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 an introduction to Commutative Algebra.

CHAPTER 1

Preliminaries and Prerequisites

1. Background Material from Set Theory

A *set* is a collection of objects X with a membership rule such that given any object x it is possible to decide whether x belongs to the set X. If x belongs to X, we say x is an *element* of X and write $x \in X$. Suppose X and Y are sets. If every element of X is also an element of Y, then we say X is a *subset* of Y, or that X is *contained* in Y, and write $X \subseteq Y$. If X and Y are subsets of each other, then we say X and Y are *equal* and write $X = Y$. The set without an element is called the *empty set* and is denoted $\emptyset$. The set of all subsets of X is called the *power set* of X, and is denoted 2^X. Notice that $\emptyset$ and X are both elements of 2^X. The *union* of X and Y, denoted $X \cup Y$, is the set of all elements that are elements of X or Y. The *intersection* of X and Y, denoted $X \cap Y$, is the set of all elements that are elements of X and Y. The *complement* of X with respect to Y, denoted $Y - X$, is the set of all elements of Y that are not elements of X. The *product* of X and Y, denoted $X \times Y$, is the set of all ordered pairs of the form (x,y) where x is an element of X and Y is an element of Y.

Let I be a set and suppose for each $i \in I$ there is a set X_i. Then we say $\{X_i \mid i \in I\}$ is a *family of sets indexed by I*. The *union* of the family is denoted $\bigcup_{i\in I} X_i$ and is defined to be the set of all elements x such that $x \in X_i$ for some $i \in I$. The *intersection* of the family is denoted $\bigcap_{i\in I} X_i$ and is defined to be the set of all elements x such that $x \in X_i$ for all $i \in I$.

Let X and Y be nonempty sets. A *relation* between X and Y is a nonempty subset R of the product $X \times Y$. Two relations are equal if they are equal as sets. The *domain* of R is the set of all first coordinates of the pairs in R. The *range* of R is the set of all second coordinates of the pairs in R.

A *function* (or *map*) from X to Y is a relation $f \subseteq X \times Y$ such that for each $x \in X$ there is a unique $y \in Y$ such that $(x,y) \in f$. In this case, we say y is the *image* of x under f, and write $y = f(x)$. The range of a function f is also called the *image* of f. The image of f is denoted $f(X)$, or $\operatorname{im}(f)$. The notation $f : X \to Y$ means f is a function from X to Y. If $T \subseteq Y$, the *preimage* of T under f, denoted $f^{-1}(T)$, is the set of all elements $x \in X$ such that $f(x) \in T$. If $S \subseteq X$, the *restriction* of f to S is the function $f|_S : S \to Y$ defined by $f|_S(x) = f(x)$ for all $x \in S$. The *identity map* from X to X, $1_X : X \to X$, is defined by $1_X(x) = x$ for all $x \in X$. If $S \subseteq X$, the *inclusion map* from S to X is the restriction of the identity map 1_X to the subset S. If $f : X \to Y$ and $g : Y \to Z$, the *product* or *composition map* is $gf : X \to Z$ defined by $gf(x) = g(f(x))$. If $h : Z \to W$, the reader should verify that $h(gf) = (hg)f$ so the product of functions is associative. We say that $f : X \to Y$ is *one-to-one* (or *injective*) in case $f(x) \neq f(y)$ whenever $x \neq y$. We say that $f : X \to Y$ is *onto* or (*surjective*) in case the image of f is equal to Y. If $f : X \to Y$ is one-to-one and onto, then we say that f is a *one-to-one correspondence* (or f is *bijective*). The reader should verify that the identity map 1_X is a one-to-one correspondence. If $S \subseteq X$, the reader should verify that the inclusion map $S \to X$ is one-to-one.

PROPOSITION 1.1.1. *Let $f : X \to Y$.*

1. *f is one-to-one if and only if there exists $g : Y \to X$ such that $gf = 1_X$. In this case g is called a* left inverse *of f.*
2. *If f is a one-to-one correspondence, then the function g of Part (1) is unique and satisfies $fg = 1_Y$. In this case g is called the* inverse *of f and is denoted f^{-1}.*
3. *If there exists a function $g : Y \to X$ such that $gf = 1_X$ and $fg = 1_Y$, then f is a one-to-one correspondence and g is equal to f^{-1}.*

PROOF. Is left to the reader. □

A *binary relation on X* is a subset of $X \times X$. Suppose $\sim$ is a binary relation on X. If (x,y) is an element of the relation, then we say x is *related* to y and write $x \sim y$. Otherwise we write $x \not\sim y$. If $x \sim x$ for every $x \in X$, then we say $\sim$ is *reflexive*. We say $\sim$ is *symmetric* in case $x \sim y$ whenever $y \sim x$. We say $\sim$ is *antisymmetric* in case $x \sim y$ and $y \sim x$ implies $x = y$. We say $\sim$ is *transitive* if $x \sim z$ whenever $x \sim y$ and $y \sim z$. If $\sim$ is reflexive, symmetric and transitive, then we say $\sim$ is an *equivalence relation* on X. If $\sim$ is an equivalence relation on X, and $x \in X$, then the *equivalence class* containing x is $\bar{x} = \{y \in X \mid x \sim y\}$. By $X/\sim$ we denote the set of all equivalence classes.

