing M.*

PROOF. (1): Each $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-lattice, so by Lemma 12.1.13,

$$\begin{aligned} R:(R:M) &= \bigcap_{\mathfrak{p}\in X_1(R)} R_\mathfrak{p} : (R:M)_\mathfrak{p} \\ &= \bigcap_{\mathfrak{p}\in X_1(R)} R_\mathfrak{p} : (R_\mathfrak{p} : M_\mathfrak{p}) \\ &= \bigcap_{\mathfrak{p}\in X_1(R)} M_\mathfrak{p} \\ &= \tilde{M}. \end{aligned}$$

The rest is left to the reader. □

COROLLARY 12.1.15. *Let R be a noetherian integrally closed integral domain with field of fractions K and let V be a finite dimensional K-vector space. Let M and N be two R-lattices in V such that N is reflexive. In order for $M \subseteq N$ it is necessary and sufficient that $M_\mathfrak{p} \subseteq N_\mathfrak{p}$ for all $\mathfrak{p} \in X_1(R)$.*

PROOF. If $M \subseteq N$, then $M_\mathfrak{p} \subseteq N_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$. Conversely, we have

$$M \subseteq R:(R:M) = \bigcap_{\mathfrak{p}\in X_1(R)} M_\mathfrak{p} \subseteq \bigcap_{\mathfrak{p}\in X_1(R)} N_\mathfrak{p} = R:(R:N) = N.$$

□

The following proposition of Auslander and Goldman ([**8**]) will be applied in Section 12.6.1.

PROPOSITION 12.1.16. *Let R be a noetherian integrally closed integral domain. Let M and N be finitely generated torsion free R-modules. Then there are R-module isomorphisms*

$$\operatorname{Hom}_R(M,N)^{**} \cong (N^* \otimes_R M)^* \cong \operatorname{Hom}_R(M,N^{**}) \cong \operatorname{Hom}_R(N^*,M^*)$$

where we write $(\cdot)^*$ for the dual $\operatorname{Hom}_R(\cdot,R)$. In particular,

$$\operatorname{Hom}_R(M,M)^{**} \cong \operatorname{Hom}_R(M^*,M^*) \cong \operatorname{Hom}_R(M^{**},M^{**}).$$

PROOF. The homomorphism

$$N^* \otimes_R M \xrightarrow{\alpha} \operatorname{Hom}_R(M,N)^*$$

of Lemma 2.4.11 is defined by $\alpha(f\otimes x)(g) = f(g(x))$. The dual of α is

$$\operatorname{Hom}_R(M,N)^{**} \xrightarrow{\alpha^*} (N^* \otimes_R M)^*.$$

For each $\mathfrak{p} \in X_1(R)$, $R_\mathfrak{p}$ is a DVR and $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module (Proposition 12.1.4). By Proposition 3.5.8 and Lemma 2.4.11,

$$N^* \otimes_R M \otimes_R R_\mathfrak{p} \xrightarrow{\alpha\otimes 1} \operatorname{Hom}_R(M,N)^* \otimes_R R_\mathfrak{p}$$

is an isomorphism. Taking duals and applying the same argument,

$$\operatorname{Hom}_R(M,N)^{**} \otimes_R R_\mathfrak{p} \xrightarrow{\alpha^*\otimes 1} (N^* \otimes_R M)^* \otimes_R R_\mathfrak{p}$$

is also an isomorphism. By Theorem 12.1.14, $\operatorname{Hom}_R(M,N)^{**}$ is a reflexive R-lattice. Without explicitly doing so, we view all of the modules as lattices in suitable vector spaces over the field of fractions of R. Applying Corollary 12.1.15, we see that α^* is an isomorphism. The second and third isomorphisms follow from the first and the Adjoint Isomorphisms (Theorem 2.4.10).

By the first part, $\operatorname{Hom}_R(M,M)^{**} \cong \operatorname{Hom}_R(M^*,M^*)$. Then

$$\begin{aligned}\operatorname{Hom}_R(M,M)^{**} &\cong (\operatorname{Hom}_R(M,M)^{**})^{**} \\ &\cong \operatorname{Hom}_R(M^*,M^*)^{**} \\ &\cong \operatorname{Hom}_R(M^{**},M^{**}).\end{aligned}$$

□

1.2.1. *A Local to Global Theorem for Reflexive Lattices.* Constructing nontrivial examples of reflexive lattices of rank greater than or equal to two is generally a difficult task. Theorem 12.1.17 provides a globalization method for constructing reflexive lattices from locally defined projective lattices. A version of Theorem 12.1.17 for sheaves of modules on a ringed space was proved by B. Auslander in [**5**, Theorem VI.5]. A partial converse is [**5**, Theorem VI.6]. In the language of schemes, it says that if U is an open subset of $\operatorname{Spec} R$ which contains $X_1(R)$, and M is a sheaf of $\mathscr{O}_U$-modules which is locally projective of finite rank, then M comes from a finitely generated reflexive R-module N. For an application of Theorem 12.1.17 to construct a locally trivial nontrivial Azumaya algebra, the interested reader is referred to [**18**, Proposition 11.3.26].

Before stating Theorem 12.1.17 we establish some notation. Let R be a noetherian integrally closed integral domain with quotient field K. Let $f_1,\dots,f_n$ be a set of nonzero elements of R. Let $f_0 = f_1 \cdots f_n$. Write R_i for the localization R_{f_i}, and U_i for the basic open set $U(f_i) = \operatorname{Spec} R_i = \{\mathfrak{p} \in \operatorname{Spec} R \mid f_i \notin \mathfrak{p}\}$. Then $U_0 \subseteq U_1 \cap \cdots \cap U_n$. Assume $f_1,\dots,f_n$ are chosen so that the open set $U_1 \cup \cdots \cup U_n$ contains $X_1(R)$. Let V be a finite dimensional K-vector space. Suppose for each i that M_i is a locally free R_i-lattice in V such that for each pair i,j we have $M_i \otimes_{R_i} R_{ij} = M_j \otimes_{R_j} R_{ij}$, where $R_{ij} = R_{f_i f_j}$. Let $\mathfrak{p} \in X_1(R)$. If $\mathfrak{p}$ is in U_i, then $(M_i)_\mathfrak{p}$ is an $R_\mathfrak{p}$-lattice in V. Moreover, if $\mathfrak{p}$ is in $U_i \cap U_j$, then $(M_i)_\mathfrak{p} = (M_j)_\mathfrak{p}$. Let L be a free R_0-lattice in V which contains $M_1 \otimes_{R_i} R_0 = \cdots = M_n \otimes_{R_n} R_0$. Let $v_1,\dots,v_r$ be a free R_0-basis for L. Then $F = Rv_1 + \cdots + Rv_r$ is a free R-lattice in V.

THEOREM 12.1.17. *Let R, K, V, $f_1,\dots,f_n$, $M_1,\dots,M_n$, F be as above. For each $\mathfrak{p} \in X_1(R)$, define $N(\mathfrak{p})$ to be $(M_i)_\mathfrak{p}$, for any i such that $\mathfrak{p}$ is in U_i. If*

$$N = \bigcap_{\mathfrak{p} \in X_1(R)} N(\mathfrak{p}),$$

then

1. *N is an R-lattice in V and $N_\mathfrak{p} = N(\mathfrak{p})$ for all $\mathfrak{p} \in X_1(R)$.*
2. *N is a reflexive R-lattice in V.*
3. *$N \otimes_R R_{f_i} = M_i$ for $1 \le i \le n$.*
4. *$N = \bigcap_{i=1}^n M_i$.*

PROOF. (1): By Corollary 9.6.12, a minimal prime of f_0 has height one. By Corollary 4.1.15, f_0 is contained in only finitely many height one primes of R. Therefore, U_0 contains all but finitely many height one primes of R. By Theorem 12.1.11 (1), $(M_i)_\mathfrak{p} = F_\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in X_1(R_0)$. Taken together, this implies that $N(\mathfrak{p}) = F_\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in X_1(R)$. Part (1) follows from Theorem 12.1.11 (2).

(2): Follows from Theorem 12.1.14 (4).

(3): For each $\mathfrak{p} \in X_1(R_i)$, $(N \otimes_R R_i)_\mathfrak{p} = N_\mathfrak{p} = N(\mathfrak{p}) = (M_i)_\mathfrak{p}$. By Exercise 12.1.3 and Corollary 12.1.15, $N \otimes_R R_i = M_i$.

(4): Follows from: $N = \bigcap_{\mathfrak{p} \in X_1(R)} N(\mathfrak{p}) = \bigcap_{i=1}^n \bigcap_{\mathfrak{p} \in X_1(R_i)} (M_i)_\mathfrak{p} = \bigcap_{i=1}^n M_i$. □

1.3. Exercises.

EXERCISE 12.1.1. Let R be an integral domain and M a finitely generated torsion free R-module. Let S be a submodule of M and consider $\bar{S} = KS \cap M$.

(1) Prove that $M/\bar{S}$ is a finitely generated torsion free R-module.
(2) Prove that $KS = K\bar{S}$.

EXERCISE 12.1.2. Let R be an integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V. Then M is a reflexive R-lattice if and only if there is an R-lattice N (in some K-vector space) such that M is isomorphic as an R-module to $R : N$.

EXERCISE 12.1.3. Let R be a noetherian integrally closed integral domain with field of fractions K. Let V be a finite dimensional K-vector space.

(1) If M and N are reflexive R-lattices in V, then $M \cap N$ is a reflexive R-lattice in V.
(2) If U is a K-subspace of V, and M is a reflexive R-lattice in V, then $M \cap U$ is a reflexive R-lattice in U.
(3) If M is a reflexive R-lattice in V and $Z \subseteq R - \{0\}$ is a multiplicative set, then $Z^{-1}M$ is a reflexive $Z^{-1}R$-lattice in V.

2. Fractional Ideals

Let R be an integral domain with field of fractions K. A *fractional ideal* of R is a nonzero R-submodule F of K such that there exists a finitely generated R-submodule N of K and $F \subseteq N \subseteq K$. In the terminology of Definition 12.1.2, a fractional ideal of R is an R-lattice in K, where we view K as a vector space over itself. The material in this section is based on various sources, including [**31**] and [**21**].

LEMMA 12.2.1. *Let R be an integral domain with field of fractions K. If F is a nonzero R-submodule of K, then the following are equivalent.*

(1) F is a fractional ideal of R in K. That is, there exists a finitely generated R-submodule N such that $F \subseteq N \subseteq K$.
(2) There are nonzero elements a, b in K such that $aR \subseteq F \subseteq bR$.
(3) There exists a nonzero c in R such that $cF \subseteq R$.
(4) There exists a nonzero d in K such that $dF \subseteq R$.

PROOF. This is a special case of Proposition 12.1.1, so we only sketch the proof.

(1) implies (3): Write $N = Rx_1 + \cdots + Rx_n$ where $x_1, \ldots, x_n$ are elements of K. If c is the product of the denominators of $x_1, \ldots, x_n$, then for each i we have $cx_i \in R$. Therefore $cF \subseteq cN \subseteq Rcx_1 + \cdots + Rcx_n \subseteq R$.

(3) implies (4): Is trivial.

(4) implies (2): Suppose $dF \subseteq R$ and $d \in K - (0)$. If $b = d^{-1}$ and $a \in F - (0)$, then we have $aR \subseteq F = bdF \subseteq bR$.

(2) implies (1): Take $N = bR$. □

EXAMPLE 12.2.2. It follows immediately from Lemma 12.2.1 that a nonzero ideal I of R is a fractional ideal.

Let R be an integral domain with field of fractions K. If E and F are fractional ideals of R, the product EF is defined to be the R-submodule of K generated by the set $\{xy \mid x \in E \text{ and } y \in F\}$.

LEMMA 12.2.3. *Let R be an integral domain with field of fractions K. If E and F are fractional ideals of R, then $E+F$, $E\cap F$ and EF are fractional ideals of R.*

PROOF. By definition, E and F are nonzero. Thus $E+F$ is nonzero. Also by definition there are finitely generated R-submodules M and N of K such that $E\subseteq M$ and $F\subseteq N$. Then $E+F$ is a submodule of the finitely generated R-submodule $M+N$ of K. This proves $E+F$ is a fractional ideal of R. By Lemma 12.2.1 (2) there are nonzero elements a,b,c,d in K such that $aR\subseteq E\subseteq bR$ and $cR\subseteq F\subseteq dR$. Then $acR\subseteq EF\subseteq bdR$, which shows EF is a fractional ideal. Now we show $E\cap F$ is a fractional ideal. Since $E\cap F\subseteq E\subseteq M$, it remains to show $E\cap F$ is nonzero. There exist r,s,u,v in R such that $a=s/t$ and $c=u/v$. Then $us=uta\in E$ and $us=svc\in F$, hence $us\in E\cap F$. □

If F is a fractional ideal, let

$$F^{-1}=R:F=\{x\in K\mid xF\subseteq R\}.$$

LEMMA 12.2.4. *Let R be an integral domain with field of fractions K. If F is a fractional ideal of R, then the following are true.*

(1) F^{-1} is a fractional ideal of R.
(2) $F^{-1}F\subseteq R$ and $F^{-1}F$ is an ideal of R.

PROOF. (1): The proof that F^{-1} is a nonzero R-submodule of K is left to the reader. Let $a\in F-(0)$ and $x\in F^{-1}$. Then $xa\in R$ says $x\in a^{-1}R$. Since x was arbitrary, this implies $F^{-1}\subseteq a^{-1}R$ and by Lemma 12.2.1 (1), we are done.
The proof of (2) is left to the reader. □

DEFINITION 12.2.5. A fractional ideal F is called an *invertible ideal* of R in case $F^{-1}F=R$.

LEMMA 12.2.6. *Let R be an integral domain with field of fractions K.*

(1) If $\alpha\in K^*$, then the principal fractional ideal $I=R\alpha$ is invertible and $I^{-1}=R\alpha^{-1}$.
(2) If F is a fractional ideal of R and $f\in\operatorname{Hom}_R(F,R)$, then for all $a,b\in F$ it is true that $af(b)=bf(a)$.
(3) Let F be a fractional ideal of R. For any $\alpha\in F^{-1}$, let $\ell_\alpha:F\to R$ be "left multiplication by α". The mapping $\alpha\mapsto\ell_\alpha$ is an isomorphism of R-modules $\ell:F^{-1}\to F^*=\operatorname{Hom}_R(F,R)$.

PROOF. (2): Let a and b be arbitrary elements of F. There exist some elements $r,s,t,u\in R$ such that $a=rs^{-1}$ and $b=tu^{-1}$. Then $as=r$ and $bu=t$ are both in R. Also, $bas=br$ and $abu=at$ are both in F. For any $f\in\operatorname{Hom}_R(F,R)$ we have

$$sf(abu)=f(sabu)=uf(abs).$$

Combining these, we get $af(b)=saf(b)s^{-1}=f(abs)s^{-1}=f(abu)u^{-1}=buf(a)u^{-1}=bf(a)$.

(3): The reader should verify that the mapping $\ell:F^{-1}\to F^*$ is a one-to-one homomorphism of R-modules. Let $f\in F^*$. Fix an arbitrary $a\in F-(0)$. By (2), if $x\in F$, then $af(x)=xf(a)$. Let $\alpha=a^{-1}f(a)$. Then $f(x)=a^{-1}xf(a)=\alpha x=\ell_\alpha(x)$. This shows $f=\ell_\alpha$.
The proof of (1) is left to the reader. □

THEOREM 12.2.7. *Let R be an integral domain with field of fractions K and let F be a fractional ideal of R. The following are equivalent.*

(1) *F is a projective R-module.*
(2) *F is an invertible fractional ideal.*
(3) *F is a rank one R-progenerator. That is, F is an invertible R-module (Definition 3.6.6).*
(4) *There exists a fractional ideal E of R such that $EF = aR$ is a principal ideal.*

PROOF. (3) implies (1): Is trivial.

(2) implies (4): Take $E = F^{-1}$.

(4) implies (3): There exist elements $x_1, \dots, x_n$ in E, $y_1, \dots, y_n$ in F, and $a_1, \dots, a_n$ in R such that $a = \sum_{i=1}^n a_i x_i y_i$. Since EF is nonzero, we know $a \neq 0$. For any $x \in E$ and $y \in F$, we have $xy \in aR$. Then $a^{-1}xy \in R$. This implies $a^{-1}x \in F^{-1}$. By Lemma 12.2.6 (3), $\ell_{a^{-1}x} \in F^*$. For each i, let $\phi_i = \ell_{a^{-1}a_i x_i}$. Consider $\{(y_i, \phi_i) \mid 1 \le i \le n\}$. Given any $y \in F$ we have $ay = \sum_{i=1}^n a_i x_i y y_i$. Therefore, $y = \sum_{i=1}^n a^{-1} a_i x_i y y_i = \sum_{i=1}^n \phi_i(y) y_i$, which shows $\{(y_i, \phi_i) \mid 1 \le i \le n\}$ is a dual basis for F. By Lemma 2.1.10, F is a finitely generated projective R-module. Since R is an integral domain, by Corollary 2.2.4, F is an R-progenerator and by Corollary 3.4.8, $\operatorname{Rank}_R(F)$ is defined. Since $K \otimes_R F = K$, we see that F has $\operatorname{Rank}_R(F) = 1$.

(1) implies (2): By Lemma 2.1.10, F has a dual basis $\{(x_i, f_i) \mid i \in I\}$. It follows from Lemma 12.2.6 (3) that for each $i \in I$ there is $\alpha_i \in F^{-1}$ such that $f_i = \ell_{\alpha_i}$. If $x \in F - (0)$, then $f_i(x) = \alpha_i x$ is zero for all but finitely many $i \in I$. Since $\alpha_i \in K$, this implies I is a finite set. In particular, this implies F is finitely generated as an R-module. Then $x = \sum_{i \in I} f_i(x) x_i = \sum_{i \in I} \alpha_i x x_i$. This equation holds in the field K, so we cancel x to get $1 = \sum_{i \in I} \alpha_i x_i$. Since each α_i is in F^{-1}, this shows $F^{-1}F$ is equal to the unit ideal R. $\square$

LEMMA 12.2.8. *Let R be an integral domain with field of fractions K.*

(1) *If $F_1, \dots, F_n$ are fractional ideals of R, then $F = F_1 F_2 \cdots F_n$ is invertible if and only if each F_i is invertible.*
(2) *If $P_1, \dots, P_r$ are invertible prime ideals in R, and $Q_1, \dots, Q_s$ are prime ideals in R such that $P_1 P_2 \cdots P_r = Q_1 Q_2 \cdots Q_s$, then $r = s$ and after re-labeling, $P_i = Q_i$.*

PROOF. (1): Is left to the reader.

(2): The proof is by induction on r. The reader should verify the basis step. Assume $r > 1$ and that the claim is true for $r - 1$ prime factors. Choose a minimal member of the set $P_1, \dots, P_r$ and for simplicity's sake, assume it is P_1. Since $Q_1 \cdots Q_s \subseteq P_1$, by Definition 6.3.1, there exists i such that $Q_i \subseteq P_1$. Re-label and assume $Q_1 \subseteq P_1$. Likewise, $P_1 \cdots P_r \subseteq Q_1$ so there exists i such that $P_i \subseteq Q_1 \subseteq P_1$. Since P_1 is minimal, $P_1 = Q_1$. Multiply by P_1^{-1} to get $P_2 \cdots P_r = Q_2 \cdots Q_s$. Apply the induction hypothesis. $\square$

LEMMA 12.2.9. *Let R be an integral domain with field of fractions K. Let M be a nonzero finitely generated torsion free R-module.*

(1) *If $\dim_K(KM) = 1$, then M is isomorphic as an R-module to a fractional ideal of R in K.*
(2) *If R is a noetherian integrally closed integral domain and there exists $\alpha \in K$ such that $\alpha M \subseteq M$, then $\alpha \in R$.*

PROOF. (1): Choose any nonzero element m_0 of M and let $F = \{\alpha \in K \mid \alpha m_0 \in M\}$. Then F is an R-submodule of K. The assignment $\alpha \mapsto \alpha m_0$ defines a one-to-one R-module homomorphism $\theta : F \to M$. Since the K-vector space KM has dimension one, m_0 is a generator. Given any $m \in M$, there exists $\alpha \in K$ such that $\alpha m_0 = m$. Therefore θ is an isomorphism, and F is a nonzero finitely generated R-submodule of K. This means F is a fractional ideal of R.

(2): Begin as in Part (1). For any $m_0 \in M-(0)$, set $F = \{\alpha \in K \mid \alpha m_0 \in M\}$. Then there is a one-to-one R-module homomorphism $\theta : F \to M$ defined by $\alpha \mapsto \alpha m_0$. It follows from Corollary 4.1.12 that F is finitely generated as an R-module. Since F is nonzero, F is a fractional ideal of R. Clearly $R \subseteq F$ and $\alpha \in F$. It follows that $\alpha^n \in F$ for all $n \geq 0$. Then $R[\alpha] \subseteq F$ and Proposition 6.1.2 implies that α is integral over R. But R is integrally closed, so $\alpha \in R$. $\square$

2.1. Exercises.

EXERCISE 12.2.1. Let R be an integral domain. Let E and F be fractional ideals of R. If $EF = R$, then $E = F^{-1}$ and F is an invertible fractional ideal.

EXERCISE 12.2.2. Let R be an integral domain with field of fractions K. Let E and F be fractional ideals of R. If E is invertible, then the multiplication mapping $\alpha \otimes \beta \mapsto \alpha\beta$ is an isomorphism $E \otimes_R F \cong EF$ of R-modules.

EXERCISE 12.2.3. Let R be an integral domain with field of fractions K. Let E and F be fractional ideals of R in K.

(1) $KF = K$.
(2) $K \otimes_R F \cong KF$ by the multiplication mapping $\alpha \otimes x \mapsto \alpha x$.
(3) If $\phi : E \to F$ is an R-module isomorphism, then ϕ extends to a K-module isomorphism $\psi : K \to K$ and ψ is "left multiplication by $\psi(1)$".
(4) E and F are isomorphic as R-modules if and only if there exists $\alpha \in K$ such that $\alpha E = F$.

EXERCISE 12.2.4. Let R be an integral domain with field of fractions K. Let $\operatorname{Invert}(R)$ denote the set of all invertible fractional ideals of R in K. Let $\operatorname{Prin}(R)$ denote the subset of $\operatorname{Invert}(R)$ consisting of all principal fractional ideals of R in K.

(1) Prove that $\operatorname{Invert}(R)$ is a group under multiplication and contains $\operatorname{Prin}(R)$ as a subgroup.
(2) Every invertible ideal $I \in \operatorname{Invert}(R)$ is an invertible R-module, hence I represents a class in the Picard group of R (Definition 3.6.6). Show that this assignment defines a homomorphism $\theta : \operatorname{Invert}(R) \to \operatorname{Pic}(R)$.
(3) Show that θ induces an isomorphism $\operatorname{Invert}(R)/\operatorname{Prin}(R) \cong \operatorname{Pic}(R)$. The group $\operatorname{Invert}(R)/\operatorname{Prin}(R)$ is called the class group of rank one projective R-modules.

EXERCISE 12.2.5. Let k be a field, $A = k[x]$ and $R = k[x^2, x^3]$. From Exercises 3.6.6 and 6.1.7, we know that the quotient field of R is $K = k(x)$, A is the integral closure of R in K, and the conductor ideal from A to R is $\mathfrak{m} = (x^2, x^3)$, which is a maximal ideal in R. For each $\alpha \in k$, $P_\alpha = R(1-\alpha x) + \mathfrak{m}$ is a fractional ideal of R in K. Notice that P_α is an R-submodule of A. Prove:

(1) P_α is isomorphic to R if and only if $\alpha = 0$.
(2) $P_\alpha P_\beta = P_{\alpha+\beta}$. (Hints: $x^4 \in \mathfrak{m}^2$, $x^3 \in P_\alpha \mathfrak{m}$, $x^2 \in P_\alpha \mathfrak{m}$, $1-(\alpha+\beta)x \in P_\alpha P_\beta$.)
(3) $\operatorname{Pic} R$ contains a subgroup isomorphic to the additive group k.
(4) $\operatorname{Pic} R$ is generated by the classes of the modules P_α, which implies $\operatorname{Pic} R \cong k$. (See [**28**, Example II.6.11.4].) This proof may involve methods not yet proved in this text. Here is an outline of a proof which uses a Mayer-Vietoris exact sequence

of Milnor (see [**18**, Exercise 14.2.19]). First show that the diagram

$$\begin{tikzcd} R \arrow[r] \arrow[d] & R/\mathfrak{m} \arrow[d] \\ A \arrow[r] & A/\mathfrak{m} \end{tikzcd}$$

is a cartesian square of commutative rings (Example 2.7.17). There is an exact sequence

$$1 \to R^* \to A^* \times (R/\mathfrak{m})^* \to (A/\mathfrak{m})^* \xrightarrow{\partial} \operatorname{Pic} R \to \operatorname{Pic} A \times \operatorname{Pic}(R/\mathfrak{m}) \to \operatorname{Pic}(A/\mathfrak{m}).$$

of abelian groups from which $\operatorname{Pic} R$ can be computed.