PROPOSITION 1.1.2. *Let X be a nonempty set and $\sim$ an equivalence relation on X.*

1. *If $x \in X$, then $\bar{x} \neq \emptyset$.*
2. $\displaystyle\bigcup_{x\in X} \bar{x} = X = \bigcup_{\bar{x}\in X/\sim} \bar{x}$
3. *If $x, y \in X$, then $\bar{x} = \bar{y}$ or $\bar{x} \cap \bar{y} = \emptyset$.*

PROOF. Is left to the reader. □

Let X be a nonempty set. A *partition* of X is a family $\mathscr{P}$ of nonempty subsets of X such that $X = \bigcup_{P\in\mathscr{P}} P$ and if $P, Q \in \mathscr{P}$, then either $P = Q$, or $P \cap Q = \emptyset$. If $\sim$ is an equivalence relation on X, then Proposition 1.1.2 shows that $X/\sim$ is a partition of X. Conversely, suppose $\mathscr{P}$ is a partition of X. There is an equivalence relation $\sim$ on X corresponding to $\mathscr{P}$ defined by $x \sim y$ if and only if x and y belong to the same element of $\mathscr{P}$.

PROPOSITION 1.1.3. *Let X be a nonempty set. There is a one-to-one correspondence between the set of all equivalence relations on X and the the set of all partitions of X. The assignment maps an equivalence relation $\sim$ to the partition $X/\sim$.*

PROOF. Is left to the reader. □

The set of *integers* is $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$. The set of *natural numbers* is $\mathbb{N} = \{0,1,2,3,\dots\}$. The set of positive integers is $\mathbb{Z}_{>0} = \{1,2,3,4,\dots\}$. The set of *rational numbers* is $\mathbb{Q} = \{n/d \mid n \in \mathbb{Z}, d \in \mathbb{Z}_{>0}\}$ where it is understood that $n/d = x/y$ if $ny = dx$. The set of *real numbers* is denoted $\mathbb{R}$, the set of *complex numbers* is denoted $\mathbb{C}$.

Let U be any set, which we assume contains $\mathbb{N}$ as a subset. Define a binary relation on the power set 2^U by the following rule. If X and Y are subsets of U, then we say X and Y are *equivalent* if there exists a one-to-one correspondence $\alpha : X \to Y$. The reader should verify that this is an equivalence relation on 2^U. If X and Y are equivalent sets, then we say X and Y have the same *cardinal number*. Define $I_0 = \emptyset$. For $n \geq 1$ define $I_n = \{1,\dots,n\}$. If a set X is equivalent to I_n, then we say X has cardinal number n. We say a set X is *finite* if X is equivalent to I_n for some n. Otherwise, we say X is *infinite*.

A *commutative diagram* is a finite family of sets $D_V = \{X_1,\dots,X_v\}$ together with a finite collection of functions $D_E = \{f_1,\dots,f_e\}$ satisfying the following properties.

(1) Each f in D_E is a function from one set in D_V to another set in D_V.

(2) Given two sets X, Y in D_V and any two paths

$$X = A_0 \xrightarrow{f_{a_1}} A_1 \xrightarrow{f_{a_2}} \cdots \to A_{r-1} \xrightarrow{f_{a_r}} A_r = Y$$

$$X = B_0 \xrightarrow{g_{b_1}} B_1 \xrightarrow{g_{b_2}} \cdots \to B_{s-1} \xrightarrow{g_{b_s}} B_s = Y$$

from X to Y consisting of functions $f_{a_1}, \dots, f_{a_r}, g_{b_1}, \dots, g_{b_s}$ in D_E, the composite functions $f_{a_r} \cdots f_{a_1}$ and $g_{b_s} \cdots g_{b_1}$ are equal.

Let X be a set and $\le$ a binary relation on X which is reflexive, antisymmetric and transitive. Then we say $\le$ is a *partial order* on X. We also say X is *partially ordered by* $\le$. If $x, y \in X$, then we say x and y are *comparable* if $x \le y$ or $y \le x$. 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 $\le$ to $S \times S$. If the restriction of $\le$ to S is a chain, then we say S is a *chain in* X.

Let X be partially ordered by $\le$ and suppose S is a nonempty subset of X. Let $a \in S$. We say a is the *least* element of S if $a \le x$ 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 $x \le a$ implies $x = a$ for all $x \in S$. We say a is a *maximal* element of S in case $a \le x$ 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 $x \le u$ for all $x \in S$. An element $l \in X$ is called a *lower bound* for S in case $l \le x$ 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.

Let X be partially ordered by $\le$. 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 $\{\dots, x_3 \le x_2 \le x_1 \le x_0\}$ is eventually constant. That is, there is a subscript n such that $x_n = x_i$ for all $i \ge n$. We say that X satisfies the *ascending chain condition* (ACC) if every chain in X of the form $\{x_0 \le x_1 \le x_2 \le x_3, \dots\}$ is eventually constant.