EXERCISE 12.2.6. Let k be a field and $A = k[x,y]$ the polynomial ring over k in two variables. Consider the subring $R = k[x^2, xy, y^2, x^3, x^2y, xy^2, y^3]$ of A. The ideal $\mathfrak{m} = (x^2, xy, y^2, x^3, x^2y, xy^2, y^3)$ in R is maximal ideal. We know from Exercises 11.3.10 and 7.3.2 that the quotient field of R is $K = k(x,y)$, A is the integral closure of R in K, and the conductor ideal from A to R is $\mathfrak{m}$. For each pair $(\alpha,\beta) \in k^2$, $P_{\alpha,\beta} = R(1-\alpha x - \beta y) + \mathfrak{m}$ is a fractional ideal of R in K. Notice that $P_{\alpha,\beta}$ is an R-submodule of A. Prove:

(1) $P_{\alpha,\beta}$ is isomorphic to R if and only if $\alpha = \beta = 0$.
(2) $P_{\alpha,\beta}P_{\gamma,\delta} = P_{\alpha+\gamma,\beta+\delta}$. (Hints: $\mathfrak{m}^2$ contains every monomial of degree 4, $P_{\alpha,\beta}\mathfrak{m}$ contains every monomial of degree 3 or 2, $P_{\alpha,\beta}\mathfrak{m}$ contains $\mathfrak{m}$, $1-(\alpha+\gamma)x-(\beta+\delta)y \in P_{\alpha,\beta}P_{\gamma,\delta}$.)
(3) $\operatorname{Pic} R$ contains a subgroup isomorphic to the additive group k^2.
(4) $\operatorname{Pic} R$ is generated by the classes of the modules $P_{\alpha,\beta}$, which implies $\operatorname{Pic} R \cong k^2$. As in Exercise 12.2.5 (4), apply the Mayer-Vietoris sequence of Milnor. Use Corollary 11.4.13 and Exercise 12.4.10 to show that ∂ is onto. Now show the image of ∂ contains each class of the form $P_{\alpha,\beta}$.

EXERCISE 12.2.7. Let k be a field, $R = k[x,y]/(xy)$, $A = R/(x) \oplus R/(y)$. Let $\mathfrak{m}$ be the maximal ideal of R generated by x,y.

(1) Show that the natural map $\theta : R \to A$ is one-to-one, hence R can be viewed as a subring of A.
(2) Show that the conductor ideal from A to R is $\mathfrak{m}$.
(3) As in Exercise 12.2.5 (4), apply the Mayer-Vietoris sequence of Milnor to show that $R^* = k^*$ and $\operatorname{Pic} R = \langle 0 \rangle$.

EXERCISE 12.2.8. Let R be an integral domain with field of fractions K. Let S be another subring of K such that $R \subseteq S \subseteq K$ is a tower of subrings. Prove that $R : S$, the conductor ideal from S to R, is nonzero if and only if S is a fractional ideal of R in K.

3. Dedekind Domains

Dedekind domains arise in Algebraic Number Theory as the integral closure of $\mathbb{Z}$ in a finite algebraic extension of $\mathbb{Q}$. They arise in Algebraic Geometry as the coordinate ring of a nonsingular algebraic curve. A principal ideal domain is a Dedekind domain, but not conversely. Nevertheless, a Dedekind domain R is in many ways similar to a principal ideal domain. For example, we see in Proposition 12.3.3 below that if I is a proper ideal, then R/I is an artinian principal ideal ring. A Dedekind domain R is a noetherian normal integral domain with Krull dimension one. Conversely, we will see in Theorem 12.3.7 below that the integral closure of a noetherian integral domain with Krull dimension one in a finite algebraic extension of its quotient field is a Dedekind domain. In general R is not a unique factorization domain. However, unique factorization does exist for the set of proper ideals in R. The results in this section are based on various sources, including [**4**], [**31**] and [**15**].

In Theorem 12.3.2 below we list six equivalent properties of an integral domain. Any of them can be taken as the definition of a Dedekind domain. We first prove a useful lemma about rings with Krull dimension one.

LEMMA 12.3.1. *Let R be a commutative noetherian integral domain of Krull dimension one. For any proper ideal I of R, there exist unique primary ideals $I_1,\dots,I_n$ such that*

(1) $\operatorname{Rad} I_1,\dots,\operatorname{Rad} I_n$ *are distinct maximal ideals of R, and*
(2) $I = I_1 I_2 \cdots I_n$.

PROOF. (Existence.) By Theorem 9.3.8, I has a reduced primary decomposition $I = I_1 \cap I_2 \cap \cdots \cap I_n$. In a reduced primary decomposition the primes $\operatorname{Rad} I_1,\dots,\operatorname{Rad} I_n$ are distinct. Because I is nonzero and $\dim R = 1$, each $\operatorname{Rad} I_i$ is a maximal ideal of R. Two distinct maximal ideals are necessarily comaximal. By Exercise 3.3.4, the ideals I_i are pairwise comaximal. By Exercise 1.1.9, $I = I_1 I_2 \cdots I_n$.

(Uniqueness.) Suppose $I_1,\dots,I_n$ are primary ideals such that $\operatorname{Rad} I_1,\dots,\operatorname{Rad} I_n$ are distinct maximal ideals of R, and $I = I_1 I_2 \cdots I_n$. By the same argument as above, $I = I_1 \cap I_2 \cap \cdots \cap I_n$ is a reduced primary decomposition of I. By Lemma 9.3.5, the primary ideals I_i are uniquely determined by I. □

THEOREM 12.3.2. *Let R be an integral domain. The following are equivalent.*

(1) R is a noetherian normal integral domain with Krull dimension one.
(2) R is a noetherian integral domain and for every prime ideal P of height greater than or equal to one, the local ring R_P is a DVR.
(3) Every proper ideal in R has a unique representation as a product of a finite number of prime ideals.
(4) Every nonzero ideal in R is invertible. By Theorem 12.2.7, this is equivalent to each of the following statements.
 (a) Every nonzero ideal of R is R-projective.
 (b) Every nonzero ideal of R is an invertible R-module.
(5) Every fractional ideal of R is invertible. By Theorem 12.2.7, this is equivalent to each of the following statements.
 (a) Every fractional ideal of R is R-projective.
 (b) Every fractional ideal of R is an invertible R-module.
(6) Let $\operatorname{Frac}(R)$ *denote the set of all fractional ideals of R. Then* $\operatorname{Frac}(R)$ *is a group under multiplication.*

An integral domain satisfying the equivalent conditions of Theorem 12.3.2 is called a *Dedekind domain*.

PROOF. (1) is equivalent to (2): Is left to the reader.

(5) is equivalent to (6): Is left to the reader.

(5) implies (4): Is trivial.

(1) implies (3): Let I be a proper ideal of R. By Lemma 12.3.1, $I = I_1 \cdots I_n$ where $I_1,\dots,I_n$ are unique primary ideals. If $P_i = \operatorname{Rad} I_i$, then P_i is a maximal ideal of R. By Theorem 11.4.3, I_i is equal to the symbolic power $P_i^{(\nu_i)}$, for some unique $\nu_i > 0$. By Proposition 9.1.2 (3), $P_i^{\nu_i}$ is a P_i-primary ideal. By Exercise 9.3.1, it follows that $I_i = P_i^{\nu_i}$.

(4) implies (5): If F is a fractional ideal, then $F^{-1}F$ is invertible. By Lemma 12.2.8, F is invertible.

(4) implies (2): Let I be a nonzero ideal of R. By Theorem 12.2.7, I is a rank one projective R-module. Then I is finitely generated and by Corollary 4.1.7, R is noetherian. Let P be a nonzero prime ideal of R and let $\mathfrak{m}$ denote the maximal ideal PR_P in R_P. By Proposition 3.4.2, $\mathfrak{m}$ is a free R_P-module of rank one. In other words, $\mathfrak{m}$ is a principal ideal and Corollary 9.6.13 says $\dim R = 1$. Theorem 11.2.10 implies R_P is a DVR.

(3) implies (4): By Lemma 12.2.8, it suffices to show every nonzero prime ideal of R is invertible. The proof is split into two steps.

Step 1: If P is an invertible prime ideal in R, then P is maximal. The proof is by contradiction. Assume $a \in R - P$ and $P + Ra \neq R$. By assumption,

$$P + Ra = P_1 \cdots P_m$$
$$P + Ra^2 = Q_1 \cdots Q_n$$

for some prime ideals $P_1, \ldots, P_m, Q_1, \ldots, Q_n$. Since P is prime, R/P is an integral domain. Let $\eta : R \to R/P$ be the natural map.

$$\eta(P + Ra) = \eta(P_1) \cdots \eta(P_m)$$
$$\eta(P + Ra^2) = \eta(Q_1) \cdots \eta(Q_n)$$

The two ideals on the left-hand side are the principal ideals in R/P generated by $\eta(a)$ and $\eta(a^2)$ respectively. By Lemma 12.2.6 (1), $\eta(P + Ra)$ and $\eta(P + Ra^2)$ are invertible. Since $P \subseteq P_i$ and $P \subseteq Q_j$ for each i and j, the ideals $\eta(P_i)$ and $\eta(Q_j)$ are prime ideals in R/P. By Lemma 12.2.8 (1), for all i and j, the ideals $\eta(P_i)$ and $\eta(Q_j)$ are invertible prime ideals in R/P. Apply Lemma 12.2.8 (2) to the two factorizations

$$\eta(Q_1) \cdots \eta(Q_n) = \eta(P_1)^2 \cdots \eta(P_m)^2$$

of the principal ideal $\eta(P + Ra^2) = \eta(P + Ra)^2$. Then $n = 2m$ and upon relabeling, $\eta(P_i) = \eta(Q_{2i-1}) = \eta(Q_{2i})$ for $i = 1, \ldots, m$. By Proposition 1.5.3, $P_i = Q_{2i-1} = Q_{2i}$ for $i = 1, \ldots, m$, which implies

$$P + Ra^2 = Q_1 \cdots Q_n = P_1^2 \cdots P_m^2 = (P + Ra)^2.$$

We see that

$$P \subseteq P + Ra^2 \subseteq (P + Ra)^2 \subseteq P^2 + Ra.$$

Suppose $x \in P^2$, $r \in R$, and $x + ra \in P$. Since P is prime and $a \notin P$, we conclude $r \in P$. Hence $P \subseteq P^2 + Pa \subseteq P$. But P is invertible, so $R = P^{-1}(P^2 + Pa) = P + Ra$, a contradiction.

Step 2: If P is a nonzero prime ideal in R, then P is invertible. Let $x \in P - (0)$. By assumption, $Rx = P_1 \cdots P_m$ for some prime ideals $P_1, \ldots, P_m$. Then $P_1 \cdots P_m \subseteq P$. By Lemma 12.2.6 (1), Rx is invertible. By Lemma 12.2.8, each P_i in the product is invertible. By Definition 6.3.1, there exists i such that $P_i \subseteq P$. By Step 1, P_i is a maximal ideal in R. This shows $P = P_i$, hence P is invertible (and maximal). $\square$

Proposition 12.3.3 is a generalization of [**19**, Exercises 4.6.18 and 4.6.19].

PROPOSITION 12.3.3. *Let R be a Dedekind domain.*

(1) *Let P be a nonzero prime ideal in R, $e > 0$ and $A = R/(P^e)$. The following are true.*
   (a) *Every ideal in A is principal.*
   (b) *A is a field if and only if $e = 1$.*
   (c) *A is a local ring with maximal ideal P/P^e.*

   (d) *A has exactly $e+1$ ideals, namely: $(0) \subseteq P^{e-1}/P^e \subseteq \cdots \subseteq P^2/P^e \subseteq P/P^e \subseteq A$.*

(2) *Let $P_1,\dots,P_n$ be distinct nonzero prime ideals of R, $e_1,\dots,e_n$ positive integers, $I = P_1^{e_1}P_2^{e_2}\cdots P_n^{e_n}$, and $A = S/I$. The following are true.*
   (a) *A is isomorphic to the direct sum of the local rings $\bigoplus_i S/P_i^{e_i}$.*
   (b) *Every ideal in A is principal.*
   (c) *Including the two trivial ideals (0) and A, there are exactly $(e_1+1)(e_2+1)\cdots(e_n+1)$ ideals in A.*
   (d) *A has exactly n maximal ideals, namely $P_1/I,\dots,P_n/I$.*

PROOF. (1): The only maximal ideal of R that contains P^e is P, which is (c). By Theorem 12.3.2 (3), the ideals of R that contain P^e are $P^e, P^{e-1},\dots,P,R$, which is (d) and (b). If $1 \le i < e$ and $\alpha \in P^i - P^{i+1}$, then $P^e + R\alpha$ is not a subset of P^{i+1}. Hence $P^e + R\alpha = P^i$, which proves (a).

(2): A direct product of commutative rings $R_1 \times \cdots \times R_t$ is a principal ideal ring if and only if each R_i is a principal ideal ring. Therefore, (2) follows from Theorems 1.1.8, 1.1.7, and Part (1). □

COROLLARY 12.3.4. *Let I be an ideal in the Dedekind domain R. If I is not principal, then I is generated by two elements. That is, there exist α,β in I such that $I = R\alpha + R\beta$.*

PROOF. Assume I is not principal and pick any nonzero element α in I. By Proposition 12.3.3, the ideal $I/R\alpha$ is a principal ideal in $R/R\alpha$. There exists $\beta \in I$ such that $R\alpha + R\beta = I$. □

If I is an ideal in a Dedekind domain R, by Corollary 12.3.4, $I = R\alpha + R\beta$, where $\alpha \in I - (0)$ is arbitrary. For this reason, a Dedekind domain is said to have the "one and a half generator property for ideals".

COROLLARY 12.3.5. *Let I and J be proper ideals in the Dedekind domain R. Then there exist an element α in R and an ideal C in R satisfying $J + C = R$ and $IC = R\alpha$.*

PROOF. By Proposition 12.3.3, the ideal I/IJ is a principal ideal in R/IJ. There exists $\alpha \in I$ such that $R\alpha + IJ = I$. By Exercise 12.3.6, there exists an ideal C in R such that $R\alpha = IC$. Multiplying $IC + IJ = I$ by I^{-1} yields $C + J = R$. □

THEOREM 12.3.6. *Let R be a Dedekind domain with quotient field K and M a finitely generated torsion free R-module. If $n = \dim_K(KM)$, then there exist fractional ideals $F_1,\dots,F_n$ of R such that $M \cong F_1 \oplus \cdots \oplus F_n$.*

PROOF. Let x be any nonzero element of M. Let $S = Rx$ be the principal submodule of M generated by x. Let $\bar{S} = KS \cap M$. By Exercise 12.1.1, $M/\bar{S}$ is torsion free and $K\bar{S} = KS$. Since $\dim_K K\bar{S} = 1$, by Lemma 12.2.9, there exists a fractional ideal F_1 of R such that $\bar{S} \cong F_1$. Since $\dim_K \left(K \otimes_R (M/\bar{S})\right) = n-1$, by induction on n, there exist fractional ideals $F_2,\dots,F_n$ of R such that $M/\bar{S} \cong F_2 \oplus \cdots \oplus F_n$. By Theorem 12.3.2, each F_i is projective. Therefore the sequence $0 \to \bar{S} \to M \to M/\bar{S} \to 0$ is split exact. □

We now prove that the integral closure of a Dedekind domain in a finite extension of its quotient field is a Dedekind domain. Theorem 12.3.7 is a corollary to the Krull-Akizuki Theorem (Theorem 9.7.5).

THEOREM 12.3.7. *Let R be a noetherian integral domain with $\dim(R) = 1$. Let K be the quotient field of R, L a finitely generated algebraic field extension of K, and S the integral closure of R in L. Then S is a Dedekind domain.*

PROOF. By Theorem 9.7.5, S is noetherian and has Krull dimension one. By Corollary 6.1.8, L is the quotient field of S. Since S is integrally closed in L, by Theorem 12.3.2 (1), S is a Dedekind domain. □

3.1. Exercises.

EXERCISE 12.3.1. Let R be a Dedekind domain and $\mathrm{Frac}(R)$ the group of fractional ideals of R.

(1) $\mathrm{Frac}(R)$ is a free abelian group on the set $\mathrm{Max}(R)$, where the binary operation is multiplication.
(2) There is an isomorphism $\mathrm{Frac}(R) \cong \mathrm{Div}(R)$ which maps a maximal ideal P to the corresponding generator of $\mathrm{Div}(R)$.

EXERCISE 12.3.2. Let R be a Dedekind domain and $\mathrm{Frac}(R)$ the group of fractional ideals of R. Let $\mathrm{Prin}(R) = \{R\alpha \mid \alpha \in K^*\}$ denote the subset of $\mathrm{Frac}(R)$ consisting of all principal fractional ideals.

(1) $\mathrm{Prin}(R)$ is a subgroup of $\mathrm{Frac}(R)$.
(2) The quotient $\mathrm{Frac}(R)/\mathrm{Prin}(R)$ is isomorphic to $\mathrm{Cl}(R)$.
(3) The following are equivalent.
   (a) R is a PID.
   (b) R is a UFD.
   (c) $\mathrm{Cl}(R) = (0)$.

EXERCISE 12.3.3. Let R be a Dedekind domain and M a finitely generated R-module. The following are equivalent.

(1) M is torsion free.
(2) M is flat.
(3) M is projective.

EXERCISE 12.3.4. Show that if R is a Dedekind domain, then $\mathrm{Pic}(R)$ and $\mathrm{Cl}(R)$ are isomorphic.

EXERCISE 12.3.5. Let R be a Dedekind domain. Let $P_1,\dots,P_m,Q_1,\dots,Q_n$ be nonzero prime ideals of R satisfying $\prod_{i=1}^m P_i \supseteq \prod_{j=1}^n Q_j$. Then $m \le n$ and upon relabeling, $P_i = Q_i$ for $i = 1,\dots,m$.

EXERCISE 12.3.6. Let R be a Dedekind domain. If A and B are ideals of R such that $A \supseteq B$, then there exists an ideal C such that $AC = B$

EXERCISE 12.3.7. Let R be a Dedekind domain. Let $P_1,\dots,P_n$ be distinct nonzero prime ideals of R and let $e_1,\dots,e_n,f_1,\dots,f_n$ nonnegative integers. Let $I = \prod P_i^{e_i}$ and $J = \prod P_i^{f_i}$. Let $m_i = \min(e_i, f_i)$ and $M_i = \max(e_i, f_i)$. Then $I + J = \prod P_i^{m_i}$ and $I \cap J = \prod P_i^{M_i}$.

EXERCISE 12.3.8. Let R be a Dedekind domain. If F_1 and F_2 are fractional ideals of R, then there exists an isomorphism of R-modules $F_1 \oplus F_2 \cong R \oplus F_1F_2$.

EXERCISE 12.3.9. Let R be a Dedekind domain and assume $I_1,\dots,I_m$ and $J_1,\dots,J_n$ are fractional ideals of R. The following are equivalent.

(1) There exists an isomorphism of R-modules $I_1 \oplus \cdots \oplus I_m \cong J_1 \oplus \cdots \oplus J_n$.
(2) $m = n$ and there exists an isomorphism of R-modules $I_1 \cdots I_m \cong J_1 \cdots J_n$.

4. The Class Group of Rank One Reflexive Modules

In Definition 11.4.11, we defined $\mathrm{Cl}(R)$, the class group of a noetherian integrally closed integral domain R, in terms of $\mathrm{Div}(R)$, the group of Weil divisors of R. The main result of this section, Theorem 12.4.4, shows that $\mathrm{Div}(R)$ is isomorphic to the group of all reflexive fractional ideals of R. Consequently, $\mathrm{Cl}(R)$ is isomorphic to the group of reflexive fractional ideals of R in K, modulo the subgroup of principal fractional ideals (see Exercise 12.4.10).

4.1. Reflexive Fractional Ideals. Let R be an integral domain with field of fractions K. In this section we study fractional ideals of R in K which are reflexive R-lattices. Such fractional ideals are called *reflexive fractional ideals*. For instance, any invertible fractional ideal is projective (Theorem 12.2.7), hence reflexive. If F is a fractional ideal of R in K, then $F \subseteq (F^{-1})^{-1}$. By Lemma 12.2.6 (3), the assignment $\alpha \mapsto \ell_\alpha$ defines an isomorphism $F^{-1} \to \mathrm{Hom}_R(F,R)$. The reader should verify that $F \to F^{**}$ is an isomorphism (that is, F is reflexive) if and only if $F = (F^{-1})^{-1}$. If E and F are two fractional ideals of R in K, then

$$E : F = \{\alpha \in K \mid \alpha F \subseteq E\}.$$

We call $E : F$ either the ideal quotient, or module quotient (Definition 11.3.5). Notice that $F^{-1} = R : F$. For convenience, we assemble in Lemma 12.4.1 some results on reflexive fractional ideals that are special cases of results on reflexive lattices that we already proved in Section 12.1.2.

LEMMA 12.4.1. *Let R be an integral domain with field of fractions K.*

1. *If E and F are fractional ideals of R, then $E : F$ is a fractional ideal of R.*
2. *Given fractional ideals $I_1 \subseteq I_2$ and $J_1 \subseteq J_2$, $J_1 : I_2 \subseteq J_2 : I_1$.*
3. *If F is a fractional ideal, then*
$$F^{-1} = R : F = R : (R : (R : F)).$$
That is, F^{-1} is a reflexive fractional ideal and $F^{-1} \cong (F^{-1})^{**}$.
4. *If F is a fractional ideal, then*
$$(F^{-1})^{-1} = \bigcap_{\alpha \in F^{-1}} \alpha^{-1} R.$$
That is, F is a reflexive fractional ideal if and only if
$$F = \bigcap_{\alpha \in F^{-1}} \alpha^{-1} R.$$
5. *If D, E and F are fractional ideals, then*
   (a) *$D : EF = (D : E) : F$, and*
   (b) *$(D : E)F \subseteq D : (E : F)$.*
6. *If F is a fractional ideal, then $(F^{-1}F)^{-1} = F^{-1} : F^{-1}$.*
7. *If F is a fractional ideal and E is a reflexive fractional ideal, then $E : F$ is a reflexive ideal.*

PROOF. The reader should verify that (1), (2), (3), (4), (5) and (7) are special cases of Proposition 12.1.6, Lemma 12.1.7, Proposition 12.1.8, Lemma 12.1.9, and Proposition 12.1.10. (6): By Part (5) (a), $R : F^{-1}F = (R : F) : F^{-1} = (R : F) : (R : F)$. $\square$

Let $\mathrm{Reflex}(R)$ denote the set of all reflexive fractional ideals of R in K. If E and F are reflexive fractional ideals of R, then EF is not necessarily reflexive. Define a binary operation on $\mathrm{Reflex}(R)$ by the formula $E * F = R : (R : EF)$. By Exercise 12.4.6, this operation turns $\operatorname{Reflex}(R)$ into an abelian monoid with identity R. If R is a noetherian normal integral domain, then Lemma 11.1.2 (3) implies that R is completely normal and Proposition 12.4.2 implies that $\operatorname{Reflex}(R)$ is an abelian group.