2. Background Material from Number Theory

AXIOM 1.2.1. *(The Well Ordering Principle) The set $\mathbb{N}$ of natural numbers is well ordered. That is, every nonempty subset of $\mathbb{N}$ contains a least element.*

PROPOSITION 1.2.2. *(Mathematical Induction) Let S be a subset of $\mathbb{N}$ such that $0 \in S$. Assume S satisfies one of the following.*

(1) For each $n \in \mathbb{N}$, if $n \in S$, then $n+1 \in S$.

(2) For each $n \in \mathbb{N}$, if $\{0, \dots, n\} \subseteq S$, then $n+1 \in S$.

Then $S = \mathbb{N}$.

PROOF. Is left to the reader. □

PROPOSITION 1.2.3. *(The Division Algorithm) If $a, b \in \mathbb{Z}$ and $a \neq 0$, then there exist unique integers $q, r \in \mathbb{Z}$ such that $0 \le r < |a|$ and $b = aq + r$.*

PROOF. Is left to the reader. □

Let $a, b \in \mathbb{Z}$. We say *a divides b*, and write $a \mid b$, in case there exists $q \in \mathbb{Z}$ such that $b = aq$. In this case, a is called a *divisor* of b, and b is called a *multiple* of a.

PROPOSITION 1.2.4. *Let $\{a_1, \dots, a_n\}$ be a set of integers and assume at least one of the a_i is nonzero. There exists a unique positive integer d such that*

(1) $d \mid a_i$ for all $1 \le i \le n$, and
(2) if $e \mid a_i$ for all $1 \le i \le n$, then $e \mid d$.

We call d the greatest common divisor *of the set, and write $d = \mathrm{GCD}(a_1, \dots, a_n)$.*

PROOF. Let S be the set of all positive linear combinations of the a_i

$$S = \{x_1 a_1 + \cdots + x_n a_n \mid x_1, \dots, x_n \in \mathbb{Z}, x_1 a_1 + \cdots + x_n a_n > 0\}.$$

The reader should verify that $S \neq \emptyset$. By the Well Ordering Principle, there exists a least element of S which we can write as $d = k_1 a_1 + \cdots + k_n a_n$ for some integers $k_1, \dots, k_n$. Fix one i and apply the division algorithm to write $a_i = dq + r$ where $0 \le r < d$. Solve $a_i = (k_1 a_1 + \cdots + k_n a_n)q + r$ for r to see that

$$r = a_i - (k_1 a_1 + \cdots + k_n a_n)q$$

is a linear combination of $a_1, \dots, a_n$. Because $r < d$, we conclude that r is not in S. Therefore $r = 0$. This proves Part (1). The reader should verify Part (2) and the claim that d is unique. □

We say the set of integers $\{a_1, \dots, a_n\}$ is *relatively prime* in case $\mathrm{GCD}(a_1, \dots, a_n) = 1$. An integer $\pi \in \mathbb{Z}$ is called a *prime* in case $\pi > 1$ and the only divisors of π are $-\pi, -1, 1, \pi$.

LEMMA 1.2.5. *Let a, b and c be integers.*

(1) (Bézout's Identity) If $d = \mathrm{GCD}(a, b)$, then there exist integers u and v such that $d = au + bv$.
(2) (Euclid's Lemma) If $\mathrm{GCD}(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

PROOF. Is left to the reader. □

LEMMA 1.2.6. *Let π be a prime number. Let a and $a_1, \dots, a_n$ be integers.*

(1) If $\pi \mid a$, then $\mathrm{GCD}(\pi, a) = \pi$, otherwise $\mathrm{GCD}(\pi, a) = 1$.
(2) If $\pi \mid a_1 a_2 \cdots a_n$, then $\pi \mid a_i$ for some i.

PROOF. Is left to the reader. □

PROPOSITION 1.2.7. *(The Fundamental Theorem of Arithmetic) Let n be a positive integer which is greater than 1. There exist unique positive integers k, $e_1, \dots, e_k$ and unique prime numbers $\pi_1, \dots, \pi_k$ such that $n = \pi_1^{e_1} \cdots \pi_k^{e_k}$.*

PROOF. Is left to the reader. □

Let m be a positive integer. Define a binary relation on $\mathbb{Z}$ by the following rule. Given $x, y \in \mathbb{Z}$, we say *x is congruent to y modulo m*, and write $x \equiv y \pmod{m}$, in case $m \mid (x - y)$. By Proposition 1.2.8 this defines an equivalence relation on $\mathbb{Z}$. The set of all equivalence classes of integers modulo m is denoted $\mathbb{Z}/(m)$.

PROPOSITION 1.2.8. *Let m be a positive integer.*

(1) Congruence modulo m is an equivalence relation on $\mathbb{Z}$.

(2) *$\{0,1,\dots,m-1\}$ is a full set of representatives for the equivalence classes. In other words, every integer is congruent to one of $0,1,\dots,m-1$ and no two distinct elements of $\{0,1,\dots,m-1\}$ are congruent to each other.*

(3) *If $u \equiv v \pmod{m}$ and $x \equiv y \pmod{m}$, then $u+x \equiv v+y \pmod{m}$ and $ux \equiv vy \pmod{m}$.*

(4) *If $\operatorname{GCD}(a,m) = 1$ and $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$.*

PROOF. Is left to the reader. □

Let $n \geq 1$ be an integer. The notation $\sum_{d|n}$ or $\prod_{d|n}$ denotes the sum or product over the set of all positive numbers d such that $d \mid n$. The Möbius function is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not squarefree,} \\ (-1)^r & \text{if } n \text{ factors into } r \text{ distinct primes.} \end{cases}$$

THEOREM 1.2.9. *(Möbius Inversion Formula) Let f be a function defined on $\mathbb{Z}_{>0}$ and define another function on $\mathbb{Z}_{>0}$ by*

$$F(n) = \sum_{d|n} f(d).$$

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

PROOF. The proof can be found in any elementary number theory book, and is left to the reader. □

3. The Well Ordering Principle and Some of Its Equivalents

AXIOM 1.3.1. *(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 1.3.2. *(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. □

PROPOSITION 1.3.3. *(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 1.3.1, there exists a well ordered set W and a one-to-one correspondence $\omega : W \to X$. Using Proposition 1.3.2, 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 $w_0 \leq w_1 \leq w_2 < \alpha$, then $C(w_1) \subseteq C(w_2)$,

(2) $C(w)$ is a well ordered chain in X, and
(3) $C(w) \subseteq \{\omega(i) \mid w_0 \leq i \leq w\}$.

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

By Proposition 1.3.2, 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 $C(w_1) \subseteq G$. □

DEFINITION 1.3.4. 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 1.3.5. *(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 1.3.1, 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. □

4. Topological Spaces

DEFINITION 1.4.1. 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 1.4.2. 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 1.4.3. 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 1.4.4. *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 1.4.5. *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. Exercise 1.5.10 shows the equivalence of (1) and (2), as well as the equivalence of (3) and (4). The rest is left to the reader. □

LEMMA 1.4.6. *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 quasi-compact. That is, every open cover of X contains a finite subcover.

PROOF. Is left to the reader. □

PROPOSITION 1.4.7. *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 $Y_1, \ldots, Y_c$ 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 1.4.5 (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 1.4.4. Then each Z_i belongs to a unique connected component of X. □

A topological space X is said to be *Hausdorff* 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. For proofs of Theorems 1.4.8 and 1.4.9, the reader is referred to a book on Point Set Topology, for example [**16**].

THEOREM 1.4.8. *(Tychonoff Product Theorem) If $\{X_i \mid i \in D\}$ is a family of compact topological spaces indexed by a set D, then with the product topology, $\prod_{i \in D} X_i$ is a compact topological space.*

THEOREM 1.4.9. *If $\{X_i \mid i \in D\}$ is a family of Hausdorff indexed by a set D, then with the product topology, $\prod_{i \in D} X_i$ is a Hausdorff topological space.*

5. Exercises

EXERCISE 1.5.1. Let $\{X_i \mid i \in I\}$ be a family of sets indexed by I and let Y any set. Prove:

(1) $Y \cap \left(\bigcup_{i \in I} X_i\right) = \bigcup_{i \in I} (Y \cap X_i)$
(2) $Y \cup \left(\bigcap_{i \in I} X_i\right) = \bigcap_{i \in I} (Y \cup X_i)$

EXERCISE 1.5.2. (DeMorgan's Laws) Let $\{X_i \mid i \in I\}$ be a family of sets indexed by I and suppose U is a set such that $X_i \subseteq U$ for all $i \in I$. Prove:

(1) $U - \left(\bigcup_{i\in I} X_i\right) = \bigcap_{i\in I}(U - X_i)$
(2) $U - \left(\bigcap_{i\in I} X_i\right) = \bigcup_{i\in I}(U - X_i)$

EXERCISE 1.5.3. Let $f : X \to Y$ and $g : Y \to Z$. Prove:

(1) If gf is onto, then g is onto.
(2) If gf is one-to-one, then f is one-to-one.
(3) If f is onto and g is onto, then gf is onto.
(4) If f is one-to-one and g is one-to-one, then gf is one-to-one.

EXERCISE 1.5.4. Let $n > 0$. Prove: If $f : I_n \to I_n$ is one-to-one, then f is onto. (Hint: Use Proposition 1.2.2.)

EXERCISE 1.5.5. Let $n > 0$. Prove: If $f : I_n \to I_n$ is onto, then f is one-to-one. (Hint: Use Proposition 1.2.2 and Proposition 1.1.1 to construct f^{-1}.)

EXERCISE 1.5.6. Let X be an infinite set. Prove that X contains a subset that is equivalent to $\mathbb{N}$.

EXERCISE 1.5.7. Let X be a set. Prove that X is infinite if and only if there exists a one-to-one function $f : X \to X$ which is not onto.