PROPOSITION 12.4.2. *If R is an integral domain with field of fractions K, then* $\operatorname{Reflex}(R)$ *is an abelian group if and only if R is completely normal (see Definition 11.1.1).*

PROOF. Assume $\operatorname{Reflex}(R)$ is an abelian group. Let I be a fractional ideal of R in K. By Exercise 12.4.5, it is enough to show $R = I : I$. Let $J = (I^{-1})^{-1}$. By Lemma 12.4.1 (3), J is a reflexive fractional ideal. By Lemma 12.4.1 (7), $J : J$ is a reflexive fractional ideal. By Exercise 12.4.3, $J : J$ is an intermediate ring $R \subseteq J : J \subseteq K$, so $(J : J)^2 = J : J$. Then $R : (R : (J : J)^2) = R : (R : (J : J)) = J : J$ says $J : J$ is the idempotent of the group $\operatorname{Reflex}(R)$. That is, $R = J : J$. Again by Exercise 12.4.3,

$$R \subseteq I : I \subseteq I^{-1} : I^{-1} \subseteq J : J = R.$$

Conversely, if $I \in \operatorname{Reflex}(R)$, then so is I^{-1} by Lemma 12.4.1 (3). By Lemma 12.4.1 (6), $R : II^{-1} = I^{-1} : I^{-1} = R$. Then $R : (R : II^{-1}) = R$, so I^{-1} is the inverse of I in $\operatorname{Reflex}(R)$. $\square$

LEMMA 12.4.3. *Let R be a noetherian normal integral domain with field of fractions K.*

(1) Suppose I is an ideal in R that is maximal among all proper reflexive ideals in R. Then there exists an element $x \in K$ such that $I = R : (Rx + R)$ and I is a prime ideal.
(2) If P is a prime ideal of R and P is a reflexive ideal, then $\operatorname{ht}(P) = 1$.
(3) If $P \in X_1(R)$, then P is reflexive.

PROOF. (1): Since I is a proper reflexive ideal, $I^{-1} \neq R$. Pick $x \in I^{-1} - R$. Then $I \subseteq R : (Rx + R) \subseteq R$ and since $x \notin R$, $1 \notin R : (Rx + R)$. The ideal $R : (Rx + R)$ is reflexive, by Lemma 12.4.1 (3). By the maximality of I, $I = R : (Rx + R)$. Now suppose $a, b \in R$ and $ab \in I$. Let $A = Ra + I$ and $B = Rb + I$. Suppose $b \notin I$. Since $AB \subseteq I$, it follows that $I \subsetneq B \subseteq I : A$. Also, $I : A \subseteq I : I = R$. By Lemma 12.4.1 (7), $I : A$ is a reflexive ideal in R. By maximality of I we conclude that $I : A = R$. Since $1 \in I : A$, we conclude that $a \in I$.

(2): Since $P \neq R$, $R \neq R : P$. Suppose $Q \in \operatorname{Spec} R$ and $(0) \subsetneq Q \subsetneq P$. Let $x \in P - Q$. Then $(R : P)x \subseteq R$, so $(R : P)xQ \subseteq Q$. But $x \notin Q$ and Q is prime, so $(R : P)Q \subseteq Q$. Thus $R : P \subseteq Q : Q$. Since R is normal, $R = Q : Q$. This is a contradiction.

(3): If $x \in P - (0)$, then Rx is free, hence reflexive. The set

$$\mathscr{S} = \{I \in \operatorname{Reflex}(R) \mid I \subseteq P \text{ and there exists } \alpha \in K^* \text{ such that } I = R\alpha^{-1} \cap R\}$$

is nonempty. Since R is noetherian, $\mathscr{S}$ has a maximal member, $M = R\alpha^{-1} \cap R$. It suffices to show that M is prime. Let a, b be elements of R such that $ab \in M$. Then $R(a\alpha)^{-1} \cap R \supseteq R\alpha^{-1} \cap R = M$. By Exercise 12.4.9, $R(a\alpha)^{-1} \cap R$ is in $\operatorname{Reflex}(R)$.

Case 1: Assume $R(a\alpha)^{-1} \cap R \subseteq P$. By the choice of M, $R(a\alpha)^{-1} \cap R = M$. Thus $ab \in R(a\alpha)^{-1} \cap R$, so there exists $r \in R$ such that $ab = r(a\alpha)^{-1} \in R$. This shows that $b = r(a\alpha)^{-1}a^{-1} \in R\alpha^{-1} \cap R = M$.

Case 2: Assume $R(a\alpha)^{-1} \cap R \not\subseteq P$. There exists $y \in R(a\alpha)^{-1} \cap R$ such that $y \notin P$. Given $w = r(y\alpha)^{-1} \in R(y\alpha)^{-1} \cap R$, $yw = r\alpha^{-1} \in M \subseteq P$. Since $y \notin P$, this proves $R(y\alpha)^{-1} \cap R \subseteq P$. We have $M = R\alpha^{-1} \cap R \subseteq R(y\alpha)^{-1} \cap R \subseteq P$. By the choice of M, this means $M = R(y\alpha)^{-1} \cap R$. Hence $a \in R(y\alpha)^{-1} \cap R = M$.

This proves that M is prime. Since $\operatorname{ht}(P) = 1$, we conclude $M = P$. Thus P is reflexive. $\square$

THEOREM 12.4.4. *Let R be a noetherian normal integral domain with field of fractions K.*

(1) *If I is an ideal in R, then I is reflexive if and only if there exist $P_1,\dots,P_n \in X_1(R)$ such that $I = R:(R:(P_1\cdots P_n))$.*
(2) *If I is a reflexive ideal in R, then there are only finitely many $P \in X_1(R)$ such that $I \subseteq P$.*
(3) *The factorization in Part (1) is unique up to the order of the factors.*
(4) $\operatorname{Reflex}(R)$ *is a free $\mathbb{Z}$-module and $X_1(R)$ is a basis. The group* $\operatorname{Reflex}(R)$ *is isomorphic to* $\operatorname{Div}(R)$*, the group of Weil divisors of R.*

PROOF. (1): Suppose I is a proper ideal of R and I is reflexive. If $I \in X_1(R)$, then I has the desired factorization. The proof is by contradiction. Since R is noetherian, there exists a maximal counterexample, say M. That is, M is a reflexive proper ideal in R and M does not have a factorization in the form $M = R:(R:(P_1\cdots P_n))$, where each P_i is in $X_1(R)$. By Lemma 12.4.3, there is a maximal reflexive ideal P_1 that properly contains M. In fact, P_1 is in $X_1(R)$. Since $R \subsetneq P_1^{-1}$, it follows that $M \neq P_1^{-1} * M$, hence $M \subsetneq (R:P_1)M$. Take double duals, $M \subsetneq R:(R:(R:P_1)M)$. Also, $M \subseteq P_1 \subseteq R$, so $(R:P_1)M \subseteq (R:P_1)P_1 \subseteq R$. That is, $R:(R:(R:P_1)M)$ is a reflexive ideal in R that properly contains M. By the choice of M, this ideal has a factorization in the desired form:

$$R:(R:(R:P_1)M) = R:(R:(P_2\cdots P_n))$$

where $P_2,\dots,P_n \in X_1(R)$. Use Exercise 12.4.6 and Proposition 12.4.2 to show that $P_1^{-1} * M = P_2 * \cdots * P_n$ and $M = P_1 * P_2 * \cdots * P_n = R:(R:(P_1\cdots P_n))$. The converse follows from Lemma 12.4.1 (3).

(2): Suppose $I = R:(R:(P_1\cdots P_m))$ and each $P_i \in X_1(R)$. Then $P_1\cdots P_m \subseteq I$. Suppose $P \in X_1(R)$ such that $I \subseteq P$. By Proposition 1.5.4, there must be some i in $1,\dots,m$ such that $P_i \subseteq P$. Since $\operatorname{ht}(P) = 1$, $P_i = P$. There are only finitely many choices for P.

(3): Suppose $I = R:(R:(P_1\cdots P_m))$ and each $P_i \in X_1(R)$. If $m = 1$, then $I = P_1$ so the claim is trivially true. Proceed by induction on m. By Part (2), we can assume $I \subseteq P_1$. It follows that $I:P_1 \subseteq P_1:P_1 = R$. By Lemma 12.4.1, $I:P_1$ is a reflexive ideal in R. By Exercise 12.4.7, $I:P_1 = I * P_1^{-1}$. By Exercise 12.4.6, $I:P_1 = P_2 * \cdots * P_m = R:(R:(P_2\cdots P_m))$ and by induction we are done.

(4): By Parts (2) and (3) it suffices to show $\operatorname{Reflex}(R)$ is generated by those ideals in $X_1(R)$. Let $I \in \operatorname{Reflex}(R)$. There exists $a \in R$ such that $aI \subseteq R$. By Part (1) there are primes Q_i and P_j in $X_1(R)$ such that $aR = Q_1 * \cdots * Q_n$ and $aI = P_1 * \cdots * P_m$. Therefore, in the group $\operatorname{Reflex}(R)$ we have

$$I * Q_1 * \cdots * Q_n = P_1 * \cdots * P_m.$$

The last claim follows from the fact that the group of Weil divisors, $\operatorname{Div}(R)$, is the free $\mathbb{Z}$-module on $X_1(R)$ (Definition 11.4.11). □

4.2. A Nodal Cubic Curve. This section is devoted to an example of an algebraic plane curve that is nonnormal and birational to the affine line $\mathbb{A}^1$. Assume that the characteristic of k, the base field, is not 2. Consider the polynomial $y^2 - x^2(x+1)$ in $k[x][y]$. By Eisenstein's Criterion, with prime $p = x+1$, $y^2 - x^2(x+1)$ is irreducible in $k[x][y]$. Let $R = k[x,y]/(y^2 - x^2(x+1))$. In the following we show that R is a nonnormal integral domain, the Krull dimension of R is one, every maximal ideal of R is reflexive, and there is exactly one maximal ideal of R that is not projective,

First we show that R is isomorphic to the ring of Exercises 3.6.8 and 6.1.9. Let $A = k[z]$ be the polynomial ring over k in the variable z. Define $\theta : k[x,y] \to k[z]$ by assigning

$\theta(x) = z^2 - 1$, $\theta(y) = z(z^2 - 1)$. The image of θ is the ring $k[z^2 - 1, z(z^2 - 1)]$. It is routine to see that $\theta(y^2 - x^2(x+1)) = 0$. Therefore, θ factors through R and the diagram

$$\begin{tikzcd} k[x,y] \arrow[r, "\theta"] \arrow[d, "\eta"'] & k[z^2 - 1, z(z^2 - 1)] \\ R = \frac{k[x,y]}{(y^2 - x^2(x+1))} \arrow[ur, "\bar{\theta}"'] & \end{tikzcd}$$

commutes. Since θ is onto, $\bar{\theta}$ is onto. Since $k[z^2 - 1, z(z^2 - 1)]$ is an integral domain, $\ker \bar{\theta}$ is a prime ideal in R. By Theorem 10.3.1 and Corollaries 9.6.12, and 10.3.4, $\dim(R) = 1$. By Theorem 9.6.17, $\dim(k[z^2 - 1, z(z^2 - 1)]) = \dim(k[z]) = 1$. Another application of Corollary 10.3.4 shows $\bar{\theta}$ is one-to-one.

PROPOSITION 12.4.5. *Let k be a field with characteristic different from 2 and $R = k[x,y]/(y^2 - x^2(x+1))$. Then the following are true.*

(1) R is a noetherian integral domain with Krull dimension 1.
(2) If K denotes the quotient field of R, then y/x is transcendental over k and $K = k(y/x)$ is the field of rational functions in one variable over k.
(3) R is equal to the k-subalgebra of K generated by the two elements $x = (y/x)^2 - 1$ and $y = (y/x)((y/x)^2 - 1)$. The integral closure of R in K is $R[y/x] = k[y/x]$.
(4) The conductor ideal from $k[y/x]$ to R is equal to the ideal $\mathfrak{m} = (x,y)$. The ideal $\mathfrak{m}$ is a maximal ideal in R and a principal ideal (x) in $k[y/x]$.

PROOF. We already proved Part (1). From Exercises 3.6.8 and 6.1.9, the quotient field of $k[z^2 - 1, z(z^2 - 1)]$ is equal to $k(z)$, the integral closure is equal to $k[z]$, and the conductor ideal from $k[z]$ to $k[z^2 - 1, z(z^2 - 1)]$ is $(z^2 - 1, z(z^2 - 1))$. Parts (2) – (4) follow from this and the isomorphism $\bar{\theta}$ derived above. To see this, note that the identity $y^2 = x^2(x+1)$ implies $x = (y/x)^2 - 1$. Starting with the isomorphism $\bar{\theta}$, there is a commutative diagram

$$\begin{tikzcd} k[y/x] \arrow[r, "\cong"] & A = k[z] \\ R = \frac{k[x,y]}{(y^2 - x^2(x+1))} \arrow[u] \arrow[r, "\cong"] & k[z^2 - 1, z(z^2 - 1)] \arrow[u] \end{tikzcd}$$

of k-algebras. The left vertical arrow is defined by $x \mapsto (y/x)^2 - 1$ and $y \mapsto (y/x)x$ and is one-to-one. The right vertical arrow is set containment. The top horizontal arrow is the isomorphism defined by $y/x \mapsto z$. $\square$

PROPOSITION 12.4.6. *Let k be a field with characteristic different from 2 and $R = k[x,y]/(y^2 - x^2(x+1))$. Let K denote the quotient field of R and $\bar{R}$ the integral closure of R in K. Then the following are true.*

(1) In R, the ideal $\mathfrak{m} = (x,y)$ has the following properties:
  (a) $\mathfrak{m}$ is a maximal ideal of R and $\mathfrak{m}$ is the only prime ideal of R that contains x.
  (b) As R-modules, $\mathfrak{m}$ is isomorphic to $\bar{R}$.
  (c) $\mathfrak{m}$ and $\bar{R}$ are reflexive fractional ideals of R.
  (d) $\mathfrak{m}$ and $\bar{R}$ are not invertible fractional ideals. That is, $\mathfrak{m}$ and $\bar{R}$ are not projective R-modules.
  (e) $R : \bar{R} = \bar{R}^{-1} = \mathfrak{m}$, $R : \mathfrak{m} = \mathfrak{m}^{-1} = \bar{R}$, and $\mathfrak{m} : \mathfrak{m} = \bar{R}$.

(2) *If P is a maximal ideal of R and x is not in P, then P is a projective R-module. That is, P is an invertible fractional ideal.*

PROOF. (1): Since $R/(x,y) = k$, this proves $\mathfrak{m} = (x,y)$ is maximal. Any prime ideal that contains x contains $x^2(x+1) = y^2$, hence contains y. From Proposition 12.4.5, $\bar{R}$ is generated as an R-module by 1 and y/x. Since $(y/x)^2 = x+1$, we have $\bar{R} = R + R(y/x)$. Therefore, $\bar{R}$ is a fractional ideal of R in K. Then $\bar{R}^{-1}$ is equal to the conductor ideal $R : \bar{R}$, which is $\mathfrak{m} = (x,y)$. As an $\bar{R}$-module, $\mathfrak{m} = \bar{R}x = \bar{R}((y/x)^2 - 1)$ is cyclic. Therefore, left multiplication by $x = (y/x)^2 - 1$ is an R-module isomorphism $\ell_x : \bar{R} \to \mathfrak{m}$. By Lemma 12.4.1, $\mathfrak{m} = R : \bar{R}$ is a reflexive fractional ideal of R. By the isomorphism $\bar{R} \cong \mathfrak{m}$, this implies $\bar{R}$ is a reflexive fractional ideal of R. Since $\bar{R}^{-1}\bar{R} = \mathfrak{m} \neq R$, by Theorem 12.2.7 we see that $\bar{R}$ and $\mathfrak{m}$ are not invertible fractional ideals. Since $\bar{R}$ is reflexive, we have $\bar{R} = R : (R : \bar{R}) = R : \mathfrak{m}$. The last identity in (e) follows from $\bar{R} \subseteq \mathfrak{m} : \mathfrak{m} \subseteq R : \mathfrak{m} = \bar{R}$.

(2): Let P be a maximal ideal in R and assume x is not in P. Since $P \otimes_R R_{\mathfrak{m}}$ is the unit ideal, it is free of rank 1 over the local ring $R_{\mathfrak{m}}$. By Exercise 3.3.10, $P \otimes_R R[1/x]$ is a maximal ideal in $R[1/x]$. By Exercise 3.6.8, $R[1/x] = \bar{R}[1/x]$. Since $\bar{R}$ is a PID, $P \otimes_R R[1/x]$ is a principal ideal, hence free of rank 1 over $R[1/x]$. From this it follows that P satisfies Proposition 3.6.2 (4). Therefore, P is locally free of rank 1. By Theorem 12.2.7, P is an invertible fractional ideal. $\square$

See Exercise 12.4.12 for a continuation of this example.

4.3. Exercises.

EXERCISE 12.4.1. Let R be an integral domain with field of fractions K. Let E and F be fractional ideals of R in K. For any $\alpha \in E : F$, let $\ell_\alpha : F \to E$ be "left multiplication by α". The mapping $\alpha \mapsto \ell_\alpha$ is an isomorphism of R-modules $E : F \to \operatorname{Hom}_R(F,E)$.

EXERCISE 12.4.2. Let R be an integral domain with field of fractions K.

(1) If M is a reflexive R-module, then M is torsion free.
(2) If M is a finitely generated reflexive R-module and $\dim_K(K \otimes_R M) = 1$, then M is isomorphic to a reflexive fractional ideal of R in K.

EXERCISE 12.4.3. Let R be an integral domain with field of fractions K. Let F be a fractional ideal of R in K.

(1) $F : F$ is a ring, and $R \subseteq F : F \subseteq K$ is a tower of subrings.
(2) $F : F \subseteq F^{-1} : F^{-1} \subseteq (F^{-1})^{-1} : (F^{-1})^{-1}$.

EXERCISE 12.4.4. Let R be an integral domain with field of fractions K and let $\alpha \in K$. The following are equivalent.

(1) α is almost integral over R.
(2) $R[\alpha]$ is a fractional ideal of R in K.
(3) There exists a fractional ideal F of R in K such that $\alpha F \subseteq F$.

EXERCISE 12.4.5. If R is an integral domain with field of fractions K, then R is completely normal if and only if $R = F : F$ for all fractional ideals F of R in K.

EXERCISE 12.4.6. Let R be an integral domain with field of fractions K. Let D, E, F be fractional ideals of R in K.

(1) Show that $(D^{-1} : E) : F = (E^{-1} : F) : D$.
(2) Show that $(D((EF)^{-1})^{-1})^{-1} = (((DE)^{-1})^{-1}F)^{-1} = (DEF)^{-1}$.
(3) Show that with the binary operation $E * F = R : (R : EF) = ((EF)^{-1})^{-1}$, $\operatorname{Reflex}(R)$ is an abelian monoid.

EXERCISE 12.4.7. Let R be a noetherian normal integral domain with field of fractions K. Let E and F be elements of the group $\operatorname{Reflex}(R)$. Prove that $E : F = E * F^{-1}$ and $F : E = F * E^{-1}$.

EXERCISE 12.4.8. Let R be an integral domain with field of fractions K. Let E and F be elements of the group $\operatorname{Reflex}(R)$. Prove that $\operatorname{Hom}_R(E,F)$ is a free R-module of rank one if and only if E is isomorphic to F.

EXERCISE 12.4.9. Let R be a noetherian normal integral domain with field of fractions K. Let E and F be reflexive fractional ideals. Prove that $E \cap F$ is a reflexive fractional ideal.

EXERCISE 12.4.10. Let R be a noetherian normal integral domain with field of fractions K.

(1) $\operatorname{Invert}(R)$ is a subgroup of $\operatorname{Reflex}(R)$.
(2) $\operatorname{Prin}(R)$ is a subgroup of $\operatorname{Reflex}(R)$.
(3) The quotient $\operatorname{Reflex}(R)/\operatorname{Prin}(R)$ is called the *class group* of rank one reflexive R-modules. Show that this group is isomorphic to the class group of Weil divisors $\operatorname{Cl}(R)$.
(4) Show that there is a one-to-one homomorphism

$$\operatorname{Invert}(R)/\operatorname{Prin}(R) \to \operatorname{Reflex}(R)/\operatorname{Prin}(R)$$

from the class group of rank one projectives into the class group of rank one reflexives.
(5) There is a one-to-one homomorphism $\operatorname{Pic}(R) \to \operatorname{Cl}(R)$.

EXERCISE 12.4.11. Let R be a noetherian normal integral domain and $\operatorname{Sing}(R)$ the set of all maximal ideals $\mathfrak{m} \in \operatorname{Max}(R)$ such that $\operatorname{Cl}(R_{\mathfrak{m}}) \neq (0)$. Show that the natural maps induce an exact sequence

$$0 \to \operatorname{Pic}(R) \to \operatorname{Cl}(R) \to \prod_{\mathfrak{m} \in \operatorname{Sing}(R)} \operatorname{Cl}(R_{\mathfrak{m}})$$

of abelian groups. (Hint: Exercise 11.4.4.)

EXERCISE 12.4.12. Let k be a field with characteristic different from 2. Let $R = k[x,y]/(y^2 - x^2(x+1))$ be the ring of Section 12.4.2. Let K denote the quotient field of R and $\bar{R}$ the integral closure of R in K. Consider the tower of rings $k[x] \subseteq R \subseteq \bar{R}$. Prove the following:

(1) R is free of rank 2 over $k[x]$.
(2) $\bar{R}$ is free of rank 2 over $k[x]$.
(3) $\bar{R}$ is not free over R.
(4) R is not separable over $k[x]$.
(5) $\bar{R}$ is not separable over $k[x]$.
(6) $\bar{R}$ is separable over R. (Hint: Theorem 10.1.12.)

5. Functorial Properties of the Class Group

Let R be a noetherian normal integral domain with field of fractions K. Let S be a noetherian normal integral domain with field of fractions L. The class group is not a functor. That is, a homomorphism $R \to S$ does not necessarily induce a homomorphism of groups $\operatorname{Cl}(R) \to \operatorname{Cl}(S)$. There are three important cases when a homomorphism on class groups does exist. The first case is when S is a localization of R in K and $K = L$. This is the context of Nagata's Theorem and the reader is referred to Theorem 11.4.14

and Exercise 11.4.4. Secondly, if S is a flat R-algebra, we show that there is an induced homomorphism $\gamma\colon \mathrm{Cl}(R) \to \mathrm{Cl}(S)$. This is the subject of Section 12.5.1. The third scenario is when S is a faithful R-algebra which is finitely generated as an R-module. In this context, we show in Section 12.5.2 that there is a homomorphism $\gamma\colon \mathrm{Cl}(R) \to \mathrm{Cl}(S)$. The special case where L/K is a finite Galois extension of fields is investigated in Section 12.5.3. Many of the results in this section have appeared in [**18**, Section 6.5].

5.1. Flat Extensions. Now assume S/R is an extension of noetherian normal integral domains and L/K is the corresponding extension of the fields of fractions. Assume S is a flat R-algebra. Then in this context, Proposition 12.5.2 shows that there is a homomorphism of divisor groups $\beta : \mathrm{Div}(R) \to \mathrm{Div}(S)$ which induces a homomorphism of class groups $\gamma\colon \mathrm{Cl}(R) \to \mathrm{Cl}(S)$.

LEMMA 12.5.1. *Let R be a noetherian integral domain with field of fractions K. Let M be a reflexive R-lattice in the finite dimensional K-vector space V. Let $\theta : R \to S$ be a flat homomorphism of commutative rings. The following are true.*

(1) $S \otimes_R M$ is a reflexive S-module.
(2) If θ is one-to-one and S is an integral domain with field of fractions L, then the image of $S \otimes_R M$ is a reflexive S-lattice in $L \otimes_K V$.

PROOF. (1): Since R is noetherian, both M and $\mathrm{Hom}_R(M,R)$ are finitely presented R-modules. Applying Proposition 3.5.8, we see that $S \otimes_R M$ is a reflexive S-module.
(2): By Proposition 12.1.5, $S \otimes_R M$ is an S-lattice in $L \otimes_K V$. □

PROPOSITION 12.5.2. *Let S/R be an extension of noetherian normal integral domains and L/K the corresponding extension of the fields of fractions. Assume S is a flat R-algebra. Let I be a reflexive fractional ideal of R in K. The following are true.*

(1) IS is a reflexive fractional ideal of S in L.
(2) $I \otimes_R S \cong IS$ by the multiplication map $a \otimes b \mapsto ab$.
(3) The action $I \mapsto IS$ induces a homomorphism $\mathrm{Cl}(R) \to \mathrm{Cl}(S)$ of abelian groups.

PROOF. (2): There is $\alpha \in R$ such that $\alpha I \subseteq R$. Since S is flat over R, the multiplication map $\alpha I \otimes_R S \to \alpha IS$ is an isomorphism, by Corollary 3.7.4. From this we get $I \otimes_R S \to IS$ is an isomorphism.
(1): This follows from (2) and Lemma 12.5.1.
(3): By (1) and (2), the assignment $I \mapsto IS$ induces a homomorphism $\mathrm{Reflex}(R) \to \mathrm{Reflex}(S)$. If I is a principal ideal of R, then IS is a principal ideal of S, hence under this homomorphism $\mathrm{Prin}(R)$ is mapped to $\mathrm{Prin}(S)$. By Exercise 12.4.10, this induces a homomorphism of groups $\mathrm{Cl}(R) \to \mathrm{Cl}(S)$. □

COROLLARY 12.5.3. *Let S/R be an extension of noetherian normal integral domains and L/K the corresponding extension of the fields of fractions. Assume S is a faithfully flat R-algebra.*

(1) Let I be a fractional ideal of R in K. Then I is a projective fractional ideal if and only if IS is a projective fractional ideal of S in L.
(2) If $\mathrm{Pic}(R) = 0$, then $\mathrm{Cl}(R) \to \mathrm{Cl}(S)$ is one-to-one.

PROOF. (1): This follows from Proposition 12.5.2 and Lemma 3.5.12.
(2): If I is a reflexive fractional ideal of R in K and IS is principal, then I is an invertible fractional ideal, by (1). Since $\mathrm{Pic}(R) = 0$, I is principal. □

COROLLARY 12.5.4. *(Mori's Theorem) Let R be a commutative noetherian ring, I an ideal contained in the Jacobson radical of R, and $\hat{R}$ the I-adic completion of R. If $\hat{R}$ is an integrally closed integral domain, then R is an integrally closed integral domain and* $\mathrm{Cl}(R) \to \mathrm{Cl}(\hat{R})$ *is one-to-one.*

PROOF. By Theorem 7.3.7, the ring R and ideal I make up a Zariski pair and $\hat{R}$ is a faithfully flat R-algebra. By Corollary 7.3.12, $\hat{R}$ is noetherian. If $\hat{R}$ is an integrally closed integral domain, then R is also, by Exercise 6.1.4. Given a reflexive fractional ideal $\mathfrak{a}$ of R, by Proposition 12.5.2 the assignment $\mathfrak{a} \mapsto \mathfrak{a}\hat{R}$ induces a homomorphism $\mathrm{Cl}(R) \to \mathrm{Cl}(\hat{R})$. There exists a nonzero element $c \in R$ such that $c\mathfrak{a} \subseteq R$. By Corollary 7.3.14, if $c\mathfrak{a}\hat{R}$ is a principal ideal, then $c\mathfrak{a}$ is a principal ideal. It follows that the map on class groups is one-to-one. $\square$

Polynomial rings are an important special case of the above. Let R be a commutative ring and x an indeterminate. By Exercise 3.5.8, $R[x]$ is a faithfully flat extension of R. If R is a normal ring, then so is $R[x]$, by Lemma 11.1.6.

THEOREM 12.5.5. *Let R be a noetherian commutative ring.*

(1) If R is an integrally closed integral domain, then the natural homomorphism $\mathrm{Cl}(R) \to \mathrm{Cl}(R[x])$ *is an isomorphism.*
(2) If R is a normal ring, then the natural homomorphism $\mathrm{Pic}(R) \to \mathrm{Pic}(R[x])$ *is an isomorphism.*

PROOF. (1): Let K be the quotient field of R. Since $K[x]$ is a unique factorization domain, $\mathrm{Cl}(K[x]) = 0$ (Corollary 11.4.13). By Nagata's Theorem (Exercise 11.4.4), $\mathrm{Cl}(R[x])$ is generated by the prime divisors $P \in X_1(R[x])$ such that $P \cap R \neq (0)$. Let $S = R[x]$ and $P \in X_1(S)$. Since S/R is faithfully flat, going down holds and Theorem 9.6.16 says $\mathrm{ht}(P) = \mathrm{ht}(P \cap R) + \mathrm{ht}(P/(P \cap R)S)$. If $P \cap R \neq (0)$, this means $P \cap R \in X_1(R)$, and $P = (P \cap R)S$. Therefore, $\mathrm{Cl}(R) \to \mathrm{Cl}(R[x])$ is onto. Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}(R) & \xrightarrow{\alpha} & \mathrm{Pic}(R[x]) \\ \downarrow & & \downarrow \\ \mathrm{Cl}(R) & \xrightarrow{\beta} & \mathrm{Cl}(R[x]) \end{array}$$

in which β is onto and the vertical maps are one-to-one (Exercise 12.4.10). If $R[x] \to R$ is the homomorphism defined by $x \mapsto 0$, then $R \to R[x] \to R$ is an isomorphism of rings. Since $\mathrm{Pic}(\,)$ is a functor, $\mathrm{Pic}(R) \to \mathrm{Pic}(R[x]) \to \mathrm{Pic}(R)$ is an isomorphism of abelian groups, hence α is one-to-one. By Corollary 12.5.3 (1) it follows that α is onto and β is one-to-one.

(2): By the proof of (1), this is true when R is an integral domain. It follows from Lemma 11.1.5 that R is a finite direct sum of normal integral domains. By Exercise 3.6.2, the Picard group distributes across direct sums. $\square$

5.2. Finite Extensions. We begin by establishing some notation that will be in effect throughout this section. Let S/R be an extension of noetherian normal integral domains and L/K the corresponding extension of the fields of fractions. Assume S is a finitely generated R-module. Then S is equal to the integral closure of R in L. Since $S \otimes_R K$ is the localization of S in L with respect to the multiplicative set $R - \{0\}$, $S \otimes_R K$ is an integral domain. By Theorem 2.3.23, $S \otimes_R K$ is a finitely generated K-vector space. Thus $S \otimes_R K$ is a field, by Lemma 6.1.4. Therefore, $S \otimes_R K = L$ which implies $\dim_K(L) = m$ is finite.

In this context, we show that there is a homomorphism of divisor groups $\beta : \mathrm{Div}(R) \to \mathrm{Div}(S)$ which induces a homomorphism of class groups $\gamma : \mathrm{Cl}(R) \to \mathrm{Cl}(S)$. By Parts (1) and

(5) of Theorem 6.3.6, the continuous map $\operatorname{Spec} S \to \operatorname{Spec} R$ is onto and going down holds for $R \to S$. Assume $\mathfrak{p} \in X_1(R)$ and $\mathfrak{q} \in \operatorname{Spec}(S)$ such that $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{p}$. By Theorem 9.6.17, $\mathfrak{q} \in X_1(S)$. By Theorem 11.2.10, $R_{\mathfrak{p}}$ is a discrete valuation ring. By Corollary 6.3.7, $S_{\mathfrak{p}} = S \otimes_R R_{\mathfrak{p}}$ is a semilocal ring whose maximal ideals correspond to the prime ideals $\mathfrak{q} \in X_1(S)$ lying over $\mathfrak{p}$. Before defining the homomorphism $\beta : \operatorname{Div} R \to \operatorname{Div} S$, we define for every prime $\mathfrak{q} \in X_1(S)$ such that $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{p}$ two important numbers $e(\mathfrak{q})$, $f(\mathfrak{q})$. These numbers are significant in their own right, hence Proposition 12.5.6 is stated in the special case where R is a discrete valuation ring with quotient field K and S is the integral closure of R in a finite algebraic extension field of K.

PROPOSITION 12.5.6. *Let R be a DVR with quotient field K, maximal ideal $\mathfrak{m}$, residue field $k = R/\mathfrak{m}$, and local parameter π. Let L/K be a finite algebraic extension of fields with $\dim_K(L) = m$ and let S be the integral closure of R in L. Then the following are true.*

(1) The ring S satisfies the following:
 (a) S is a noetherian normal integral domain with Krull dimension one. In other words, S is a Dedekind domain (see Theorem 12.3.2).
 (b) The quotient field of S is L.
 (c) S is a torsion free R-module and $S \otimes_R K = L$. If S is a finitely generated R-module, then S is a free R-module of rank m.
 (d) $X_1(S)$ is a finite set, say $\{\mathfrak{q}_1, \dots, \mathfrak{q}_t\}$.
 (e) S is semilocal.
 (f) $\operatorname{Pic} S = \operatorname{Cl} S = (0)$.
 (g) S is a PID and hence a UFD.

(2) For each $1 \le i \le t$, $S_{\mathfrak{q}_i}$ is a DVR and $R \to S_{\mathfrak{q}_i}$ is a local homomorphism of local rings. Denote the maximal ideal of $S_{\mathfrak{q}_i}$ by $\mathfrak{m}(\mathfrak{q}_i)$ and the residue field by $k(\mathfrak{q}_i)$. There exist unique positive integers e_i and f_i satisfying:
 (a) $\mathfrak{m} S_{\mathfrak{q}_i} = \mathfrak{m}(\mathfrak{q}_i)^{e_i}$.
 (b) $k(\mathfrak{q}_i)$ is a finite dimensional extension field of k and $\dim_k k(\mathfrak{q}_i) = f_i$.

(3) The numbers t, e_i, f_i satisfy the identity: $\dim_k S \otimes_R k = \sum_{i=1}^{t} e_i f_i$. If S is a finitely generated R-module, then $\dim_k S \otimes_R k = \operatorname{Rank}_R(S) = \dim_K(L)$.

PROOF. (1): By Theorem 12.3.7, S is a Dedekind domain and L is the quotient field of S. By Lemma 9.7.1, $S \otimes_R K = L$. Therefore S is a torsion free R-module of rank $\dim_K(L) = m$. By Corollary 9.7.6, S is semilocal and the maximal ideals of S are precisely the minimal prime over-ideals of $\mathfrak{m}$. For some $t \ge 1$ we have $X_1(S) = \{\mathfrak{q}_1, \dots, \mathfrak{q}_t\}$. Over a semilocal integral domain a finitely generated projective module is free, by Exercise 4.2.5. By Exercises 12.3.4 and 12.3.2, $\operatorname{Pic} S = \operatorname{Cl} S = (0)$ and S is a PID. This proves (1).

(2): Fix $1 \le i \le t$. By Theorem 11.2.10, $S_{\mathfrak{q}_i}$ is a discrete valuation ring for L. Let $\mathfrak{m}(\mathfrak{q}_i)$ be the maximal ideal and $k(q_i)$ the residue field of $S_{\mathfrak{q}_i}$. Since $\mathfrak{m} = \mathfrak{q}_i \cap R$, the ideal $\mathfrak{m} S_{\mathfrak{q}_i}$ is contained in $\mathfrak{m}(\mathfrak{q}_i)$. By Lemma 11.2.9, $\mathfrak{m} S_{\mathfrak{q}_i} = \mathfrak{m}(\mathfrak{q}_i)^{e_i}$ for a unique $e_i \ge 1$, which is (a). By Theorem 9.7.5, $S \otimes_R k$ is a finite dimensional k-vector space. By Exercise 4.1.13 and Theorem 4.5.6, $S \otimes_R k$ decomposes into the direct sum of local rings

$$S \otimes_R k = \bigoplus_{i=1}^{t} S_{\mathfrak{q}_i} / \mathfrak{m} S_{\mathfrak{q}_i}. \tag{5.1}$$

Each local ring $S_{\mathfrak{q}_i} / \mathfrak{m} S_{\mathfrak{q}_i}$ is finite dimensional over k. Therefore, the residue field $k(\mathfrak{q}_i)$ is finite dimensional over k. Then $\dim_k k(\mathfrak{q}_i) = f_i$ is finite, which is (b).

(3): Fix $1 \le i \le t$. By (2) we have the identity

$$\mathfrak{m}S_{\mathfrak{q}_i} = \mathfrak{m}(\mathfrak{q}_i)^{e_i}.$$

The local ring $S_{\mathfrak{q}_i}/\mathfrak{m}S_{\mathfrak{q}_i} = S_{\mathfrak{q}_i}/\mathfrak{m}(\mathfrak{q}_i)^{e_i}$ is a k-vector space with filtration by subspaces

$$\frac{\mathfrak{m}(\mathfrak{q}_i)^{e_i}}{\mathfrak{m}(\mathfrak{q}_i)^{e_i}} \subseteq \frac{\mathfrak{m}(\mathfrak{q}_i)^{e_i-1}}{\mathfrak{m}(\mathfrak{q}_i)^{e_i}} \subseteq \cdots \subseteq \frac{\mathfrak{m}(\mathfrak{q}_i)^{2}}{\mathfrak{m}(\mathfrak{q}_i)^{e_i}} \subseteq \frac{\mathfrak{m}(\mathfrak{q}_i)}{\mathfrak{m}(\mathfrak{q}_i)^{e_i}} \subseteq \frac{S_{\mathfrak{q}_i}}{\mathfrak{m}(\mathfrak{q}_i)^{e_i}}.$$

Since $S_{\mathfrak{q}_i}$ is a DVR, for $1 \le j \le e_i$, the factor $\mathfrak{m}(\mathfrak{q}_i)^{j-1}/\mathfrak{m}(\mathfrak{q}_i)^j$ is isomorphic to $k(\mathfrak{q}_i)$ as a k-vector space. Thus the dimension of each factor of the filtration is equal to f_i. There are e_i factors in the filtration, so $\dim_k S_{\mathfrak{q}_i}/\mathfrak{m}S_{\mathfrak{q}_i} = e_i f_i$. Combining this with the direct sum in (5.1), we have $\dim_k S \otimes_R k = \sum_{i=1}^t e_i f_i$, which completes the proof. □

DEFINITION 12.5.7. In Proposition 12.5.6 (2), the number e_i is called the *ramification index of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$ and the number f_i is called the *degree of the residue field extension of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$. Notice that $e_i = 1$ if and only if $\mathfrak{m}S_{\mathfrak{q}_i} = \mathfrak{m}(\mathfrak{q}_i)$. In this case we say $\mathfrak{q}_i$ is *unramified* over $\mathfrak{p}$.

COROLLARY 12.5.8. *In the context of Proposition 12.5.6, $S \otimes_R k$ is separable over k if and only if for each i, $e_i = 1$ and the extension of residue fields $k(\mathfrak{q}_i)/k$ is separable.*

PROOF. This follows from Corollary 5.5.9 and Proposition 12.5.6. □

Now let S/R be an extension of noetherian normal integral domains and L/K the corresponding extension of the fields of fractions. Assume S is a finitely generated R-module. Let $\mathfrak{p} \in X_1(R)$. By Theorem 11.2.10, $R_\mathfrak{p}$ is a discrete valuation ring. Since $S_\mathfrak{p}$ is the localization of S in L with respect to the multiplicative set $R - \mathfrak{p}$, by Lemma 6.1.7, $S_\mathfrak{p}$ is the integral closure of $R_\mathfrak{p}$ in L and $S_\mathfrak{p}$ is an integrally closed integral domain by Theorem 6.1.3. Then $R_\mathfrak{p}$, with quotient field K and $S_\mathfrak{p}$, with quotient field L are in the context of Proposition 12.5.6. Then $X_1(S_\mathfrak{p})$ is a finite set. If $\mathfrak{q}$ is in $X_1(S_\mathfrak{p})$, the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$ is denoted $e_\mathfrak{q}$ and the degree of the residue field extension is denoted $f_\mathfrak{q}$. A prime $\mathfrak{q}$ in $X_1(S_\mathfrak{p})$ corresponds to a minimal prime over-ideal of $\mathfrak{p}S$ in $\operatorname{Spec} S$, which will also be denoted $\mathfrak{q}$. The local ring of $S_\mathfrak{p}$ at $\mathfrak{q}$ is equal to the local ring $S_\mathfrak{q}$. The homomorphism

$$\beta : \operatorname{Div} R \to \operatorname{Div} S$$

is defined by sending the prime divisor $\mathfrak{p} \in X_1(R)$ to the divisor $\sum_{\mathfrak{q} \cap R = \mathfrak{p}} e_\mathfrak{q} \mathfrak{q}$, where the sum runs over the set of primes in $X_1(S)$ lying over $\mathfrak{p}$, which is equal to the set $X_1(S_\mathfrak{p})$. Thus,

$$\begin{aligned}\beta(\mathfrak{p}) &= \sum_{\mathfrak{q} \cap R = \mathfrak{p}} e_\mathfrak{q} \mathfrak{q} \\ &= \sum_{\mathfrak{q} \in X_1(S_\mathfrak{p})} e_\mathfrak{q} \mathfrak{q}.\end{aligned}$$

PROPOSITION 12.5.9. *Let S/R be an extension of noetherian normal integral domains and L/K the corresponding extension of the fields of fractions. Assume S is a finitely generated R-module. Then there is a homomorphism $\gamma : \operatorname{Cl}(R) \to \operatorname{Cl}(S)$ which is induced on divisors by the homomorphism β defined above.*

PROOF. Let $\alpha \in K^*$. Let $\mathfrak{q} \in X_1(S)$ and $\mathfrak{q} \cap R = \mathfrak{p}$. By definition of ramification index, $\nu_{\mathfrak{q}}(\alpha) = e_{\mathfrak{q}} \nu_{\mathfrak{p}}(\alpha)$. Therefore, β maps a principal divisor to a principal divisor, the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Prin}(R) \arrow[r] \arrow[d] & \mathrm{Div}(R) \arrow[r] \arrow[d, "\beta"] & \mathrm{Cl}(R) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & \mathrm{Prin}(S) \arrow[r] & \mathrm{Div}(S) \arrow[r] & \mathrm{Cl}(S) \arrow[r] & 0
\end{tikzcd}$$

commutes and the rows are exact. □

In the context of Proposition 12.5.9, the *ramification divisor* on $\operatorname{Spec} S$ is the subset of $X_1(S)$ consisting of all primes $\mathfrak{q}$ of height one such that $e_{\mathfrak{q}} > 1$. In Proposition 12.5.10 we show that the ramification divisor is a finite set if the extension of fields L/K is separable.

PROPOSITION 12.5.10. *Let R be a noetherian integrally closed integral domain with field of fractions K. Let L/K be a finite separable extension of fields and S the integral closure of R in L. The ramification divisor,*

$$\{\mathfrak{q} \in X_1(S) \mid e_{\mathfrak{q}} > 1\},$$

is a finite set.

PROOF. By the Primitive Element Theorem, Theorem 5.5.8, there exists $\alpha \in L$ such that $L = K(\alpha)$ is a simple extension. Let $f = \operatorname{Irr.poly}_K(\alpha)$ be the irreducible polynomial of α in $K[x]$. So f is separable and the ideal in $K[x]$ generated by f and f' contains 1. There exist $g, h \in K[x]$ such that $gf + hf' = 1$. The polynomials f, g, h, f' have coefficients in K. Let a be a nonzero element of R such that the polynomials af, ag, ah, af' have coefficients in R. Let $A = R[a^{-1}]$ be the localization of R in K formed by inverting a. Then the polynomials f, g, h, f' have coefficients in A and the ideal in $A[x]$ generated by f and f' contains 1. By Proposition 5.6.2, $T = A[x]/(f)$ is separable over A and T is a free A-module of rank $m = \deg(f) = \dim_K(L)$. Since $L = K[x]/(f)$, we can map T isomorphically onto $A[\alpha]$ by the assignment $x \mapsto \alpha$. The quotient field of T contains K and α, hence L is equal to the quotient field of T. The diagram of subrings

$$\begin{tikzcd}
 & & L = K(\alpha) & \\
 & T = A[\alpha] \arrow[ur] & & K \arrow[ul] \\
S \arrow[ur] & & A = R[a^{-1}] \arrow[ul] \arrow[ur] & \\
 & R \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

commutes where each arrow is set inclusion. By change of base (Corollary 5.3.2), given any $\mathfrak{p} \in \operatorname{Spec}(A)$, we have $T \otimes_A k(\mathfrak{p})$ is separable over $k(\mathfrak{p})$. By Corollary 12.5.8, every $\mathfrak{q} \in X_1(T)$ is unramified over $\mathfrak{q} \cap A$. For each $\mathfrak{p} \in \operatorname{Spec}(A)$, we have $T \otimes_A k(\mathfrak{p})$ is a direct sum of fields by Corollary 5.5.9. Therefore, $T \otimes_A k(\mathfrak{p})$ is a regular ring. So T is normal by Corollary 11.5.6. This means T is the integral closure of A in L. By Lemma 6.1.7, $S[a^{-1}]$ is the integral closure of A in L. This proves $T = S[a^{-1}]$. As in the proof of Theorem 11.4.14, we can view $\mathrm{Div}(R[a^{-1}])$ as the free $\mathbb{Z}$-submodule of $\mathrm{Div}(R)$ generated by the primes in

$X_1(R[a^{-1}])$. Let $\operatorname{Div}(a) = \nu_1\mathfrak{p}_1 + \cdots + \nu_n\mathfrak{p}_n$. Then $X_1(R) = X_1(R[a^{-1}]) \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Let $\mathfrak{q}$ be a ramified height one prime in $X_1(S)$ and set $\mathfrak{p} = \mathfrak{q} \cap R$. Then $\mathfrak{p}$ is not in $X_1(R[a^{-1}])$, so $\mathfrak{p}$ is in the finite set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By Proposition 12.5.6, there are only finitely many primes of S that lie over each $\mathfrak{p}_i$. $\square$

We apply the results of this section to a ramified radical extension (see Section 11.5.3).

COROLLARY 12.5.11. *Let R be a noetherian normal integral domain and a a nonzero element of R such that* $\operatorname{Div}(a) = P_1 + \cdots + P_v$ *is a reduced effective divisor. If $n \geq 2$ is invertible in R and $S = R[x]/(x^n - a)$, then the following are true.*

(1) There are unique primes $Q_1, \ldots, Q_v$ in $X_1(S)$ such that $P_i = Q_i \cap R$ and $\operatorname{Div}(x) = Q_1 + \cdots + Q_v$.
(2) For each i, the ramification index e_{Q_i} is equal to n.
(3) The ramification divisor of the extension S/R is equal to $\{Q_1, \ldots, Q_v\}$.

PROOF. This follows from the proofs of Parts (4) and (5) of Theorem 11.5.14. $\square$

5.3. Galois Descent of Divisor Classes. References for the material in this section are [**21**], [**50**], and [**53**]. Let R be a noetherian integrally closed integral domain with quotient field K. Let L/K be a finite dimensional extension of fields which is Galois with group G. The degree of the extension is denoted n. Let S be the integral closure of R in L. Then L is the quotient field of S and S is finitely generated as an R-module (Theorem 6.1.13). We are in the context of Proposition 12.5.9. The reader should verify that that G acts on S as a group of R-algebra automorphisms, and $S^G = R$. If $\mathfrak{q} \in \operatorname{Spec} S$, then it is clear that for every $\sigma \in G$, $\sigma(\mathfrak{q})$ is in $\operatorname{Spec} S$. Moreover, if $\mathfrak{p} \in X_1(R)$, then $S_\mathfrak{p}$ is the integral closure of $R_\mathfrak{p}$ in L and G acts as a group of permutations of $X_1(S_\mathfrak{p})$. The prime ideals in $X_1(S_\mathfrak{p})$ correspond to height one primes in S lying over $\mathfrak{p}$. By Theorem 6.3.5 (6), any two primes in $X_1(S_\mathfrak{p})$ are conjugate to each other. Therefore, G acts as a group of permutations on $X_1(S)$. Since $\operatorname{Div}(S)$ is the free abelian group on $X_1(S)$, this makes $\operatorname{Div}(S)$ into a $\mathbb{Z}G$-module. In Proposition 12.5.12, we employ the notation of Section 8.5.

PROPOSITION 12.5.12. *In the above context, the following are true.*

(1) There is a monomorphism $\beta : \operatorname{Div}(R) \to \operatorname{Div}(S)^G$ of abelian groups.
(2) $\operatorname{Cl}(S)$ is a $\mathbb{Z}G$-module and there is a homomorphism of groups $\gamma : \operatorname{Cl}(R) \to \operatorname{Cl}(S)^G$.
(3) There is a natural exact sequence
$$0 \to \ker \gamma \to \mathrm{H}^1(G, S^*) \to \operatorname{Div}(S)^G / \operatorname{Div}(R)$$
of abelian groups.
(4) If each $\mathfrak{q} \in X_1(S)$ is unramified over $\mathfrak{q} \cap R$, then $\beta : \operatorname{Div}(R) \to \operatorname{Div}(S)^G$ is an isomorphism.