EXERCISE 1.5.8. Let $f : X \to Y$ be a function. Prove that f is onto if and only if there exists a function $g : Y \to X$ such that $fg = 1_Y$. In this case g is called a *right inverse* of f. (Hint: Use Proposition 1.3.5.)

EXERCISE 1.5.9. Let I be a set and $\{X_i \mid i \in I\}$ a family of nonempty sets indexed by I. For each $k \in I$ define $\pi_k : \prod_{i\in I} X_i \to X_k$ by the rule $\pi_k(f) = f(k)$. We call π_k the *projection onto coordinate k*. Show that π_k is onto.

EXERCISE 1.5.10. Let X be a set that is partially ordered by $\leq$.

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

EXERCISE 1.5.11. Let X be a topological space. We say that a family $\{Z_i \subseteq X \mid i \in D\}$ of closed subsets of X has the *finite intersection property* if for every finite subset $J \subseteq D$, $\bigcap_{j\in J} Z_j \neq \emptyset$. Show that the following are equivalent:

(1) X is compact.
(2) For any family $\{Z_i \subseteq X \mid i \in D\}$ of closed subsets of X with the finite intersection property, $\bigcap_{i\in D} Z_i \neq \emptyset$.

CHAPTER 2

Rings

1. Definitions and Terminology

DEFINITION 2.1.1. 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. The *trivial ring* is $\{0\}$, in which $0=1$. Otherwise $0\neq 1$. Multiplication distributes over addition from both the left and the right. If $(R,\cdot)$ is commutative, then we say R is a *commutative ring*.

PROPOSITION 2.1.2. *Let R be a ring. Let $a,b\in R$, $n,m\in\mathbb{Z}$, $a_1,\dots,a_n,b_1,\dots,b_m\in R$.*

(1) $0a=a0=0$.
(2) $(-a)b=a(-b)=-(ab)$.
(3) $(-a)(-b)=ab$.
(4) $(na)b=a(nb)=n(ab)$.
(5) $\left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^m b_j\right)=\sum_{i=1}^n\sum_{j=1}^m a_ib_j$

PROOF. Is left to the reader. □

DEFINITION 2.1.3. Let R be a ring and $a\in R$. We say a 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 (Exercise 2.1.11 (1)). 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 $\text{Units}(R)$ or R^* and is called *the group of units in R*.

REMARK 2.1.4. Notice that in Definition 2.1.3, we have explicitly required a domain to have at least two elements. The only ring with order one is the trivial ring (0). In Example 2.1.13 (4) we see that (0) plays the role of a terminal object in the category of rings. Besides this, there is no significant result that can be proved about the ring (0). It has no proper ideals, is not a subring of any larger ring, and there is no nontrivial module or algebra over (0).

EXAMPLE 2.1.5. Standard examples of rings and fields are listed here.

(1) The ring of integers $\mathbb{Z}$ is an integral domain. The ring of integers modulo n, denoted $\mathbb{Z}/(n)$, is a commutative ring containing n elements.
(2) Denote by $\mathbb{Q}$ the field of rational numbers, by $\mathbb{R}$ the field of real numbers and by $\mathbb{C}$ the field of complex numbers.

(3) If k is a field and $n \geq 1$, the ring of n-by-n matrices over k is denoted by $M_n(k)$. If $n > 1$, then $M_n(k)$ is noncommutative.

(4) If R is any ring, the ring of n-by-n matrices over R is denoted by $M_n(R)$.

EXAMPLE 2.1.6. If k is a field the ring of quaternions over k is the four-dimensional vector space over k with basis $1, i, j, k$ with multiplication defined by extending these relations by associativity and distributivity:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = -ji &= k \\ ik = -ki &= -j. \end{aligned}$$

The ring of quaternions is a division ring if k is equal to either $\mathbb{Q}$ or $\mathbb{R}$ (Exercise 2.1.2). The ring of quaternions is isomorphic to $M_2(k)$, if k is equal to $\mathbb{C}$ (Exercise 2.1.4). If k is equal to $\mathbb{Z}/(2)$, the ring of quaternions is commutative (Exercise 2.1.3).

EXAMPLE 2.1.7. Let R be a commutative ring and G a finite multiplicative group. Assume the order of G is n and enumerate the elements $G = \{g_1, \dots, g_n\}$, starting with the group identity $g_1 = e$. Let $R(G)$ be the set of all formal sums

$$R(G) = \{r_1 g_1 + \cdots + r_n g_n \mid r_i \in R\}.$$

Define addition and multiplication rules on $R(G)$ by

$$\begin{aligned} \sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i &= \sum_{i=1}^{n} (r_i + s_i) g_i \\ \left(\sum_{i=1}^{n} r_i g_i\right)\left(\sum_{i=1}^{n} s_i g_i\right) &= \sum_{i=1}^{n}\sum_{j=1}^{n} (r_i s_j)(g_i g_j) \end{aligned}$$

The additive identity is $0 = 0g_1 + 0g_2 + \cdots + 0g_n$. The multiplicative identity is $1 = 1g_1 + 0g_2 + \cdots + 0g_n$. Then $R(G)$ is a ring. We call $R(G)$ a *group ring*.