PROOF. (1): Clearly β is one-to-one. Given $\mathfrak{q} \in X_1(S)$, let $\mathfrak{p} = R \cap \mathfrak{q}$. Each $\sigma \in G$ induces a commutative diagram

$$\begin{tikzcd} S_\mathfrak{q} \arrow[rr, "\sigma"] \arrow[dr] & & S_{\sigma(\mathfrak{q})} \\ & R_\mathfrak{p} \arrow[ur] & \end{tikzcd}$$

where the top row is an isomorphism. From this we see that the ramification index of $\mathfrak{q}$ is equal to the ramification index of $\sigma(\mathfrak{q})$. Hence the image of β is fixed by σ.

(2): If $\alpha \in L^*$, then $v_{\mathfrak{q}}(\alpha) = v_{\sigma(\mathfrak{q})}(\sigma(\alpha))$, so σ maps a principal divisor to a principal divisor and $\mathrm{Cl}(S)$ is a $\mathbb{Z}G$-module. The rest follows from (1).

(3): The long exact sequence of cohomology associated to

$$1 \to S^* \to L^* \to \operatorname{Prin} S \to 0 \tag{5.2}$$

and Hilbert's Theorem 90 (Theorem 8.5.23) yield the exact sequence

$$\begin{aligned} 1 \to R^* \to K^* \to \operatorname{Prin}(S)^G \to \mathrm{H}^1(G,S^*) \to 0 \\ \to \mathrm{H}^1(G,\operatorname{Prin} S) \xrightarrow{\delta^1} \mathrm{H}^2(G,S^*) \xrightarrow{\varepsilon} \mathrm{H}^2(G,L^*). \end{aligned} \tag{5.3}$$

By definition, $K^*/R^* = \operatorname{Prin} R$. The diagram

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Prin} R \arrow[r] \arrow[d] & \operatorname{Div} R \arrow[r] \arrow[d, "\beta"] & \operatorname{Cl} R \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & \operatorname{Prin}(S)^G \arrow[r] & \operatorname{Div}(S)^G \arrow[r] & \operatorname{Cl}(S)^G & \end{tikzcd} \tag{5.4}$$

commutes and the rows are exact. To finish (3), combine (5.3) and (5.4) with the Snake Lemma (Theorem 2.5.2).

(4): For each $\mathfrak{p} \in X_1(R)$, let $P(\mathfrak{p}) = \{\mathfrak{q} \in X_1(S) \mid \mathfrak{q} \cap R = \mathfrak{p}\}$ be the set of those prime divisors in $X_1(S)$ lying over $\mathfrak{p}$. Then $\beta(\mathfrak{p}) = \sum_{\mathfrak{q}\in P(\mathfrak{p})} e_{\mathfrak{q}}\mathfrak{q} = \sum_{\mathfrak{q}\in P(\mathfrak{p})} \mathfrak{q}$ because each ramification index is assumed to be 1. By Theorem 6.3.6 (6), if $\mathfrak{q} \cap R = \mathfrak{p}$, then the set $P(\mathfrak{p})$ is equal to the orbit of $\mathfrak{q}$ under the action of G on $\operatorname{Div}(S)$. Let $D = \sum_{\mathfrak{q}\in X_1(S)} a_{\mathfrak{q}}\mathfrak{q}$ be a divisor in $\operatorname{Div}(S)^G$. Since D is fixed by each $\sigma \in G$, the coefficients $a_{\mathfrak{q}}$ are constant as $\mathfrak{q}$ runs through $P(\mathfrak{p})$. If we denote this constant by $a_{\mathfrak{p}}$, then

$$D = \sum_{\mathfrak{p}\in X_1(R)} \left(a_{\mathfrak{p}} \sum_{\mathfrak{q}\in P(\mathfrak{p})} \mathfrak{q} \right) = \sum_{\mathfrak{p}\in X_1(R)} a_{\mathfrak{p}} \beta(\mathfrak{p})$$

which shows D is in the image of β. □

PROPOSITION 12.5.13. *In the above context,* $\mathrm{H}^1(G, \operatorname{Div} S) = (0)$.

PROOF. For each $\mathfrak{p} \in X_1(R)$ fix a prime $Q_{\mathfrak{p}} \in X_1(S)$ lying above $\mathfrak{p}$. Let $G_{\mathfrak{p}}$ be the subgroup of G fixing $Q_{\mathfrak{p}}$. The reader should verify that

$$\operatorname{Div}(S) = \bigoplus_{\mathfrak{p}\in X_1(R)} \mathbb{Z}G \otimes_{\mathbb{Z}G_{\mathfrak{p}}} \mathbb{Z}$$

as G-modules. Since G is finite, $\operatorname{Hom}_{\mathbb{Z}G_{\mathfrak{p}}}(\mathbb{Z}G,\mathbb{Z})$ and $\mathbb{Z}G \otimes_{\mathbb{Z}G_{\mathfrak{p}}} \mathbb{Z}$ are isomorphic as G-modules (Lemma 8.5.18). From Theorem 8.5.13, for each $\mathfrak{p} \in X_1(R)$ we have the identity $\mathrm{H}^1(G, \operatorname{Hom}_{\mathbb{Z}G_{\mathfrak{p}}}(\mathbb{Z}G,\mathbb{Z})) = \mathrm{H}^1(G_{\mathfrak{p}},\mathbb{Z})$. But $\mathbb{Z}$ is a trivial $G_{\mathfrak{p}}$-module and by Proposition 8.5.9 we see that $\mathrm{H}^1(G_{\mathfrak{p}},\mathbb{Z}) = \operatorname{Hom}(G_{\mathfrak{p}},\mathbb{Z})$. But G is finite, so the last group is the trivial group (0). It follows from Exercise 8.5.6 that $\mathrm{H}^1(G, \operatorname{Div}(S)) = (0)$. □

The exact sequence that we derive in Theorem 12.5.14 is a special case of the main theorem of [**50**].

THEOREM 12.5.14. *(D. S. Rim) In the above context, there is an exact sequence*

$$\begin{aligned} 0 \to \mathrm{Cl}(S/R) \xrightarrow{\gamma_0} \mathrm{H}^1(G,S^*) \xrightarrow{\gamma_1} \operatorname{Div}(S)^G/\operatorname{Div}(R) \\ \xrightarrow{\gamma_2} \mathrm{Cl}(S)^G/\mathrm{Cl}(R) \xrightarrow{\gamma_3} \mathrm{H}^2(G,S^*) \xrightarrow{\gamma_4} \mathrm{H}^2(G,L^*) \end{aligned} \tag{5.5}$$

of abelian groups where $\mathrm{Cl}(S/R)$ *is the kernel of* $\mathrm{Cl}(R) \to \mathrm{Cl}(S)$.

PROOF. The long exact sequence of cohomology associated to the short exact sequence

$$0 \to \operatorname{Prin} S \to \operatorname{Div} S \to \operatorname{Cl} S \to 0 \tag{5.6}$$

is

$$0 \to \operatorname{Prin}(S)^G \to \operatorname{Div}(S)^G \to \operatorname{Cl}(S)^G \xrightarrow{\delta^0} \mathrm{H}^1(G, \operatorname{Prin} S) \to \mathrm{H}^1(G, \operatorname{Div} S). \tag{5.7}$$

By Proposition 12.5.13, δ^0 is onto. Combine (5.3) with (5.7) to get

$$\begin{aligned} 0 \to \operatorname{Cl}(S/R) \xrightarrow{\gamma_0} \mathrm{H}^1(G, S^*) &\xrightarrow{\gamma_1} \operatorname{Div}(S)^G \\ &\xrightarrow{\gamma_2} \operatorname{Cl}(S)^G \xrightarrow{\delta^1\delta^0} \mathrm{H}^2(G, S^*) \xrightarrow{\gamma_4} \mathrm{H}^2(G, L^*). \end{aligned} \tag{5.8}$$

Using Diagram (5.4) it is straightforward to derive (5.5) from (5.8). □

In Proposition 12.5.12 we saw that the group $\operatorname{Div}(S)^G/\operatorname{Div}(R)$ is trivial whenever S/R is unramfied at every height one prime. We end this section with a description of this group for another important class of examples. In Proposition 12.5.15 we assume that for every prime $\mathfrak{q} \in X_1(S)$, if $\mathfrak{q}$ is ramified, then $\mathfrak{q}$ is fixed by the Galois group. That is, $e_{\mathfrak{q}} f_{\mathfrak{q}} = n$.

PROPOSITION 12.5.15. *In the context of Section 12.5.3, assume that for every height one prime $\mathfrak{q}$ of S, if $\mathfrak{q}$ is ramified, then $\mathfrak{q}$ is fixed by the Galois group. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_v$ be those primes in $X_1(S)$ with ramification index $e_{\mathfrak{q}_i} > 1$. The case $v = 0$ is allowed. In the context of Theorem 12.5.14,*

$$\operatorname{Div}(S)^G/\operatorname{Div}(R) \cong \begin{cases} (0) & \text{if } v = 0 \\ \bigoplus_{i=1}^{v} (\mathbb{Z}/e_{\mathfrak{q}_i})\mathfrak{q}_i & \text{if } v > 0. \end{cases}$$

PROOF. Let $\mathfrak{p}_i = \mathfrak{q}_i \cap R$, $U = X_1(R) - \{\mathfrak{p}_1, \dots, \mathfrak{p}_v\}$ and $V = X_1(S) - \{\mathfrak{q}_1, \dots, \mathfrak{q}_v\}$. Start with the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \bigoplus_{i=1}^{v} \mathbb{Z}\mathfrak{p}_i \arrow[r] \arrow[d, "\alpha"] & \operatorname{Div}(R) \arrow[r, "\pi"] \arrow[d, "\beta"] & \bigoplus_{\mathfrak{p}\in U} \mathbb{Z}\mathfrak{p} \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & \bigoplus_{i=1}^{v} \mathbb{Z}\mathfrak{q}_i \arrow[r] & \operatorname{Div}(S)^G \arrow[r, "\theta"] & \left(\bigoplus_{\mathfrak{q}\in V} \mathbb{Z}\mathfrak{q}\right)^G & \end{tikzcd}$$

where the map π is the projection onto the submodule spanned by U and θ is the projection onto the submodule spanned by V. The vertical maps α and γ are induced by β. The map α is defined by $\mathfrak{p}_i \mapsto e_{\mathfrak{q}_i}\mathfrak{q}_i$. The proof of Proposition 12.5.12 (4) shows γ is an isomorphism. The rest follows from the Snake Lemma (Theorem 2.5.2). □

We apply the results of this section to a ramified radical extension (see Section 11.5.3).

COROLLARY 12.5.16. *Let R be a noetherian normal integral domain with quotient field K. Assume R is a $\mathbb{Z}[n^{-1}, \zeta]$-algebra, where ζ is a primitive nth root of unity in $\mathbb{C}$. Let a be a nonzero element of R and assume $\operatorname{Div}(a)$ is a reduced effective divisor. If $S = R[x]/(x^n - a)$ and $L = K[x]/(x^n - a)$, then the following are true.*

(1) L/K is a cyclic Galois extension with group $G = \langle\sigma\rangle$, and $\sigma(x) = \zeta x$.

(2) If $\operatorname{Div}(x) = Q_1 + \cdots + Q_v$, then in the context of Theorem 12.5.14,

$$\bigoplus_{i=1}^{v} (\mathbb{Z}/n)Q_i = \operatorname{Div}(S)^G/\operatorname{Div}(R)$$

is a free $\mathbb{Z}/n$-module of rank v.

PROOF. By [**19**, Theorem 5.6.3], L/K is a Kummer extension of degree n. By Corollary 12.5.11, the ramification divisor of the extension S/R is equal to $\{Q_1,\dots,Q_v\}$. For each i, the action by G on $\mathrm{Div}(S)$ fixes each ramified prime divisor $Q_i = P_iS + (x)$. The ramification index e_{Q_i} is equal to n. The rest follows from Proposition 12.5.15. □

5.4. Exercises.

EXERCISE 12.5.1. Let $n \geq 2$ be an integer and k a field in which $2n$ is invertible. Also assume k contains a primitive $2n$th root of unity, ζ. For $T = k[x,y,z]/(z^n - x^{n-1}y + 1)$, prove the following.

(1) T is an integrally closed integral domain.
(2) If $\alpha : T[x^{-1}] \to k[x,z,x^{-1}]$ is the function defined by $y \mapsto (z^n+1)x^{1-n}$, $x \mapsto x$, $z \mapsto z$, then α is an isomorphism of k-algebras.
(3) For $i = 1,\dots,n$, the ideal $Q_i = (x, z+\zeta^{2i-1})$ is a height one prime ideal of T.
(4) The divisor of x is $\mathrm{Div}\, x = Q_1 + \cdots + Q_n$.
(5) $\mathrm{Cl}(T) = \mathbb{Z}Q_1 \oplus \cdots \oplus \mathbb{Z}Q_{n-1}$.
(6) Let σ be the $k[x,y]$-algebra automorphism of T defined by $z \mapsto \zeta^2 z$ (see Exercise 1.1.7). Let $G = \langle\sigma\rangle$ and $A = k[x,y]$.
    (a) G is a cyclic group of order n which acts on $\mathrm{Cl}(T)$ by $\sigma Q_1 = -Q_1 - Q_2 - \cdots - Q_{n-1}$, $\sigma Q_2 = Q_1, \dots, \sigma Q_{n-1} = Q_{n-2}$.
    (b) $\mathfrak{p} = \langle x^{n-1}y - 1\rangle$ is a height one prime in A and $\mathfrak{q} = \langle z, x^{n-1}y-1\rangle$ is a height one prime in T.
    (c) For the extension $A \to T$, the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$ is n.
    (d) $\mathrm{Div}(T)^G/\mathrm{Div}(A)$ is a cyclic group of order n generated by $\mathfrak{q}$.
    (e) $\mathrm{Cl}(T)^G = \langle 0\rangle$ (Hint: Exercise 8.5.11).
    (f) In the exact sequence of Theorem 12.5.14 for the extension $A \to T$, the homomorphism $\gamma_1 : \mathrm{H}^1(G,T^*) \to \mathrm{Div}(T)^G/\mathrm{Div}(A)$ is an isomorphism between cyclic groups of order n.

EXERCISE 12.5.2. Let $n \geq 2$ be an integer and k a field in which $2n$ is invertible. Also assume k contains a primitive $2n$th root of unity, ζ. For $T = k[x,y,z]/(z^n - x^{n-1} + y^n)$, prove the following.

(1) T is an integrally closed integral domain.
(2) Let
$$T[x^{-1}] \xrightarrow{\alpha} k[u,v][(u^n+v^n)^{-1}]$$
be the function defined by $x \mapsto (u^n+v^n)^{-1}$, $y \mapsto u(u^n+v^n)^{-1}$, $z \mapsto v(u^n+v^n)^{-1}$. Then α is an isomorphism of k-algebras.
(3) For $i = 1,\dots,n$, let $\ell = z + \zeta^{2i-1}y$. Then the ideal $P_i = (x,\ell_i)$ is a height one prime ideal of T.
(4) In $\mathrm{Div}(T)$ we have $\mathrm{Div}\, x = P_1 + \cdots + P_n$, and $\mathrm{Div}\,\ell_i = (n-1)P_i$.
(5) $\mathrm{Cl}(T)$ is isomorphic to the free $\mathbb{Z}/(n-1)$ module of rank $n-1$, and is generated by $P_1,\dots,P_{n-1}$.
(6) Let σ be the $k[x,y]$-algebra automorphism of T defined by $z \mapsto \zeta^2 z$ (see Exercise 1.1.7). Let $G = \langle\sigma\rangle$ and $A = k[x,y]$.
    (a) G is a cyclic group of order n which acts on $\mathrm{Cl}(T)$ by $\sigma P_1 = -P_1 - P_2 - \cdots - P_{n-1}$, $\sigma P_2 = P_1, \dots, \sigma P_{n-1} = P_{n-2}$.
    (b) $\mathfrak{p} = \langle x^{n-1} - y^n\rangle$ is a height one prime in A and $\mathfrak{q} = \langle z, x^{n-1} - y^n\rangle$ is a height one prime in T.
    (c) For the extension $A \to T$, the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$ is n.

(d) $\mathrm{Div}(T)^G/\mathrm{Div}(A)$ is a cyclic group of order n generated by $\mathfrak{q}$.
(e) $\mathrm{Cl}(T)^G = \langle 0 \rangle$ (Hint: Exercise 8.5.11).
(f) In the exact sequence of Theorem 12.5.14 for the extension $A \to T$, the homomorphism $\gamma_1 : \mathrm{H}^1(G, T^*) \to \mathrm{Div}(T)^G/\mathrm{Div}(A)$ is an isomorphism between cyclic groups of order n.

6. Reflexive Lattices over Regular Domains

In this section R denotes a noetherian regular integral domain with field of fractions K. In Section 12.6.1 we prove that if the ring of endomorphisms of a reflexive R-lattice M is projective, then M is projective. This theorem of Auslander and Goldman was stated without proof in [**18**, Theorem 6.5.10]. In Section 12.6.2 we prove that the Picard group of R is equal to the class group of R. As an application, for any $n \geq 2$, we construct an example of a ring R such that $\mathrm{Cl}(R)$ is a finite cyclic group of order n.

6.1. A Theorem of Auslander and Goldman. The goal of this section is to prove that if a reflexive R-lattice M has a projective ring of endomorphisms, then M is projective (Theorem 12.6.8). The proof given here is essentially the original proof by Auslander and Goldman in [**8**].

THEOREM 12.6.1. *Let R be a noetherian regular integral domain and assume the Krull dimension of R is less than or equal to two. Let M be a finitely generated R-lattice. Then M is reflexive if and only if M is projective.*

PROOF. By Exercise 2.4.6, if M is projective, then M is reflexive. Assume M is a reflexive R-lattice. By Proposition 3.6.2, it suffices to show this when R is a regular local ring. If $\dim(R) = 0$, then R is a field and every R-module is projective. If $\dim(R) = 1$, then R is a DVR (Theorem 11.2.10), and M is free by Proposition 12.1.4. Assume $\dim(R) = 2$. By Proposition 12.1.6, $M^* = R : M$ is an R-lattice. Let

$$0 \to K_0 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M^* \to 0$$

be an exact sequence, where F_0 is a finitely generated free R-module. Apply the functor $\mathrm{Hom}_R(\cdot, R)$ to get the exact sequence

$$0 \to M^{**} \xrightarrow{\varepsilon^*} F_0^* \xrightarrow{d_1^*} K_0^*.$$

By hypothesis, $M = M^{**}$. Since K_0 is an R-submodule of F_0, K_0 is an R-lattice. By Proposition 12.1.6, K_0^* is an R-lattice and we can embed K_0^* in a free R-lattice F_1. If we define N to be the cokernel of $F_0^* \to F_1$, then the sequence

$$0 \to M \xrightarrow{\varepsilon^*} F_0^* \xrightarrow{d_1^*} F_1 \to N \to 0 \tag{6.1}$$

is exact. Since F_0 is free, so is F_0^* (Corollary 2.4.9). By Theorem 11.3.20, $\mathrm{coh.dim}(R) = \dim(R) = 2$. By Theorem 8.4.5, M is projective because it is the first syzygy of (6.1). □

PROPOSITION 12.6.2. *Let R be a noetherian integrally closed local integral domain with maximal ideal $\mathfrak{m}$. If M is a finitely generated R-module such that $\mathrm{Hom}_R(M,M)$ is reflexive and $\mathrm{Ext}^1_R(M,M) = 0$, then $M = M^{**}$.*

PROOF. By Exercise 9.2.15, $\mathrm{Hom}_R(M,M) = \mathrm{Hom}_R(M,M)^{**}$ is torsion free. By Exercise 9.2.13, M is torsion free. In particular, M is an R-lattice. If ν is the natural map and C denotes the cokernel of ν, then

$$0 \to M \xrightarrow{\nu} M^{**} \to C \to 0 \tag{6.2}$$

is an exact sequence. If $\dim(R) \leq 1$, then M is a finitely generated free R-module, hence is reflexive (Exercise 2.4.6). Inductively, assume $d = \dim(R) > 1$ and that the proposition is true for all noetherian integrally closed local integral domains of Krull dimension less than d. For any $\mathfrak{p} \in \operatorname{Spec} R$, if $\operatorname{ht}(\mathfrak{p}) < d$, then by the induction hypothesis, $C_{\mathfrak{p}} = 0$. Therefore, $\operatorname{Supp}_R(C) \subseteq \{\mathfrak{m}\}$ and by Exercise 9.2.14, to show $C = 0$, it suffices to show $\operatorname{Hom}_R(M,C) = 0$. The long exact sequence of Ext modules associated to (6.2) is

$$0 \to \operatorname{Hom}_R(M,M) \xrightarrow{\nu^*} \operatorname{Hom}_R(M,M^{**}) \to \operatorname{Hom}_R(M,C) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(M,M) \to \dots \tag{6.3}$$

(Proposition 8.3.9). Since $\operatorname{Ext}^1_R(M,M) = 0$ by assumption, it suffices to show ν^* is an isomorphism. The reader should verify that the diagram

$$\begin{tikzcd} \operatorname{Hom}_R(M,M) \arrow[r, "\nu^*"] \arrow[d, "="'] & \operatorname{Hom}_R(M,M^{**}) \\ \operatorname{Hom}_R(M,M)^{**} \arrow[r, "\alpha^*"] & (M^* \otimes_R M)^* \arrow[u, "\beta^*"'] \end{tikzcd} \tag{6.4}$$

commutes where α^* and β^* are the isomorphisms of Proposition 12.1.16. $\square$

LEMMA 12.6.3. *Let R be a noetherian commutative local ring with maximal ideal $\mathfrak{m}$. Let M and N be finitely generated R-modules such that $\operatorname{Hom}_R(M,N)$ is nonzero.*

(1) If $\operatorname{depth}(N) \geq 1$, then $\operatorname{depth}(\operatorname{Hom}_R(M,N)) \geq 1$.
(2) If $\operatorname{depth}(N) \geq 2$, then $\operatorname{depth}(\operatorname{Hom}_R(M,N)) \geq 2$.

PROOF. (1): Let x be a regular element for N in $\mathfrak{m}$. Applying the left exact covariant functor $\operatorname{Hom}_R(M,\cdot)$ to the short exact sequence

$$0 \to N \xrightarrow{\ell_x} N \to N/xN \to 0$$

yields the exact sequence

$$0 \to \operatorname{Hom}_R(M,N) \xrightarrow{\mathrm{H}(\ell_x)} \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(M,N/xN).$$

The module $\operatorname{Hom}_R(M,N)$ is finitely generated (Exercise 4.1.8). By Nakayama's Lemma (Corollary 2.2.5), the cokernel of $\mathrm{H}(\ell_x)$ is a nonzero submodule of $\operatorname{Hom}_R(M,N/xN)$. This shows x is a regular element for $\operatorname{Hom}_R(M,N)$.

(2): Let y be a regular element for N/xN in $\mathfrak{m}$. It follows from (1) that y is a regular element for $\operatorname{Hom}_R(M,N/xN)$ and (x,y) is a regular sequence for $\operatorname{Hom}_R(M,N)$ in $\mathfrak{m}$. $\square$

LEMMA 12.6.4. *Let R be a regular local ring of dimension greater than or equal to three. Let M and N be nonzero finitely generated R-modules satisfying*

(1) $\operatorname{depth}(N) \geq 2$,
(2) $\operatorname{Hom}_R(M,N)$ is R-projective, and
(3) $\operatorname{Ext}^1_R(M,N) \neq 0$.

Then $\operatorname{depth}(\operatorname{Ext}^1_R(M,N)) > 0$.

PROOF. Let $n = \dim(R)$, $\mathfrak{m}$ the maximal ideal, and $k = R/\mathfrak{m}$ the residue field. Let $x \in \mathfrak{m}$ a regular element for N. The long exact Ext sequence associated to

$$0 \to N \xrightarrow{\ell_x} N \to N/xN \to 0$$

is

$$(6.5)\quad 0 \to \operatorname{Hom}_R(M,N) \xrightarrow{\mathrm{H}(\ell_x)} \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(M,N/xN) \to \\ \operatorname{Ext}^1_R(M,N) \xrightarrow{\mathrm{H}^1(\ell_x)} \operatorname{Ext}^1_R(M,N) \to \dots$$

(Proposition 8.3.9). Write E for $\operatorname{Ext}^1_R(M,N)$ and assume for contradiction's sake that the depth of E is equal to zero. Since R is noetherian, and M and N are finitely generated, we know that E is finitely generated (Lemma 8.3.10 (2)). Let $\Psi = \{\mathfrak{p} \in \operatorname{Assoc}_R(E) \mid x \notin \mathfrak{p}\}$. Let K denote the kernel of the localization map $\theta : E \to R[x^{-1}] \otimes_R E$. By Proposition 9.2.6, K is the unique submodule of E such that $\operatorname{Assoc}_R(K) = \operatorname{Assoc}_R(E) - \Psi$ and $\operatorname{Assoc}_R(E/K) = \Psi$. By Exercise 11.3.2, $\mathfrak{m}$ is an associated prime of E. Since $x \in \mathfrak{m}$, $\mathfrak{m} \in \operatorname{Assoc}_R(K)$. Since K is a finitely generated R-module, the reader should verify that for some $j > 0$, the kernel of the left multiplication map $\ell_{x^j} : E \to E$ is equal to K. Since $R[x^{-1}] = R[x^{-j}]$, if necessary we replace x with x^j and assume K is equal to the kernel of $\mathrm{H}^1(\ell_{x^j})$ in (6.5). Since $\mathfrak{m} \in \operatorname{Assoc}_R(K)$, by Exercise 11.3.2, $\operatorname{depth}(K) = 0$. Write H for $\operatorname{Hom}_R(M,N)$ and Q for $\operatorname{Hom}_R(M,N/xN)$. The short exact sequence

$$(6.6)\qquad 0 \to H/xH \to Q \to C \to 0$$

of R-modules gives rise to the long exact sequence of the modules $\operatorname{Tor}^R_i(\cdot,k)$

$$(6.7)\quad \cdots \to \operatorname{Tor}_{n+1}(Q,k) \to \operatorname{Tor}_{n+1}(K,k) \to \operatorname{Tor}_n(H/xH,k) \\ \to \operatorname{Tor}_n(Q,k) \to \operatorname{Tor}_n(K,k) \to \operatorname{Tor}_{n-1}(H/xH,k) \to \dots$$

(Lemma 8.3.2). Because H is projective and the sequence $H \to H \to H/xH \to 0$ is exact, $\operatorname{proj.dim}(H/xH) \le 1$. By Proposition 8.4.10, we have $\operatorname{Tor}_i(H/xH,k) = 0$ for $i \ge 2$. Because $n-1 \ge 2$, the sequence (6.7) produces two isomorphisms

$$(6.8)\qquad \begin{aligned} \operatorname{Tor}_{n+1}(Q,k) &\cong \operatorname{Tor}_{n+1}(K,k) \\ \operatorname{Tor}_n(Q,k) &\cong \operatorname{Tor}_n(K,k) \end{aligned}$$

Since R is a regular local ring with dimension n, by Proposition 11.3.28, $\operatorname{proj.dim}(K) = \dim(R) - \operatorname{depth}(K) = n$. By Proposition 8.4.10, we have $\operatorname{Tor}_{n+1}(K,k) = 0$ and $\operatorname{Tor}_n(K,k)$ is nonzero. By Eq. (6.8) and Proposition 8.4.10, $\operatorname{proj.dim}(Q) = n$. By Proposition 11.3.28, $\operatorname{depth}(Q) = \operatorname{depth}(\operatorname{Hom}_R(M,N/xN) = 0$. This is a contradiction to Lemma 12.6.3 (2). □

LEMMA 12.6.5. *Let R be a regular local ring. If M is a finitely generated reflexive R-module such that* $\operatorname{Hom}_R(M,M)$ *is free, then* $\operatorname{Ext}^1_R(M,M) = 0$.

PROOF. The proof is by induction on $n = \dim(R)$. If $\dim(R) \le 2$, then M is projective, by Theorem 12.6.1, and $\operatorname{Ext}^1_R(M,M) = 0$, by Proposition 8.3.9. Assume $n \ge 3$ and that the proposition is true for all rings of dimension less than n. Let $\mathfrak{m}$ be the maximal ideal in R. Let $\mathfrak{p}$ be a prime ideal in $\operatorname{Spec} R - \{\mathfrak{m}\}$. By Corollary 11.3.27, $R_\mathfrak{p}$ is a regular local ring and $\dim(R_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}) < n$. Applying Proposition 3.5.8, the reader should verify that $R_\mathfrak{p}$ together with the module $M_\mathfrak{p} = M \otimes_R R_\mathfrak{p}$ satisfy the hypotheses of the proposition. By Lemma 8.3.10 (3) and the induction hypothesis, $\operatorname{Ext}^1_R(M,M)_\mathfrak{p} = \operatorname{Ext}^1_{R_\mathfrak{p}}(M_\mathfrak{p},M_\mathfrak{p}) = 0$. This proves $\operatorname{Supp}(\operatorname{Ext}^1_R(M,M)) \subseteq \{\mathfrak{m}\}$. For contradiction's sake, assume $\operatorname{Ext}^1_R(M,M) \neq 0$. By Theorem 9.2.7, $\mathfrak{m}$ is the only associated prime of $\operatorname{Ext}^1(M,M)$. By Exercise 11.3.2, this implies $\operatorname{depth}(\operatorname{Ext}^1_R(M,M)) = 0$, which contradicts Lemma 12.6.4. □

LEMMA 12.6.6. *Let R be a noetherian commutative local ring. Let M and N be finitely generated R-modules such that* $\operatorname{proj.dim}(M) = n$ *is finite. Then* $\operatorname{Ext}^n_R(M,N) \neq 0$.

PROOF. By Theorem 8.4.5 and Exercise 8.4.5, there exists a resolution

$$0 \to F_n \xrightarrow{d_n} \cdots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M \to 0$$

such that for all $i \geq 0$, F_i is a finitely generated free R-module and $\operatorname{im} d_{i+1} \subseteq \mathfrak{m}F_i$. By Theorem 8.2.11, there is an exact sequence

$$\operatorname{Hom}_R(F_{n-1}, N) \xrightarrow{H(d_n)} \operatorname{Hom}_R(F_n, N) \to \operatorname{Ext}^n_R(M, N) \to 0.$$

If we write $\operatorname{Rank}_R(F_i) = r_i$, then $\operatorname{Hom}_R(F_i, N) \cong N^{r_i}$. Since the image of d_n is contained in $\mathfrak{m}F_{n-1}$, the image of $H(d_n) : N^{r_{n-1}} \to N^{r_n}$ is contained in $\mathfrak{m}N^{r_n}$. By Nakayama's Lemma (Corollary 2.2.2), $H(d_n)$ is not onto. $\square$

PROPOSITION 12.6.7. *Let R be a regular local ring. Let M be a nonzero finitely generated R-module. Then the following are true.*

(1) *If $\dim(R) \leq 2$, then $M^* = \operatorname{Hom}_R(M, R)$ is a finitely generated free R-module.*
(2) *If $\dim(R) \leq 2$, and $M = M^{**}$, then M is free.*
(3) *If $M = M^{**}$ and $\operatorname{Hom}_R(M, M)$ is free, then M is free.*

PROOF. (1) and (2): Follow directly from Proposition 11.3.28 and Lemma 12.6.3 (or Example 12.1.3 (2), Exercise 12.1.2 and Theorem 12.6.1).

(3): The proof is by induction on $n = \dim(R)$. Part (2) covers the cases $n \leq 2$. We now prove the $n = 3$ case. By Proposition 11.3.28, $\operatorname{depth}(R) = \dim(R) = 3$. Lemma 12.6.3 applied to $M = M^{**}$ gives $\operatorname{depth}(M) \geq 2$. By Proposition 11.3.28, $\operatorname{proj.dim}_R(M) \leq 1$. By Lemma 12.6.5, $\operatorname{Ext}^1_R(M, M) = 0$. Lemma 12.6.6 implies $\operatorname{proj.dim}_R(M) \neq 1$, so we conclude that $\operatorname{proj.dim}_R(M) = 0$, which proves that M is free.

Inductively, assume $n \geq 4$ and that (3) is true for any ring of dimension less than n. Let $\mathfrak{m}$ be the maximal ideal of R. Let $a_1, \dots, a_n$ be a regular system of parameters for R, and take a to be a_1. Since $M = M^{**}$ is torsion free, $\operatorname{Assoc}_R(M) = (0)$ and a is a regular element for M in $\mathfrak{m}$. By Theorem 11.3.20, $\bar{R} = R/aR$ is a regular local ring with Krull dimension $\dim(\bar{R}) = n - 1$. Let $\bar{M} = M/aM$. The short exact sequence $0 \to M \xrightarrow{\ell_a} M \to \bar{M} \to 0$ gives rise to the long exact sequence

$$0 \to \operatorname{Hom}_R(M, M) \xrightarrow{\mathrm{H}(\ell_a)} \operatorname{Hom}_R(M, M) \to \operatorname{Hom}_R(M, \bar{M}) \xrightarrow{\partial} \operatorname{Ext}^1_R(M, M)$$

(Proposition 8.3.9). By Lemma 12.6.5, $\operatorname{Ext}^1_R(M, M) = 0$, so we have the isomorphism of $\bar{R}$-modules $\operatorname{Hom}_R(M, M) \otimes_R \bar{R} \cong \operatorname{Hom}_R(M, \bar{M})$. Since $\operatorname{Hom}_R(M, M)$ is a free R-module, $\operatorname{Hom}_R(M, \bar{M})$ is a free $\bar{R}$-module. By Theorem 2.4.10 (the Adjoint Isomorphism),

$$\operatorname{Hom}_{\bar{R}}(\bar{M}, \bar{M}) \cong \operatorname{Hom}_R(M, \bar{M})$$

hence both modules are $\bar{R}$-free. By Exercise 9.2.13, $\bar{M}$ is torsion free. By Proposition 12.1.16,

$$\operatorname{Hom}_{\bar{R}}(\bar{M}, \bar{M}) = \operatorname{Hom}_{\bar{R}}(\bar{M}, \bar{M})^{**} \cong \operatorname{Hom}_{\bar{R}}(\bar{M}^*, \bar{M}^*)$$

is $\bar{R}$-free. By Lemma 12.1.9, $\bar{M}^*$ is reflexive. By our induction hypothesis applied to $\bar{R}$ and $\bar{M}^*$, we conclude that $\bar{M}^*$ is $\bar{R}$-free.

Now $\operatorname{depth}(\bar{R}) = \dim(\bar{R}) = n - 1 \geq 3$ and $\operatorname{Hom}_{\bar{R}}(\bar{M}, \bar{R}) = \bar{M}^*$ is $\bar{R}$-free. If follows from Lemma 12.6.4, that the statement:

$$\text{If } \operatorname{Ext}^i_{\bar{R}}(\bar{M}, \bar{R}) \neq 0, \text{ then } \operatorname{depth}(\operatorname{Ext}^i_{\bar{R}}(\bar{M}, \bar{R})) > 0. \tag{6.9}$$

is true. The Adjoint Isomorphism (Lemma 8.3.11) induces isomorphisms

$$\operatorname{Ext}^i_{\bar{R}}(\bar{M}, \bar{R}) \cong \operatorname{Ext}^i_R(M, \bar{R}) \tag{6.10}$$

for all $i \geq 0$. Therefore, the statement:

$$\text{If } \operatorname{Ext}^i_R(M,\bar{R}) \neq 0, \text{ then } \operatorname{depth}(\operatorname{Ext}^i_R(M,\bar{R})) > 0. \tag{6.11}$$

is equivalent to (6.9). The short exact sequence

$$0 \to R \xrightarrow{\ell_a} R \to \bar{R} \to 0 \tag{6.12}$$

gives rise to the long exact sequence

$$0 \to M^* \xrightarrow{\ell_a^*} M^* \to \operatorname{Hom}_R(M,\bar{R}) \xrightarrow{\partial} \operatorname{Ext}^1_R(M,R) \xrightarrow{\ell_a^*} \operatorname{Ext}^1_R(M,R) \to \operatorname{Ext}^1_R(M,\bar{R})$$

(Proposition 8.3.9). Let $\mathfrak{p} \in \operatorname{Spec} R - \{\mathfrak{m}\}$. By Lemma 8.3.10,

$$\operatorname{Ext}^1_R(M,R)_\mathfrak{p} \cong \operatorname{Ext}^1_{R_\mathfrak{p}}(M_\mathfrak{p},R_\mathfrak{p}). \tag{6.13}$$

Our induction hypothesis applied to $R_\mathfrak{p}$ and $M_\mathfrak{p}$ implies that $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module. By Proposition 8.3.9, both groups in (6.13) are trivial. This proves that $\operatorname{Supp}(\operatorname{Ext}^1_R(M,R)) \subseteq \{\mathfrak{m}\}$. For contradiction's sake assume that $\operatorname{Ext}^1_R(M,R)) \neq (0)$. Since $a \in \mathfrak{m}$, the image of

$$\operatorname{Ext}^1_R(M,R) \xrightarrow{\ell_a^*} \operatorname{Ext}^1_R(M,R)$$

is contained in $\mathfrak{m}\operatorname{Ext}^1_R(M,R)$. By Lemma 8.3.10 the module $\operatorname{Ext}^1_R(M,R)$ is finitely generated. By Nakayama's Lemma, $\operatorname{coker}(\ell_a^*)$ is a nontrivial submodule of $\operatorname{Ext}^1_R(M,\bar{R})$. Since

$$\operatorname{Supp}(\operatorname{coker}(\ell_a^*)) \subseteq \operatorname{Supp}(\operatorname{Ext}^1_R(M,R)) \subseteq \{\mathfrak{m}\}$$

it follows from Theorem 9.2.7 that $\mathfrak{m}$ is the only associated prime of $\operatorname{Ext}^1_R(M,\bar{R})$. By Exercise 11.3.2, this implies $\operatorname{depth}(\operatorname{Ext}^1_R(M,\bar{R})) = 0$, which is a contradiction to the statement in (6.11). This shows that $Ext^1(M,R) = 0$, so the sequence

$$0 \to M^* \xrightarrow{\ell_a^*} M^* \to \operatorname{Hom}_R(M,\bar{R}) \to 0$$

is exact. As mentioned in (6.10), $\operatorname{Hom}_{\bar{R}}(\bar{M},\bar{R}) \cong \operatorname{Hom}_R(M,\bar{R})$. Since $\bar{M}^*$ is $\bar{R}$-free, this proves M^*/aM^*, which is isomorphic to $\operatorname{Hom}_R(M,\bar{R})$, is also $\bar{R}$-free. We know that $\operatorname{proj.dim}_R(\bar{R}) = 1$ (for instance, by the exact sequence (6.12)), hence $\operatorname{proj.dim}_R(M^*/aM^*) = 1$. By Proposition 8.4.10, $\operatorname{proj.dim}_R(M^*) = 0$, hence M^* is R-free. Therefore, $M = M^{**}$ is R-free. □

THEOREM 12.6.8. *Let R be a noetherian regular integral domain with field of fractions K. Let V be a finite dimensional K-vector space and M an R-lattice in V. If M is R-reflexive and* $\operatorname{Hom}_R(M,M)$ *is R-projective, then M is R-projective.*

PROOF. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then $R_\mathfrak{p}$ is a regular local ring (Corollary 11.3.27). By Proposition 3.5.8 we see that $M_\mathfrak{p}$ is $R_\mathfrak{p}$-reflexive and $\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p},M_\mathfrak{p})$ is $R_\mathfrak{p}$-free. By Proposition 12.6.7, $M_\mathfrak{p}$ is $R_\mathfrak{p}$-free. □

6.2. The Class Group of a Regular Domain.

THEOREM 12.6.9. *Let R be a noetherian regular integral domain with field of fractions K. Then the following are true.*

(1) $\operatorname{Pic}(R) = \operatorname{Cl}(R)$.
(2) If R is a local ring, then $\operatorname{Cl}(R) = (0)$ *and R is a unique factorization domain.*
(3) If R is a semilocal ring, then $\operatorname{Cl}(R) = (0)$ *and R is a unique factorization domain.*

PROOF. (1): Let F be a reflexive fractional ideal of R in K. It follows from Exercise 12.4.7 that $F : F = R$ is free of rank one. By Theorem 12.6.8, F is projective. The equality $\mathrm{Pic}(R) = \mathrm{Cl}(R)$ follows from Exercise 12.4.10.

(2) and (3): For any local ring the Picard group is trivial since a finitely generated projective module is free, by Proposition 3.4.2. The same is true for finitely generated projective modules of constant rank over a semilocal ring, by Exercise 4.2.5. By (1), the class group, $\mathrm{Cl}(R)$, is trivial. By Corollary 11.4.13, R is a UFD. □

EXAMPLE 12.6.10. In this example we show how to construct a regular integral domain R such that $\mathrm{Pic}(R)$ is a finite cyclic group of order n. The example comes from Algebraic Geometry and is based on the fact that if k is a field, then the class group of the projective plane $\mathbb{P}^2_k$ is an infinite cyclic group and is generated by a line. For simplicity's sake we construct our example using the projective plane. However, the same ideas apply in higher dimensions. Start with any field k and any integer $n > 1$. Let

$$S = k[x,y,z] = S_0 \oplus S_1 \oplus S_2 \oplus \cdots \oplus S_n \oplus \cdots$$

be the polynomial ring in three variables, with the usual grading (Example 7.2.1). Let $f \in S_n$ be a homogeneous irreducible polynomial of degree n. The localized ring $S[f^{-1}]$ has a $\mathbb{Z}$-grading: $S[f^{-1}] = \bigoplus_{i\in\mathbb{Z}} S[f^{-1}]_i$. If $p \in S_m$ is homogeneous of degree m, then pf^{-d} is a typical homogeneous element of degree $m - dn \in S[f^{-1}]_i$. Let $R = S[f^{-1}]_0$ be the subring of homogeneous elements in $S[f^{-1}]$ of degree 0. We will show the following.

(1) R is a finitely generated k-algebra, a regular noetherian integral domain, and the Krull dimension of R is $\dim(R) = 2$.
(2) $\mathrm{Pic}(R) = \mathrm{Cl}(R) \cong \mathbb{Z}/n$.
(3) $R^* = k^*$.

A typical element of R is a fraction pf^{-d} where $p \in S_{dn}$. Since R is a subring of the field $k(x,y,z)$, R is an integral domain. Since f is irreducible and has degree $n \geq 2$, $f(0,y,z)$ is a homogeneous polynomial in $k[y,z]$ of degree n. Therefore, the homomorphism $k[x,y,z] \to k[y,z]$ defined by $x \mapsto 0$ induces

$$R = S[f^{-1}]_0 \xrightarrow{\theta} k[y,z][(f(0,y,z))^{-1}]_0.$$

Notice that θ is onto, and since the image is an integral domain, $\mathfrak{p} = \ker(\theta)$ is a prime ideal in R. Consider the local ring $R_\mathfrak{p}$. We will now show that $R_\mathfrak{p}$ is a DVR and x/y is a local parameter. If $h + i + j = dn$, then the monomial $x^h y^i z^j f^{-d}$ is in the kernel of θ if and only if $h \geq 1$. Then

$$\frac{x^h y^i z^j}{f^d} \frac{f^d}{y^{h+i} z^j} = \frac{x^h}{y^h} \tag{6.14}$$

shows $\mathfrak{p}R_\mathfrak{p}$ is generated by x/y. This also proves that $\mathrm{ht}(\mathfrak{p}) = 1$. Notice that in $S[f^{-1}]$, which is a UFD, the element $x^n f^{-1}$ belongs to the unique minimal prime ideal $(x) = (xf^{-1})$. Viewing R as a subring of $S[f^{-1}]$, we see that $x^n f^{-1}$ is irreducible in R, and $\mathfrak{p}$ is the unique minimal prime of R containing $x^n f^{-1}$. Using (6.14) we compute

$$\nu_\mathfrak{p}(x^n f^{-1}) = n. \tag{6.15}$$

Consider the localized ring $R[fx^{-n}]$. Given $p \in S_{dn}$ we multiply and divide by $(x^n f^{-1})^d$ to get

$$\begin{aligned} pf^{-d} &= (px^{-dn} f^d)(fx^{-n})^{-d} f^{-d} \\ &= p(1, y/x, z/x)\,(f(1, y/x, z/x))^{-d}. \end{aligned}$$

Therefore, the assignments $x \mapsto 1$, $y \mapsto u$, $z \mapsto v$ induce an isomorphism of k-algebras

$$R[fx^{-n}] \to k[u,v][(f(1,u,v))^{-1}]. \tag{6.16}$$

The homomorphism in (6.16) is usually specified by saying "dehomogenize with respect to x". Notice that the ring on the right hand side of (6.16) is a finitely generated k-algebra, a regular integral domain, and has Krull dimension two. By the same argument used in (6.16), but dehomogenizing with respect to y and z, the reader should verify that $R[fy^{-n}]$ and $R[fz^{-n}]$ are finitely generated regular integral k-algebras of Krull dimension two. For some $N > 0$, f^N is a sum of monomials of the form $x^h y^i z^j$ where at least one of h,i,j is greater than n. Therefore, $1 = f^N f^{-N}$ is in the ideal of R generated by $x^n f^{-1}, y^n f^{-1}, z^n f^{-1}$. This shows that $R[fx^{-n}] \oplus R[fy^{-n}] \oplus R[fz^{-n}]$ is a faithfully flat extension of R (Exercise 3.5.13) By Proposition 3.5.16, R is finitely generated as a k-algebra. For each prime ideal $P \in \operatorname{Spec} R$, the local ring R_P is regular and has dimension two. This proves (1). Since $f(x,y,z)x^{-n} = f(1, yx^{-1}, zx^{-1})$, we see that $f(1,u,v)$ is irreducible because $f(x,y,z)$ is irreducible. Applying Nagata's Theorem (Theorem 11.4.14) to the ring R, the sequence

$$1 \to R^* \to (R[fx^{-n}])^* \xrightarrow{\text{Div}} \mathbb{Z}\mathfrak{p} \to \operatorname{Cl}(R) \to \operatorname{Cl}(R[fx^{-n}]) \to 0 \tag{6.17}$$

is exact. By the isomorphism in (6.16), we see that $R[fx^{-n}]$ is a UFD. Hence $\operatorname{Cl}(R[fx^{-n}])$ is equal to (0) by Corollary 11.4.13. Using (6.16) and the fact that $k[u,v]$ is a UFD, we see that

$$(R[fx^{-n}])^* = k^* \times \langle x^n f^{-1} \rangle$$

is an internal direct sum. This and (6.15) shows that the image of Div in (6.17) is $n\mathbb{Z}\mathfrak{p}$. Therefore, $\operatorname{Cl}(R)$ is generated by $\mathfrak{p}$ and has order n. Part (2) follows from Theorem 12.6.9, and the reader is asked to prove Part (3) in Exercise 12.6.1.

6.3. Exercise.

EXERCISE 12.6.1. If R is the ring of Example 12.6.10, prove the following.

(1) $R^* = k^*$.
(2) $\mathfrak{p}^n$ is equal to the principal ideal generated by $x^n f^{-1}$.

7. The Class Group of a Graded Ring

Most of the results in this section were originally published in [**53**]. For additional results on this subject, the interested reader is referred to [**53**], [**21**, § 10], and [**46**, § B.II.1]. Throughout this section all rings are commutative. The reader is referred to Section 7.2 for the definitions of graded rings and modules. Let $R = \oplus_{n=0}^{\infty} R_n$ be a graded integral domain and $W = R^h - \{0\}$ the set of nonzero homogeneous elements. The localization $W^{-1}R$ is viewed as a subring of the quotient field K of R. An element aw^{-1} in $W^{-1}R$ is said to be *homogeneous* if $a \in R^h$ and $w \in W$. The *degree* of a homogeneous element aw^{-1} is defined to be $\deg a - \deg w$. The reader should verify:

(1) The degree function is well defined on homogeneous elements.
(2) The sum of two homogeneous elements of the same degree d is homogeneous of degree d.
(3) The product of a homogeneous element of degree d with a homogeneous element of degree e is homogeneous of degree $d+e$.
(4) Every element of $W^{-1}R$ can be written uniquely as a finite sum of homogeneous elements of different degrees.

LEMMA 12.7.1. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a graded integral domain and $W = R^h - \{0\}$. Then the following are true.*

(1) *$W^{-1}R$ is a $\mathbb{Z}$-graded ring, a graded R-module and contains R as a graded subring. If $K_0 = \left(W^{-1}R\right)_0$ is the subring consisting of all homogeneous elements of degree zero, then K_0 is a field.*
(2) *If $R \neq R_0$, then $W^{-1}R$ is isomorphic to the Laurent polynomial ring $K_0[t,t^{-1}]$.*

PROOF. (1): Is left to the reader.
(2): Since $R \neq R_0$, K_0 is not equal to $W^{-1}R$. Therefore, the set

$$\{\deg a - \deg w \mid a \in R^h, w \in W\}$$

contains nonzero integers. Let $t = aw^{-1} \in W^{-1}R$, be a homogeneous element of minimal positive degree. That is, $\deg a > \deg w$ and $d = \deg a - \deg w$ is minimal. The proof is a series of three steps.