If R is a commutative ring and G is a group which is not necessarily finite, we can still define the group ring $R(G)$. In this case, take $R(G)$ to be the set of all finite formal sums

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

EXAMPLE 2.1.8. If A is an abelian group, let $\operatorname{Hom}(A,A)$ be the set of all homomorphisms from A to A. Turn $\operatorname{Hom}(A,A)$ into a ring by coordinate-wise addition and composition of functions:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(g(x)) \end{aligned}$$

DEFINITION 2.1.9. If R is any ring, the *opposite ring of* R is denoted R^o. As an additive abelian group, the opposite ring of R is equal to R. However, the multiplication of R^o is reversed from that of R. Writing the multiplication of R by juxtaposition and multiplication of R^o with the asterisk symbol, we have $x * y = yx$.

DEFINITION 2.1.10. If A is a ring and $B \subseteq A$, then we say B is a *subring* of A if B contains both 0 and 1 and B is a ring under the addition and multiplication rules of A. Let A be a ring. The *center* of A is the set

$$Z(A) = \{x \in A \mid xy = yx \, (\forall y \in A)\}.$$

The reader should verify that $Z(A)$ is a subring of A and $Z(A)$ is a commutative ring. If $x \in Z(R)$, then we say x is *central*.

DEFINITION 2.1.11. A *left ideal* of A is a nonempty subset $I \subseteq A$ such that $(I,+)$ is a subgroup of $(A,+)$ and $ax \in I$ for all $a \in A$ 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*.

DEFINITION 2.1.12. If R and S are rings, a *homomorphism* from R to S is a function $f \colon R \to S$ satisfying

(1) $f(x+y) = f(x) + f(y)$
(2) $f(xy) = f(x)f(y)$
(3) $f(1) = 1$

The *kernel* of the homomorphism f is $\ker(f) = \{x \in R \mid f(x) = 0\}$. The reader should verify that the kernel of f is an ideal in R and that f is one-to-one if and only if $\ker f = (0)$. The *image* of the homomorphism f is $\operatorname{im}(f) = \{f(x) \in S \mid x \in R\}$. The reader should verify that the image of f is a subring of S. An *isomorphism* is a homomorphism $f : R \to S$ that is one-to-one and onto. In this case, we say R and S are *isomorphic*. An *automorphism* of R is a homomorphism $f : R \to R$ that is one-to-one and onto.

EXAMPLE 2.1.13. Standard examples of homomorphisms are listed here.

(1) The natural projection $\mathbb{Z} \to \mathbb{Z}/(n)$ maps an integer to its congruence class modulo n. It is a homomorphism of rings which is onto. The kernel is the subgroup generated by n.
(2) If u is an invertible element of R, the *inner automorphism* of R defined by u is $\sigma_u \colon R \to R$ where $\sigma_u(x) = uxu^{-1}$. The reader should verify that σ_u is a homomorphism of rings and is a one-to-one correspondence.
(3) Suppose R is a commutative ring, H and G are groups and $\theta \colon H \to G$ is a homomorphism of groups. The action $rh \mapsto r\theta(h)$ induces a homomorphism of group rings $R(H) \to R(G)$ (see Example 2.1.7).
    (a) 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 $R(G)$.
    (b) The homomorphism $G \to \langle e \rangle$ induces $\varepsilon : R(G) \to R$. Notice that η is onto, and the kernel of η contains the set of elements $D = \{1 - g \mid g \in G\}$. The reader should verify that the kernel of η is the ideal generated by D in $R(G)$ (see Definition 2.1.14). Sometimes ε is called the *augmentation map*.
(4) 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.)
(5) 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. If R is a domain, the image of χ is called the *prime ring 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 $n = \operatorname{char}(R)$.

DEFINITION 2.1.14. Let R be any ring and $X \subseteq R$. The *left ideal generated by* X is

$$\left\{ \sum_{i=1}^{n} r_i x_i \mid n \geq 1,\ r_i \in R,\ x_i \in X \right\}.$$

The reader should verify that the left ideal generated by X is equal to the intersection of the left ideals containing X. The *ideal generated by* X is

$$\left\{ \sum_{i=1}^{n} r_i x_i s_i \mid n \geq 1,\ r_i, s_i \in R,\ x_i \in X \right\}.$$

The reader should verify that the ideal generated by X is equal to the intersection of the ideals containing X. If A and B are left ideals of R, then $A+B$ is the set $\{a+b \mid a \in A,\ b \in B\}$. The reader should verify that if A and B are ideals, then $A+B$ is an ideal. The left ideal generated by the set $\{ab \mid a \in A,\ b \in B\}$ is denoted AB. The reader should verify that if A and B are ideals, then AB is an ideal. A left ideal (or ideal) is *principal* if it is generated by a single element. If I is generated by X, we write $I = (X)$. A commutative ring R is called a *principal ideal ring* if every ideal is a principal ideal. A *principal ideal domain* is an integral domain in which every ideal is principal. Sometimes we say R is a PID.