Step 1: Show that $t = aw^{-1}$ is transcendental over K_0. Suppose we have an integral relation

$$\alpha_0 t^r + \alpha_1 t^{r-1} + \cdots + \alpha_{r-1} t + \alpha_r = 0 \tag{7.1}$$

where each $\alpha_i \in K_0$. Write $\alpha_i = a_i w_i^{-1}$, where $\deg a_i = \deg w_i$. Let $y = w_0 w_1 \cdots w_r$ and set $y_i = y w_i^{-1}$. Then $\alpha_i = a_i y_i y^{-1}$. If we set $b_i = a_i y_i$, then $\deg b_i = \deg y$ for each i. Upon multiplying both sides of (7.1) by yw^r, we get

$$b_0 a^r + b_1 w a^{r-1} + \cdots + b_{r-1} w^{r-1} a + b_r w^r = 0 \tag{7.2}$$

which is a relation in R. The left hand side of (7.2) is a sum of homogeneous elements. Since $\deg a^r > \deg wa^{r-1} > \cdots > \deg w^{r-1}a > \deg w^r$, no two terms in (7.2) have the same degree. Therefore, $b_i = 0$ for all i. This implies $\alpha_i = 0$ for all i.

Step 2: Since t is transcendental over K_0, we have $K_0[t] \subseteq W^{-1}R$. In the quotient field of R we have the chain of subrings: $K_0 \subseteq K_0[t] \subseteq K_0[t,t^{-1}] \subseteq K_0(t)$. Since $\deg a > 0$, it follows that $a \in W$. Hence $t^{-1} = wa^{-1} \in W^{-1}R$. Therefore, we have $K_0[t,t^{-1}] \subseteq W^{-1}R$.

Step 3: Show that $W^{-1}R = K_0[t,t^{-1}]$. Suppose $x \in R^h$, $y \in W$, and $\deg x - \deg y = m$. By the division algorithm, there exist integers q, r, such that $m = qd + r$ and $0 \le r < d$. Then

$$(\deg x - \deg y) - q(\deg a - \deg w) = m - qd = r.$$

Since t was chosen so that d is minimal, this implies the homogeneous element $xy^{-1}t^{-q}$ is of degree zero. That is, $z = xy^{-1}t^{-q} \in K_0$, which implies $xy^{-1} = t^q z \in K_0[t,t^{-1}]$. Since every element of $W^{-1}R$ is a sum of homogeneous terms of the form xy^{-1}, this shows $W^{-1}R \subseteq K_0[t,t^{-1}]$. □

PROPOSITION 12.7.2. *If $R = \oplus_{n=0}^{\infty} R_n$ is a graded noetherian integrally closed integral domain, then the natural map $\operatorname{Div}_h(R) \to \operatorname{Cl}(R)$ is onto, where $\operatorname{Div}_h(R)$ is the subgroup of $\operatorname{Div}(R)$ generated by those prime ideals in $X_1(R)$ which are homogeneous.*

PROOF. Let $W = R^h - \{0\}$. By Lemma 12.7.1, $W^{-1}R = K_0[t,t^{-1}]$. Since $K_0[t]$ is factorial, so is the localization $W^{-1}R = K_0[t,t^{-1}]$. By Exercise 11.4.4, $\operatorname{Cl}(R)$ is generated by the classes of those prime divisors $\mathfrak{p} \in X_1(R) - X_1(W^{-1}R)$. Let $\mathfrak{p}$ be a prime ideal in R of height one and assume $\mathfrak{p} \cap W \neq \emptyset$. Then $\mathfrak{p}$ is homogeneous, by Lemma 9.5.2 (4). □

LEMMA 12.7.3. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a graded noetherian integral domain with field of fractions K. Let F be a fractional ideal of R in K which is a graded R-submodule of $W^{-1}R$. Then the following are true.*

(1) *There is a nonzero homogeneous $r \in R^h$ such that $rF \subseteq R$.*
(2) *$F^{-1} = R : F$ is a fractional ideal of R in K and a graded R-submodule of $W^{-1}R$.*

PROOF. (1): By Lemma 12.2.1, there exists $c \in R-(0)$ such that $cF \subseteq R$. Write $c = c_0 + c_1 + \cdots + c_d$ as a sum of homogeneous elements, and assume $c_d \neq 0$. Let $y \in F^h - (0)$ be a nonzero homogeneous element of F. By Lemma 12.7.1, R is a graded subring of $W^{-1}R$. Since $cy = (c_0 + c_1 + \cdots + c_d)y$ is in R, it follows that $c_d y \in R$. If we set $r = c_d$, then $rF \subseteq R$.

(2): By Proposition 12.1.6, F^{-1} is a fractional ideal of R in K. By (1), there is $r \in R^h - \{0\}$ such that $rF \subseteq F \cap R$. Then there exists $s \in F \cap R^h$, $s \neq 0$. If $t \in F^{-1}$, then $ts = x$ is an element of R. Since $s \in W$, we see that $t = xs^{-1}$ is in $W^{-1}R$. This shows F^{-1} is an R-submodule of $W^{-1}R$. Write $t = t_1 + t_2 + \cdots + t_d$ as a sum of homogeneous elements in $W^{-1}R$, where $\deg t_i = d_i$. Then for each homogeneous element $y \in F^h$, we have $ty = t_1 y + t_2 y + \cdots + t_d y$ is in R. By Lemma 12.7.1, R is a graded subring of $W^{-1}R$. Therefore, $t_i y \in R$, for each i. Since y was arbitrary, this implies $t_i \in F^{-1}$, for each i. Therefore, F^{-1} is a graded R-submodule of $W^{-1}R$. □

COROLLARY 12.7.4. *Let $R = \oplus_{n=0}^{\infty} R_n$ be a graded noetherian integrally closed integral domain. If R_0 is a field and hence, the exceptional ideal $\mathfrak{m} = R_+ = \bigoplus_{n=1}^{\infty} R_n$ is maximal, then the natural homomorphism $\mathrm{Cl}(R) \to \mathrm{Cl}(R_{\mathfrak{m}})$ is an isomorphism.*

PROOF. The natural map $\gamma : \mathrm{Cl}(R) \to \mathrm{Cl}(R_{\mathfrak{m}})$ is onto, by Exercise 11.4.4. Let K be the field of fractions of R and I a reflexive fractional ideal of R in K. To show that γ is one-to-one, we prove that if $I_{\mathfrak{m}}$ is principal, then I is principal. By Proposition 12.7.2, we can assume I is in the subgroup of $\mathrm{Reflex}(R)$ generated by the homogeneous prime ideals of R in $X_1(R)$. The reader should verify that the product of two fractional ideals of R which are graded R-submodules of $W^{-1}R$ is again a graded R-submodule of $W^{-1}R$. Using this, and Lemma 12.7.3 (2), we see that if I is in the subgroup of $\mathrm{Reflex}(R)$ generated by the homogeneous prime divisors, then I is a graded R-submodule of $W^{-1}R$. By

Now let I be a reflexive fractional ideal of R which is a graded R-submodule of $W^{-1}R$ and assume $I_{\mathfrak{m}}$ is principal. We show that I is principal. By Lemma 12.7.3 (1), we can assume $I \subseteq R$. If $\xi_1, \dots, \xi_s$ is a set of homogeneous elements of I which generate I as an R-module, then the vector space $I_{\mathfrak{m}} \otimes R/\mathfrak{m}$ has dimension one and is generated by the image of one of the elements ξ_i. By Proposition 3.4.2, $I_{\mathfrak{m}}$ is generated by the image of the same element ξ_i. Let $\xi \in I$ be a homogeneous element such that $I_{\mathfrak{m}} = \xi R_{\mathfrak{m}}$. Let x be any nonzero homogeneous element of I. Then $x = \xi(yz^{-1})$ for some $y \in R - \{0\}$, $z \in R - \mathfrak{m}$. Write $y = y_q + y_{q+1} + \cdots + y_{q+d}$ and $z = z_0 + z_1 + \cdots + z_e$ as sums of homogeneous elements. Since $y \neq 0$, assume $y_q \neq 0$. Since $z \in R - R_+$, we know that $z_0 \neq 0$. Then $xz = \xi y$ implies that the relation

$$xz_0 + xz_1 + \cdots + xz_e = \xi y_q + \xi y_{q+1} + \cdots + \xi y_{q+d}$$

holds in the graded module I. Therefore, $xz_0 = \xi y_q$. Since R_0 is a field, z_0 is invertible in R. Therefore, $x = \xi(y_q z_0^{-1})$ is an element of ξR. Since I is generated by homogeneous elements, this shows $I = \xi R$. □

8. The Ring of Integers in a Global Field

In this section we prove two main results from classical Algebraic Number Theory. A field L is said to be a *global field*, if one of the following is true:

(1) L is a finitely generated algebraic extension field of $\mathbb{Q}$ and B is the integral closure of $\mathbb{Z}$ in K. In this case we also say L is an *algebraic number field* and B is the *ring of algebraic integers in L.*

(2) $k[t]$ is the ring of polynomials in one variable over a finite field k, $k(t)$ is the field of rational functions, L is a finitely generated separable extension field of $k(t)$, and B is the integral closure of $k[t]$ in L. In this case we also say L is the *function field of an algebraic curve over the finite field* k and B is called the *ring of integers in* L.

Notice that in (2) the ring of integers B depends not only on the field L but also on the choice of t.

Let L be a global field and B the ring of integers in L. By Corollary 6.1.8, L is the quotient field of B. In Section 8.1 we show that the class group of the ring B is finite. This is proved in Theorem 12.8.8. In Section 8.2 we assume B is the ring of integers in an algebraic number field. In this case, we show that B^*, the group of units in B, is a finitely generated abelian group. The torsion subgroup of B^* is a cyclic group.

This is half of the Dirichlet Units Theorem. The second half of Dirichlet's theorem, which we do not prove here, describes the rank of the torsion free part of B^*.

8.1. The Class Group of a Global Field is Finite. In this section we show that if R is the ring of integers in a global field, then R is a Dedekind domain (Proposition 12.8.3) and the class group of R is a finite abelian group (Theorem 12.8.8). The proof we give is based on [**57**] and [**15**, §20]. For the remainder of this section, let A be either $\mathbb{Z}$ or $k[t]$, where k is a fixed finite field of order q. Let K be the quotient field of A, L a global field which is a finitely generated separable extension field of K, and B the ring of integers in L. The ring A is a UFD, hence is integrally closed in K (Proposition 6.1.5). Hence K is itself a global field with ring of integers A.

LEMMA 12.8.1. *In the above context, let V be a finite dimensional K-vector space, and $M_1 \subseteq M_2$ a tower of A-lattices in V. Then the following are true.*

(1) Each M_i is a finitely generated free A-module and $\operatorname{Rank}_A(M_i) = \dim_K(V)$.

(2) The index $[M_2 : M_1]$ is finite. The group M_2/M_1 is a finite abelian group.

(3) There are only finitely many A-lattices M such that $M_1 \subseteq M \subseteq M_2$.

PROOF. (1): Since A is a PID, this follows from Proposition 12.1.4.

(2): By Proposition 12.1.1 there exists an element $\alpha \in A - (0)$ such that $\alpha M_2 \subseteq M_1 \subseteq M_2$. By (1), $M_2/\alpha M_2$ is isomorphic to the direct sum of $\dim_K(V)$ copies of the cyclic A-module $A/\alpha A$. If $A = \mathbb{Z}$, then the group $A/\alpha A$ is finite of order $|\alpha|$. If $A = k[t]$, then by Example 1.6.10 (2), $A/\alpha A$ is a k-vector space of dimension $\deg \alpha$. The group $A/\alpha A$ has order $q^{\deg \alpha}$. The rest follows from Lagrange's Theorem, Theorem 1.1.1.

(3): By Proposition 12.1.1, any A-module M such that $M_1 \subseteq M \subseteq M_2$ is an A-lattice in V. This follows from (2) and Theorem 1.1.12 (3). □

In the above context, if I is a nonzero ideal in A, then as seen in Lemma 12.8.1 (2), the index $[A : I]$ is finite. Let $N_A : A \to \mathbb{N} \cup \{0\}$ be the function defined by

$$N_A(\alpha) = \begin{cases} 0 & \text{if } \alpha = 0 \\ [A : \alpha A] & \text{if } \alpha \neq 0. \end{cases}$$

Suppose $\alpha \neq 0$. The proof of Lemma 12.8.1 (2) shows that

$$N_A(\alpha) = \begin{cases} |\alpha| & \text{if } A = \mathbb{Z} \\ q^{\deg \alpha} & \text{if } A = k[t]. \end{cases}$$

LEMMA 12.8.2. *In the above context, the function $N_A : A \to \mathbb{N} \cup \{0\}$ satisfies:*

(1) If $m \in \mathbb{N}$ and $\Xi = \{\alpha \in A \mid N_A(\alpha) \leq m\}$, then Ξ is a finite set and $|\Xi| \geq m$.

(2) *If* $\alpha, \beta \in A$, *then* $N_A(\alpha\beta) = N_A(\alpha)N_A(\beta)$ *and* $N_A(\alpha+\beta) \le N_A(\alpha)+N_A(\beta)$.
(3) *If* $\alpha \in A^*$, *then* $N_A(\alpha) = [A : \alpha A] = 1$.

PROOF. Part (3) is left to the reader. The proofs of (1) and (2) are split into two cases.
First assume $A = \mathbb{Z}$. The set $\Xi = \{\alpha \in \mathbb{Z} \mid |\alpha| \le m\}$ has cardinality $2m+1$, which proves (1). Part (2) follows from the fact that on $\mathbb{Z}$ the absolute value function satisfies $|\alpha\beta| = |\alpha||\beta|$ and $|\alpha+\beta| \le |\alpha|+|\beta|$.

If $A = k[t]$ and $\alpha \in A$, then $N_A(\alpha) = q^{\deg\alpha} \le m$ if and only if $\deg\alpha \le \log_q(m)$. If i is the unique integer such that $q^i \le m < q^{i+1}$, then $i \le \log_q(m) < i+1$ and the set $\Xi = \{\alpha \in A \mid \deg(\alpha) < i+1\}$ has cardinality q^{i+1}. Since $q^{i+1} \ge m$, this proves (1). Part (2) is obviously true if one or more of α, β, or $\alpha+\beta$ is equal to 0. Otherwise,

$$N_A(\alpha\beta) = q^{\deg(\alpha\beta)} = q^{\deg(\alpha)+\deg(\beta)} = q^{\deg(\alpha)}q^{\deg(\beta)} = N_A(\alpha)N_A(\beta)$$

and

$$N_A(\alpha+\beta) = q^{\deg(\alpha+\beta)} \le q^{\max(\deg(\alpha),\deg(\beta))} \le q^{\deg(\alpha)} + q^{\deg(\beta)} = N_A(\alpha)+N_A(\beta).$$

□

PROPOSITION 12.8.3. *In the above context, let L be a global field and B the ring of integers in L. Then the following are true.*

(1) *B is a Dedekind domain with quotient field L.*
(2) *B is a finitely generated A-lattice in L, hence is a free A-module of rank* $\dim_K(L)$.
(3) *If* $A = k[t]$, *then B is a finitely generated k-algebra.*

PROOF. Part (1) follows from Theorem 12.3.7. Parts (2) and (3) follow from Theorem 6.1.13, Lemma 12.8.1, and Exercise 1.1.6. □

As above, A is either $\mathbb{Z}$ or $k[t]$, where k is a fixed finite field of order q. The quotient field of A is denoted K. Let Λ be a finite dimensional K-algebra. Assume Λ is a domain. By Lemma 6.1.4, this is equivalent to assuming Λ is a division ring. We say Λ is a finite dimensional *K-division algebra*. Let B be an A-subalgebra of Λ which is also an A-lattice in Λ. We call the ring B an *A-order in* Λ.

By Lemma 12.8.1, B is a free A-module of rank $n = \dim_K(\Lambda)$. If $u_1,\dots,u_n$ is an A-basis for B, then $u_1,\dots,u_n$ is also a K-basis for Λ. As in Example 6.2.13, the norm $N_K^\Lambda : \Lambda \to K$ is a homogeneous polynomial function on Λ of degree n. With respect to the basis $u_1,\dots,u_n$ we can identify Λ with affine n-space over K. Under this identification, the norm $N_K^\Lambda : \Lambda \to K$ corresponds to a homogeneous polynomial $F(x_1,\dots,x_n)$ in $K[x_1,\dots,x_n]$ of degree n. Given a point $(s_1,\dots,s_n)$ in K^n, we have the element $\beta = s_1u_1+\cdots+s_nu_n$ in Λ, and ℓ_β is the "left multiplication by β" map on Λ. Then $F(s_1,\dots,s_n)$ is equal to $N_K^\Lambda(\beta)$, which is the determinant $\det(\ell_\beta)$. The norm $N_K^\Lambda : \Lambda \to K$ restricts to a norm $N_A^B : B \to A$ (Exercise 1.7.2).

The formula derived in Lemma 12.8.4 below bears an interesting resemblance to that of Exercise 1.7.4 (2).

LEMMA 12.8.4. *In the above context, let* β *be a nonzero element in B. Then the right ideal* βB *is an A-submodule of B of finite index and* $[B : \beta B] = N_A(N_A^B(\beta)) = |\det(\ell_\beta)|$.

PROOF. By Lemma 12.8.1, the index $[B : \beta B]$ is finite. By the Simultaneous Bases Theorem (Corollary 1.7.20), there is a basis $u_1,\dots,u_n$ for B over A and elements $\delta_1,\dots,\delta_n$

in $A-(0)$ such that $\beta u_i = \delta_i u_i$ for each i and $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_n$. Then $\det(\ell_\beta)) = \delta_1\delta_2\cdots\delta_n$. The sequence of A-modules

$$0 \to B \xrightarrow{\beta} B \to B/\beta B \to 0$$

is exact and $B/\beta B$ is isomorphic to the direct sum $A/\delta_1 A \oplus \cdots \oplus A/\delta_n A$ of cyclic A-modules. The group $A/\delta_i A$ has order $N_A(\delta_i)$. By Lemma 12.8.2, N_A is multiplicative. Therefore $[B:\beta B] = N_A(\delta_1)\cdots N_A(\delta_n) = N_A(\delta_1\cdots\delta_n) = N_A(\det(\ell_\beta)) = N_A(N_A^B(\beta))$ $\square$

LEMMA 12.8.5. *In the above context, let $u_1,\dots,u_n$ be an A-basis for B and $F(x_1,\dots,x_n)$ the homogeneous polynomial of degree n in $A[x_1,\dots,x_n]$ associated to the norm map $N_A^B : B \to A$. Then there is a constant $U \in \mathbb{N}$ such that for every $\varepsilon \in \mathbb{N}$, if $0 \le s_i \le \varepsilon$ for each $1 \le i \le n$ and $\beta = s_1u_1 + \cdots + s_nu_n$, then $[B:\beta B] \le \varepsilon^n U$.*

PROOF. As in [**19**, Section 3.6.1], write F as a linear combination of monomials of degree n: $F(x_1,\dots,x_n) = \sum_{i=1}^r a_i x_1^{e_{i,1}}\cdots x_n^{e_{i,n}}$, where $a_i \in A$, $e_{i,j} \in \mathbb{N}\cup\{0\}$, and $e_{i,1}+\cdots+e_{i,n} = n$ for every i. Let $U = \sum_{i=1}^r N_A(a_i)$ and assume $\varepsilon \in \mathbb{N}$, $(s_1,\dots,s_n) \in A^n$, $N_A(s_i) \le \varepsilon$ for each $1 \le i \le n$, and $\beta = s_1u_1+\cdots+s_nu_n$. Using Lemmas 12.8.4 and 12.8.2, we have

$$\begin{aligned}
[B:\beta B] &= N_A(N_A^B(\beta)) \\
&= N_A(F(s_1,\dots,s_n)) \\
&= N_A\left(\sum_{i=1}^r a_i s_1^{e_{i,1}}\cdots s_n^{e_{i,n}}\right) \\
&\le \sum_{i=1}^r \left(N_A(a_i)N_A(s_1)^{e_{i,1}}\cdots N_A(s_n)^{e_{i,n}}\right) \\
&\le \sum_{i=1}^r N_A(a_i)\varepsilon^n \\
&\le \varepsilon^n U.
\end{aligned}$$

$\square$

LEMMA 12.8.6. *As above, let A be either $\mathbb{Z}$ or $k[t]$, where k is a fixed finite field of order q. Let K be the quotient field of A, Λ a finite dimensional K-division algebra, B an A-order in Λ. Then there exists $N \in \mathbb{N}$ such that for every right ideal J of B that is also an A-lattice in Λ, the following are true.*

(1) *There exists an element ξ in $J-(0)$ such that $[B:\xi B] = N_A(N_A^B(\xi)) \le [B:J]N$.*
(2) *$\xi^{-1}J$ is a right B-submodule and A-lattice in Λ such that $B \subseteq \xi^{-1}J$ and $[\xi^{-1}J : B] \le N$.*

PROOF. (1): Let $\{u_1,\dots,u_n\}$ be an A-basis for B. Let r be the maximum integer in $\{r \in \mathbb{N} \mid r^n \le [B:J]\}$. Then r is well defined, by Lemma 12.8.1, and $(r+1)^n > [B:J]$. By Lemma 12.8.2, the set $\Xi = \{\alpha \in A \mid N_A(\alpha) \le 2r\}$ has at least $2r$ elements. Since $2r \ge r+1$, the subset $X = \{s_1u_1+\cdots+s_nu_n \mid s_i \in \Xi\}$ of B has at least $(r+1)^n$ elements. Since $(r+1)^n > [B:J]$, there are two distinct elements ξ_1,ξ_2 in X such that $\xi = \xi_1 - \xi_2 = s_1u_1+\cdots+s_nu_n$ is in J. If s,t are in Ξ, then by Lemma 12.8.2, $N_A(s-t) \le N_A(s)+N_A(t) \le 2(2r)$. Therefore, $N_A(s_i) \le 4r$, for each i. By Lemma 12.8.5, there exists $U \in \mathbb{N}$ such that $[B:\xi B] = N_A(N_A^B(\xi)) \le (4r)^nU \le 4^nU[B:J]$. Taking $N = 4^nU$, Part (1) follows.

(2): Since $\xi \in J$, we have $\xi B \subseteq J$. Multiplying by $\xi^{-1} \in K$, it follows that $B \subseteq \xi^{-1}J$. The diagram of right B-modules

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d, "\xi"] & \xi^{-1}J \arrow[r] \arrow[d, "\xi"] & \xi^{-1}J/B \arrow[r] \arrow[d, "\xi"] & 0 \\
0 \arrow[r] & \xi B \arrow[r] & J \arrow[r] & J/\xi B \arrow[r] & 0
\end{tikzcd}$$

commutes. The rows are exact sequences. The vertical arrows are left multiplication by ξ and are isomorphisms. The groups in the right hand column are finite, by Lemma 12.8.1. Combining all of this with Part (1) and Lagrange's Theorem, Theorem 1.1.1. applied to $\xi B \subseteq J \subseteq B$, we have

$$\begin{aligned}
[\xi^{-1}J : B] &= [J : \xi B] \\
&= [B : \xi B]/[B : J] \\
&\leq N.
\end{aligned}$$

□

LEMMA 12.8.7. *As above, let A be either $\mathbb{Z}$ or $k[t]$, where k is a fixed finite field of order q. Let K be the quotient field of A, Λ a finite dimensional K-division algebra, B an A-order in Λ. For any $N \in \mathbb{N}$, let $\mathscr{S}$ be the set of all right B-submodules of Λ such that $B \subseteq M$, M is an A-lattice in Λ, and $[M : B] \leq N$. Then $\mathscr{S}$ is a finite set.*

PROOF. Let $M \in \mathscr{S}$. By Lemma 12.8.1, M/B is a finitely generated torsion A-module. By the Basis Theorem Theorem 1.7.17, M/B is isomorphic as an A-module to $\bigoplus_{i=1}^{\ell} A/\alpha_i A$, where $\alpha_1, \dots, \alpha_\ell$ are the invariant factors of M/B. Then α_ℓ annihilates M/B, hence $\alpha_\ell M \subseteq B$. We have $\alpha_\ell B \subseteq \alpha_\ell M \subseteq B$. For each i, the order of $A/\alpha_i A$ is equal to $N_A(\alpha_i)$, hence α_i belongs to the finite set $\Xi = \{\alpha \in A - (0) \mid N_A(\alpha) \leq N\}$. Since Ξ is a finite subset of $A - (0)$, there exists $\gamma \in A - (0)$ such that for every $\alpha \in \Xi$, α divides γ. Therefore, $\gamma B \subseteq \gamma M \subseteq B$ for every M in $\mathscr{S}$. By Lemma 12.8.1, there are only finitely many choices for γM. Therefore, there are only finitely many M in $\mathscr{S}$. □

THEOREM 12.8.8. *If B is the ring of integers in the global field L, then $\mathrm{Cl}(B)$ is a finite abelian group.*

PROOF. By Proposition 12.8.3, B is a Dedekind domain and an A-lattice in L, where A is $\mathbb{Z}$ if $\mathrm{char}(L) = 0$ and $A = k[t]$ otherwise. The class group of B is the group of fractional ideals modulo the group of principal fractional ideals. If F is a fractional ideal, then for some $d \in L$, $J = dF$ is a nonzero ideal in B. By Lemma 12.8.6, there is an upper bound $N \in \mathbb{N}$ that depends only on B, an element ξ in J such that $\xi^{-1}J$ is a fractional ideal of B containing B and $[\xi^{-1}J : B] \leq N$. By Lemma 12.8.7, there are only finitely many such fractional ideals $\xi^{-1}J$. Therefore, there are only finitely many ideal classes. □

COROLLARY 12.8.9. *If B is the ring of integers in the global field L, then there exists $\beta \in B$ such that the localization $B[\beta^{-1}]$ is a principal ideal domain.*

PROOF. Assume B is not a principal ideal domain. Let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ be a set of maximal ideals in B that generate $\mathrm{Cl}(B)$ (Theorem 12.8.8). Then $U = \operatorname{Spec} B - \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ is a nonempty open. By Lemma 3.3.11, there is $\beta \in B$ such that the basic open subset $U(\beta)$ is a nonempty open subset of U. By Theorem 11.4.14, $\mathrm{Cl}(B[\beta^{-1}]) = (0)$. By Exercise 12.3.2, $B[\beta^{-1}]$ is a unique factorization domain and a principal ideal domain. □

8.2. The Dirichlet Units Theorem. The following proof of the Dirichlet Units Theorem is based on Chapter 6 of [**3**].

Let F be a Galois extension of $\mathbb{Q}$ with finite group $G = \operatorname{Aut}_{\mathbb{Q}}(F)$. As in Proposition 5.6.12, $F \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{\sigma\in G} \mathbb{C}e_\sigma$ is isomorphic to the trivial G-Galois extension of $\mathbb{C}$. The change of base function

$$\phi : F \to F \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{\sigma\in G} \mathbb{C}e_\sigma$$

is a homomorphism of $\mathbb{Q}$-algebras and the composite map is defined by $\phi(\alpha) = \sum_{\sigma\in G} \sigma(\alpha)e_\sigma$. The absolute value of a complex number is $|a+bi| = \sqrt{a^2+b^2}$. The absolute value followed by the logarithm defines a homomorphism $\ln|\cdot| : \mathbb{C}^* \to \mathbb{R}$ from the multiplicative group of $\mathbb{C}$ to the additive group of $\mathbb{R}$. Define $\lambda : F^* \to \bigoplus_{\sigma\in G} \mathbb{R}e_\sigma$

$$\begin{tikzcd}
F^* \arrow[d, "\phi"'] \arrow[dr, "\lambda"] & \\
\bigoplus_{\sigma\in G} \mathbb{C}^* e_\sigma \arrow[r, "\oplus \ln|\,|"] & \bigoplus_{\sigma\in G} \mathbb{R}e_\sigma
\end{tikzcd}$$

to be ϕ followed by the logarithm function applied coordinate-wise. On an element $\alpha \in F^*$, λ is defined by $\lambda(\alpha) = \sum_{\sigma\in G} \ln|\sigma(\alpha)|e_\sigma$. If $n = [G : 1]$, then in Lemma 12.8.10 we identify $\bigoplus_{\sigma\in G} \mathbb{R}e_\sigma$ with $\mathbb{R}^n$ together with the usual euclidean metric space.

LEMMA 12.8.10. *In the above context, let $F/\mathbb{Q}$ be a Galois extension of fields with finite group G of order n. Let B be the integral closure of $\mathbb{Z}$ in F. If X is a bounded subset of $\bigoplus_{\sigma\in G} \mathbb{R}e_\sigma$ then the preimage of X under $\lambda : B^* \to \bigoplus_{\sigma\in G} \mathbb{R}e_\sigma$ is a finite set.*

PROOF. In this proof for convenience we use interval notation for subsets of $\mathbb{R}$. The logarithm is a monotonic increasing function $(0,\infty) \to (-\infty,\infty)$ Since X is bounded, there is a real number $U > 0$ such that $X \subseteq \prod_{\sigma\in G}[-U,U]e_\sigma$. Then there is a real number $V > 1$ such that $V^{-1} \le y \le V$ whenever $\ln y \in X$. If $\alpha \in B^*$ and $\lambda(\alpha) \in X$, then for each $\sigma \in G$, $V^{-1} \le |\sigma(\alpha)| \le V$.

By Exercise 1.8.3, the polynomial $g_\alpha(x) = \prod_{\sigma\in G}(x - \sigma(\alpha))$ has only one irreducible factor, namely $\operatorname{Irr.poly}_{\mathbb{Q}}(\alpha)$. The coefficients of $g_\alpha(x)$ are elementary symmetric polynomials (see [**19**, Section 5.7.2]) in $\{\sigma(\alpha) \mid \sigma \in G\}$. By Lemma 6.1.10, Gauss' Lemma, the coefficients of $g_\alpha(x)$ are in $\mathbb{Z}$. The elementary symmetric polynomials are continuous functions from $\prod_{\sigma\in G} \mathbb{R}^*$ to $\mathbb{R}$. By choosing V larger if necessary, we may assume the coefficients of $g_\alpha(x)$ are integers in $[-V,V]$. This means the set of polynomials $\{g_\alpha(x) \mid \alpha \in B^* \text{ and } \lambda(\alpha) \in X\}$ is finite. Consequently, the set of polynomials $\{\operatorname{Irr.poly}_{\mathbb{Q}}(\alpha) \mid \alpha \in B^* \text{ and } \lambda(\alpha) \in X\}$ is finite. Therefore, the set $\{\alpha \mid \alpha \in B^* \text{ and } \lambda(\alpha) \in X\}$ is finite. $\square$

COROLLARY 12.8.11. *In the context of Lemma 12.8.10, let F be a finite Galois extension of $\mathbb{Q}$ with group G and let B be the ring of integers in F. If T denotes the kernel of the homomorphism $\lambda : B^* \to \bigoplus_{\sigma\in G} \mathbb{R}e_\sigma$, then*

(1) T is a finite cyclic group, and
(2) T is equal to the group of all roots of unity in F.

PROOF. We know T is a finite group by Lemma 12.8.10 applied to $X = \{0\}$. We know T is cyclic by [**19**, Corollary 3.6.11]. Suppose $\zeta \in F^*$ and $\zeta^m = 1$ for some $m > 1$. Then ζ is integral over $\mathbb{Z}$, hence $\zeta \in B$. For each $\sigma \in G$, $|\sigma(\zeta)|^m = |\sigma(\zeta)^m| = |\sigma(\zeta^m)| = 1$. So $|\sigma(\zeta)| = 1$. By the definition of λ, this shows $\zeta \in T$. $\square$

LEMMA 12.8.12. *Fix $n > 0$ and let $\mathbb{R}^n$ be the n-dimensional real vector space with the usual euclidean metric. Let M be a nontrivial $\mathbb{Z}$-submodule of $\mathbb{R}^n$ with the property that $X \cap M$ is a finite set whenever X is a bounded subset of $\mathbb{R}^n$. Then there exist vectors $\{e_1, \dots, e_r\}$ in M satisfying the following:*

(1) $1 \le r \le n$,
(2) $\sum_{i=1}^r \mathbb{R}e_i$ is an r-dimensional subspace of $\mathbb{R}^n$, and contains M,
(3) M is a free $\mathbb{Z}$-module of rank r,
(4) M is a $\mathbb{Z}$-lattice in $\sum_{i=1}^r \mathbb{Q}e_i$.

PROOF. Let V be the subspace of $\mathbb{R}^n$ spanned by M. Let $r = \dim_{\mathbb{R}}(V)$ and let $\{e_1, \dots, e_r\}$ be an $\mathbb{R}$-basis for V contained in M. Let

$$X = \left\{ \sum_{i=1}^r a_i e_i \mid a_i \in \mathbb{R}, 0 \le a_i \le 1 \right\}.$$

Then X is a bounded subset of $\mathbb{R}^n$. By hypothesis on M, $X \cap M$ is a finite set. Notice that $X \cap M$ contains $\{e_1, \dots, e_r\}$. Let y be an arbitrary element of M. There are unique $r_i \in \mathbb{R}$ such that $y = \sum_{i=1}^r r_i e_i$. Define $\rho(y)$ by the rule

$$\begin{aligned} \rho(y) &= y - \sum_{i=1}^r \lfloor r_i \rfloor e_i \\ &= \sum_{i=1}^r (r_i - \lfloor r_i \rfloor) e_i \end{aligned}$$

where $\lfloor\,\rfloor : \mathbb{R} \to \mathbb{Z}$ is the floor function. Since $0 \le x - \lfloor x \rfloor < 1$ for all $x \in \mathbb{R}$, it follows that $\rho(y) \in X$. Since $y \in M$ and $\sum_{i=1}^r \lfloor r_i \rfloor e_i \in M$, we see that $\rho(y) \in M \cap X$. This shows M is generated as a $\mathbb{Z}$-module by the finite set $M \cap X$. Therefore M is a finitely generated torsion free $\mathbb{Z}$-module, hence free of finite rank by Theorem 1.7.14. Since M contains $\{e_1, \dots, e_r\}$, the rank of M is at least r. The set $\{\rho(jy) \mid j \in \mathbb{Z}\}$ is a subset of the finite set $M \cap X$. For some pair of integers $j < k$ we have $\rho(jy) = \rho(ky)$. For $1 \le i \le r$ we have $(jr_i - \lfloor jr_i \rfloor)e_i = (kr_i - \lfloor kr_i \rfloor)e_i$. Thus $(k-j)r_i = \lfloor kr_i \rfloor - \lfloor jr_i \rfloor$. This proves $r_i \in \mathbb{Q}$ for each i, hence $M \subseteq \sum_{i=1}^r \mathbb{Q}e_i$. By Proposition 12.1.1 (1), M is a $\mathbb{Z}$-lattice in $\sum_{i=1}^r \mathbb{Q}e_i$. By Proposition 12.1.4, M is has rank r. □

LEMMA 12.8.13. *In the context of Lemma 12.8.10, let F be a finite Galois extension of $\mathbb{Q}$ with group G and let B be the ring of integers in F. Then*

(1) B^* is a finitely generated abelian group.
(2) The torsion subgroup of B^* is equal to the group of all roots of unity in F and is a finite cyclic group.

PROOF. By Lemma 12.8.12, the image of $\lambda : B^* \to \bigoplus_{\sigma \in G} \mathbb{R}e_\sigma$ is a finitely generated free $\mathbb{Z}$-module of rank $r \le [G:1]$. By Corollary 12.8.11, the kernel of λ is equal to the group $T = \langle \zeta \rangle$ of all roots of unity in F and is a finite cyclic group. The sequence

$$\langle 1 \rangle \to \langle \zeta \rangle \to B^* \xrightarrow{\lambda} \mathbb{Z}^r \to \langle 0 \rangle$$

is split exact. □

LEMMA 12.8.14. *Let L be an algebraic number field with ring of integers A. Then*

(1) A^* is a finitely generated abelian group.
(2) The torsion subgroup of A^* is equal to the group of all roots of unity in L and is a finite cyclic group.

PROOF. By the Embedding Theorem, there is a finite dimensional Galois extension $F/\mathbb{Q}$ containing L as an intermediate field. If B is the ring of integers in F, then A is a subring of B.

$$\begin{tikzcd}
F & \\
L \arrow[u] & B \arrow[ul] \\
\mathbb{Q} \arrow[u] & A \arrow[ul] \arrow[u] \\
& \mathbb{Z} \arrow[ul] \arrow[u]
\end{tikzcd}$$

The group of units in A is a subgroup of the group of units in B. By Lemma 12.8.13, A^* is finitely generated and if T denotes the torsion subgroup of A^*, then T is a finite cyclic group. The proof of Corollary 12.8.11 shows that T is equal to the group of all roots of unity in L. $\square$

We end this section with a statement of the Dirichlet Units Theorem. First we establish some notation. Let L be an algebraic number field with ring of integers A. By the Primitive Element Theorem, Theorem 5.5.8, $L = \mathbb{Q}(u)$ for some element $u \in L$. Let $f = \operatorname{Irr.poly}_{\mathbb{Q}}(u)$. Since f is separable, the unique factorization of f as a polynomial in $\mathbb{R}[x]$ has the form

$$f = (x-u_1)\cdots(x-u_{r_1})q_1(x)\cdots q_{r_2}(x)$$

where $u_1,\dots,u_{r_1}$ are the distinct real roots of f, $r_1 \geq 0$, $q_1(x),\dots,q_{r_2}(x)$ are the irreducible monic quadratic factors of f in $\mathbb{R}[x]$, and $r_2 \geq 0$ ([**19**, Theorem 5.4.11]). Then

$$\begin{aligned}
L \otimes_{\mathbb{Q}} \mathbb{R} &= \frac{\mathbb{Q}[x]}{(f)} \otimes_{\mathbb{Q}} \mathbb{R} \\
&= \left(\bigoplus_{i=1}^{r_1} \frac{\mathbb{R}[x]}{(x-u_i)} \right) \oplus \left(\bigoplus_{i=1}^{r_2} \frac{\mathbb{R}[x]}{(q_i(x))} \right) \\
&\cong \left(\bigoplus_{i=1}^{r_1} \mathbb{R} \right) \oplus \left(\bigoplus_{i=1}^{r_2} \mathbb{C} \right).
\end{aligned}$$

That is, $L \otimes_{\mathbb{Q}} \mathbb{R}$ is the ring direct sum of r_1 copies of the field $\mathbb{R}$ and r_2 copies of the field $\mathbb{C}$.

THEOREM 12.8.15. *(The Dirichlet Units Theorem) Let L be an algebraic number field with ring of integers A. In the above notation, the group of units in A is a finitely generated abelian group isomorphic to* $\langle \zeta \rangle \oplus \mathbb{Z}^r$, *where* $r = r_1 + r_2 - 1$ *and* $\langle \zeta \rangle$ *is the group of all roots of unity in L.*

PROOF. By Lemma 12.8.14, A^* is finitely generated and the torsion subgroup is cyclic. The only part that has not been proved is the formula for the rank. See [**3**] for a proof that is based on an application of Minkowski's Convex Body Theorem. $\square$

Acronyms

ACC	Ascending Chain Condition
DCC	Descending Chain Condition
PID	Principal Ideal Domain
UFD	Unique Factorization Domain
DVR	Discrete Valuation Ring

Bibliography

[1] S. A. Amitsur, *Simple algebras and cohomology groups of arbitrary fields*, Trans. Amer. Math. Soc. **90** (1959), 73–112. MR 0101265 (21 #78)

[2] Emil Artin and John T. Tate, *A note on finite ring extensions*, J. Math. Soc. Japan **3** (1951), 74–77. MR 44509

[3] Robert B. Ash, *A course in algebraic number theory*, Dover Publications, Inc., Mineola, NY, 2010. MR 2779252

[4] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802 (39 #4129)

[5] Bernice Auslander, *The Brauer group of a ringed space*, J. Algebra **4** (1966), 220–273. MR 0199213 (33 #7362)

[6] Maurice Auslander and D. A. Buchsbaum, *Unique factorization in regular local rings*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 733–734. MR 0103906 (21 #2669)

[7] Maurice Auslander and Oscar Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409. MR 0121392 (22 #12130)

[8] ———, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1–24. MR 0117252 (22 #8034)

[9] Gorô Azumaya, *On maximally central algebras*, Nagoya Math. J. **2** (1951), 119–150. MR 0040287 (12,669g)

[10] Hyman Bass, *Algebraic K-theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR 0249491 (40 #2736)

[11] F. Rudolf Beyl, *The connecting morphism in the Kernel-Cokernel sequence*, Arch. Math. (Basel) **32** (1979), no. 4, 305–308. MR 545150

[12] Nicolas Bourbaki, *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1989, Translated from the French, Reprint of the 1972 edition. MR 979760 (90a:13001)

[13] Hans-Berndt Brinkmann and Dieter Puppe, *Abelsche und exakte Kategorien, Korrespondenzen*, Lecture Notes in Mathematics, Vol. 96, Springer-Verlag, Berlin-New York, 1969. MR 0269713

[14] Henri Cartan and Samuel Eilenberg, *Homological algebra*, Princeton University Press, Princeton, N. J., 1956. MR 0077480 (17,1040e)

[15] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962. MR 0144979 (26 #2519)

[16] F. R. DeMeyer and Edward Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics, Vol. 181, Springer-Verlag, Berlin, 1971. MR 0280479 (43 #6199)

[17] Alan H. Durfee, *Fifteen characterizations of rational double points and simple critical points*, Enseign. Math. (2) **25** (1979), no. 1-2, 131–163. MR 543555 (80m:14003)

[18] Timothy J. Ford, *Separable algebras*, Graduate Studies in Mathematics, vol. 183, American Mathematical Society, Providence, RI, 2017. MR 3618889

[19] ———, *Introduction to abstract algebra*, Open Math Notes, American Mathematical Society, 2020, available at the URL: `https://www.ams.org/open-math-notes/omn-view-listing?listingId=110827`.

[20] Timothy J. Ford and Drake M. Harmon, *The Brauer group of an affine rational surface with a non-rational singularity*, J. Algebra **388** (2013), 107–140. MR 3061681

[21] Robert M. Fossum, *The divisor class group of a Krull domain*, Springer-Verlag, New York, 1973. MR 0382254 (52 #3139)

[22] A. Grothendieck, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I.*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11, 167. MR 217085

[23] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I*, Inst. Hautes Études Sci. Publ. Math. (1964), no. 20, 259. MR 0173675 (30 #3885)

[24] ______, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 24, 231. MR 0199181 (33 #7330)

[25] Alexander Grothendieck, *Fondements de la géométrie algébrique. [Extraits du Séminaire Bourbaki, 1957–1962.]*, Secrétariat mathématique, Paris, 1962. MR 0146040

[26] Alexandre Grothendieck, *Revêtements étales et groupe fondamental*, Springer-Verlag, Berlin-New York, 1971, Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud, Lecture Notes in Mathematics, Vol. 224. MR 0354651 (50 #7129)

[27] ______, *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)]. MR 2017446 (2004g:14017)

[28] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. MR 0463157 (57 #3116)

[29] G. Hochschild, *On the cohomology groups of an associative algebra*, Ann. of Math. (2) **46** (1945), 58–67. MR 0011076

[30] Raymond Taylor Hoobler, *A generalization of the Brauer group and Amitsur cohomology*, ProQuest LLC, Ann Arbor, MI, 1966, Thesis (Ph.D.)–University of California, Berkeley. MR 2615918

[31] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, Reprint of the 1974 original. MR 600654 (82a:00006)

[32] Nathan Jacobson, *Lie algebras*, Dover Publications, Inc., New York, 1979, Republication of the 1962 original. MR 559927 (80k:17001)

[33] G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), 461–479. MR 35 #1585

[34] M. A. Knus, M. Ojanguren, and D. J. Saltman, *On Brauer groups in characteristic p*, Brauer groups (Proc. Conf., Northwestern Univ., Evanston, Ill., 1975), Springer, Berlin, 1976, pp. 25–49. Lecture Notes in Math., Vol. 549. MR 0429859 (55 #2869)

[35] Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 294, Springer-Verlag, Berlin, 1991, With a foreword by I. Bertuccioni. MR 1096299 (92i:11039)

[36] Max-Albert Knus and Manuel Ojanguren, *Théorie de la descente et algèbres d'Azumaya*, Springer-Verlag, Berlin, 1974, Lecture Notes in Mathematics, Vol. 389. MR 0417149 (54 #5209)

[37] T. Y. Lam, *Serre's problem on projective modules*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006. MR 2235330

[38] Johann B. Leicht, *Über die elementaren Lemmata der homologischen Algebra in quasi-exacten Kategorien*, Monatsh. Math. **68** (1964), 240–254. MR 0170924

[39] Joseph Lipman, *Rational singularities, with applications to algebraic surfaces and unique factorization*, Inst. Hautes Études Sci. Publ. Math. (1969), no. 36, 195–279. MR 0276239 (43 #1986)

[40] Akhil Mathew and The CRing Project Authors, *The CRing project*, `http://people.fas.harvard.edu/~amathew/cr.html`, 2015, A collaborative, open source textbook on commutative algebra.

[41] Hideyuki Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980. MR 575344 (82i:13003)

[42] Bernard R. McDonald, *Linear algebra over commutative rings*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 87, Marcel Dekker, Inc., New York, 1984. MR 769104 (86d:13008)

[43] Thomas McKenzie, *The separable closure of a local ring*, J. Algebra **207** (1998), no. 2, 657–663. MR 1644231 (99g:13006)

[44] James S. Milne, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980. MR 559531 (81j:14002)

[45] David Mumford, *The red book of varieties and schemes*, expanded ed., Lecture Notes in Mathematics, vol. 1358, Springer-Verlag, Berlin, 1999, Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello. MR 1748380 (2001b:14001)

[46] C. Năstăsescu and F. van Oystaeyen, *Graded ring theory*, North-Holland Mathematical Library, vol. 28, North-Holland Publishing Co., Amsterdam-New York, 1982. MR 676974

[47] Morris Orzech and Charles Small, *The Brauer group of commutative rings*, Marcel Dekker, Inc., New York, 1975, Lecture Notes in Pure and Applied Mathematics, Vol. 11. MR 0457422 (56 #15627)

[48] Michel Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Mathematics, Vol. 169, Springer-Verlag, Berlin-New York, 1970. MR 0277519 (43 #3252)

[49] I. Reiner, *Maximal orders*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975, London Mathematical Society Monographs, No. 5. MR 0393100 (52 #13910)

[50] Dock Sang Rim, *An exact sequence in Galois cohomology*, Proc. Amer. Math. Soc. **16** (1965), 837–840. MR 0179232 (31 #3480)

[51] Joseph J. Rotman, *An introduction to homological algebra*, Pure and Applied Mathematics, vol. 85, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1979. MR 538169 (80k:18001)

[52] David J. Saltman, *Lectures on division algebras*, CBMS Regional Conference Series in Mathematics, vol. 94, Published by American Mathematical Society, Providence, RI, 1999. MR 1692654 (2000f:16023)

[53] P. Samuel, *Lectures on unique factorization domains*, Notes by M. Pavman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30, Tata Institute of Fundamental Research, Bombay, 1964. MR 0214579

[54] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

[55] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[56] John R. Silvester, *Determinants of block matrices*, The Mathematical Gazette **84** (2000), no. 501, 460–467.

[57] Alexander Stasinski, *A uniform proof of the finiteness of the class group of a global field*, Amer. Math. Monthly **128** (2021), no. 3, 239–249. MR 4217755

[58] Robert R. Stoll, *Set theory and logic*, Dover Publications, Inc., New York, 1979, Corrected reprint of the 1963 edition. MR 634799 (83e:04002)

[59] O. E. Villamayor and D. Zelinsky, *Galois theory for rings with finitely many idempotents*, Nagoya Math. J. **27** (1966), 721–731. MR 34 #5880

[60] Oscar Zariski, *A new proof of Hilbert's Nullstellensatz*, Bull. Amer. Math. Soc. **53** (1947), no. 4, 362–368. MR 0020075

[61] Oscar Zariski and Pierre Samuel, *Commutative algebra. Vol. 1*, Springer-Verlag, New York-Heidelberg-Berlin, 1975, With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28. MR 0384768 (52 #5641)

[62] ———, *Commutative algebra. Vol. II*, Springer-Verlag, New York-Heidelberg, 1975, Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29. MR 0389876 (52 #10706)