EXAMPLE 2.1.15. Standard examples of ideals are listed here.

(1) In any ring, the set (0) is an ideal.
(2) In any ring R, if u is invertible, then for any $r \in R$ we see that $r = (ru^{-1})u$ is in the left ideal generated by u. That is, $(u) = R$. We call R the *unit ideal* of R. In R, the *trivial ideals* are (0) and R. If R is a division ring, the only left ideals in R are the trivial ideals.
(3) The ideals in $\mathbb{Z}$ are precisely the subgroups of $(\mathbb{Z}, +)$. That is, I is an ideal of $\mathbb{Z}$ if and only if $I = (n)$ for some n. The ring $\mathbb{Z}$ is a principal ideal domain.

DEFINITION 2.1.16. Let R be a ring and I an ideal in R. The *residue class ring* is the set $R/I = \{a+I \mid a \in R\}$ of all left cosets of I in R. We sometimes call R/I the factor ring, or quotient ring of R modulo I. We define addition and multiplication of cosets by the rules

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

The reader should verify that R/I is a ring with additive identity $0+I$ and multiplicative identity $1+I$. Let $\eta\colon R \to R/I$ be the natural map defined by $x \mapsto x+I$. Then η is a homomorphism, $\operatorname{im}\eta = R/I$, and $\ker\eta = I$.

PROPOSITION 2.1.17. *Let $\theta\colon R \to S$ be a homomorphism of rings. Let I be an ideal of R contained in $\ker\theta$. There exists a homomorphism $\varphi\colon R/I \to S$ satisfying the following.*

(1) $\varphi(a+I) = \theta(a)$, or in other words $\theta = \varphi\eta$.
(2) φ is the unique homomorphism from $R/I \to S$ such that $\theta = \varphi\eta$.
(3) $\operatorname{im}\theta = \operatorname{im}\varphi$.
(4) $\ker\varphi = \eta(\ker\theta) = \ker(\theta)/I$.
(5) φ is one-to-one if and only if $I = \ker\theta$.
(6) φ is onto if and only if θ is onto.

(7) *There is a unique homomorphism $\phi\colon R/I \to R/\ker\theta$ such that the diagram*

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

commutes.

PROOF. Is left to the reader. □

PROPOSITION 2.1.18. *Let R be a ring and $I \subseteq J \subseteq R$ a chain of ideals in R. Then J/I is an ideal in R/I and*

$$R/J \cong \frac{R/I}{J/I}.$$

PROOF. Is left to the reader. □

DEFINITION 2.1.19. 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. By Definition 2.1.3, an integral domain has at least two elements, so the unit ideal is never prime.

PROPOSITION 2.1.20. *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.*

PROOF. Is left to the reader. □

EXAMPLE 2.1.21. In an integral domain, the zero ideal (0) is a prime ideal. In a commutative ring R, the zero ideal (0) is a maximal ideal if and only if R is a field (Exercise 2.1.11). Let P be a nonzero prime ideal in $\mathbb{Z}$. Then $\mathbb{Z}/P$ is a finite integral domain which is a field, by Exercise 2.1.15. The maximal ideals in $\mathbb{Z}$ are the nonzero prime ideals.

PROPOSITION 2.1.22. *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 $J \subseteq P$.*

PROOF. Is left to the reader. □

PROPOSITION 2.1.23. *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) *R contains a maximal ideal.*
(3) *If I is a proper ideal of R, then R contains a maximal ideal M such that $I \subseteq M$.*

PROOF. (1): By Exercise 2.1.11 and Proposition 2.1.20 R/M is a field if and only if there is no proper ideal J such that $M \subsetneq J$.

(2): Let $\mathscr{S}$ be the set of all ideals I in R such that $I \neq R$. Then $(0) \in \mathscr{S}$. Order $\mathscr{S}$ by set inclusion. Let $\{A_\alpha\}$ be a chain in $\mathscr{S}$. The union $J = \bigcup A_\alpha$ is an ideal in R, by Exercise 2.1.13. Since 1 is not in any element of $\mathscr{S}$, it is clear that $1 \notin J$. Therefore, $J \in \mathscr{S}$ is an upper bound for the chain $\{A_\alpha\}$. By Zorn's Lemma, Proposition 1.3.3, $\mathscr{S}$ contains a maximal member. By Part (1), this ideal is a maximal ideal.

(3): Is left to the reader. □

1.1. Exercises.

EXERCISE 2.1.1. Prove that if $\theta\colon R \to S$ is a homomorphism of rings, then the image of θ is a subring of S.

EXERCISE 2.1.2. Prove that the ring of quaternions (see Example 2.1.6) over $\mathbb{Q}$ (or $\mathbb{R}$) is a division ring.

EXERCISE 2.1.3. Let $G = \langle a, b \mid a^2 = b^2 = e,\ ab = ba \rangle$ be an elementary 2-group of order 4. Let $R = \mathbb{Z}/(2)$ be the field with 2 elements. For the definition of the ring of quaternions, see Example 2.1.6. For the definition of a group ring, see Example 2.1.7.

(1) Prove that the ring of quaternions over R is isomorphic to the group ring $R(G)$.
(2) Determine the group of units in $R(G)$.
(3) Determine the set of zero divisors in $R(G)$.
(4) Determine all elements in $R(G)$ that satisfy the equation $e^2 = e$. These elements are the so-called idempotents.

EXERCISE 2.1.4. Prove that the ring of quaternions over $\mathbb{C}$ is isomorphic to $M_2(\mathbb{C})$. (Hint: Find matrices that play the roles of i and j.)

EXERCISE 2.1.5. Let R be the ring $M_2(\mathbb{Z}/(2))$ of two-by-two matrices over $\mathbb{Z}/(2)$.

(1) Determine the group of units in R.
(2) Determine the set of zero divisors in R.
(3) Determine all elements in R that satisfy the equation $e^2 = e$. These elements are the so-called idempotents in R.

EXERCISE 2.1.6. If $\theta\colon R \to S$ is a homomorphism of rings, then θ is one-to-one if and only if $\ker\theta = (0)$.

EXERCISE 2.1.7. Let R be any ring.

(1) If $n = \operatorname{char} R$, then $nx = 0$ for any $x \in R$.
(2) If R is a domain, then the characteristic of R is either 0 or a prime number.

EXERCISE 2.1.8. Let R be any ring. Let x and y be elements of R such that $xy = yx$. Prove the Binomial Theorem:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

for any $n \geq 0$.

EXERCISE 2.1.9. Let R be any ring and suppose $p = \operatorname{char} R$ is a prime number. Let x and y be elements of R such that $xy = yx$. Prove:

(1) $(x+y)^p = x^p + y^p$.
(2) $(x-y)^p = x^p - y^p$.

(3) $(x-y)^{p-1} = \sum_{i=0}^{p-1} x^i y^{p-1-i}$.

(Hint: $\binom{p}{i}$ is divisible by p for $i = 1, \dots, p-1$.)

EXERCISE 2.1.10. Let R be a commutative ring and assume $\operatorname{char} R = p$ is a prime number. Define $\theta \colon R \to R$ by $x \mapsto x^p$. Show that θ is a homomorphism of rings. We usually call θ the *Frobenius homomorphism*. For any $a \geq 1$, show that $\theta^a(x) = x^{p^a}$.

EXERCISE 2.1.11. Let G be a monoid. Prove:

(1) An invertible element of G has a unique inverse.
(2) If $x \in G$ has a left inverse, say ℓ, and a right inverse, say r, then $\ell = r$.
(3) If every element in G has a left inverse, then G is a group.
(4) If R is a ring with no proper left ideal, then every nonzero element has a left inverse.
(5) If R is a ring with no proper left ideal, then R is a division ring. (Hint: $R - (0)$ is a monoid.)
(6) A commutative ring R is a field if and only if R has no proper ideal.

EXERCISE 2.1.12. Let R be a ring and $M_n(R)$ the ring of n-by-n matrices over R where addition and multiplication are defined in the usual way.

(1) Let e_{ij} be the elementary matrix which has 0 in every position except in position (i, j) where there is 1. Determine the left ideal in $M_n(R)$ generated by e_{ij}.
(2) If $n \geq 2$, show that $M_n(R)$ has proper left ideals.
(3) If I is an ideal in $M_n(R)$, show that $I = M_n(J)$ for some ideal J in R. (Hint: Use multiplication by the various E_{ij}.)
(4) If D is a division ring, show that $M_n(D)$ has no proper ideal. We say that $M_n(D)$ is a *simple ring*.

EXERCISE 2.1.13. Let R be a ring, I an index set, and $\{A_i \mid i \in I\}$ a family of left ideals in R.

(1) Show that $\bigcap_{i \in I} A_i$ is a left ideal in R.
(2) Suppose $\{A_i \mid i \in I\}$ is an ascending chain of left ideals in R. That is, I is a partially ordered set that is a chain, and if $\alpha \leq \beta$ in I, then $A_\alpha \subseteq A_\beta$. Show that $\bigcup_{i \in I} A_i$ is a left ideal in R.

EXERCISE 2.1.14. Let U and V be ideals in the commutative ring R. Let UV be the ideal generated by the set $\{uv \mid u \in U, v \in V\}$. Prove the following.

(1) $UV \subseteq U \cap V$.
(2) If $U + V = R$, then $UV = U \cap V$.
(3) Show by counterexample that $UV = U \cap V$ is false in general.

EXERCISE 2.1.15. Prove that a finite domain is a division ring, hence a finite integral domain is a field. By a theorem of Wedderburn ([**10**, Theorem 7.5.4]), a finite division ring is always commutative.

EXERCISE 2.1.16. Let $n > 1$.

(1) Show that every prime ideal in $\mathbb{Z}/(n)$ is a maximal ideal.
(2) Let $n = \pi_1^{e_1} \cdots \pi_k^{e_k}$ be the unique factorization of n (Proposition 1.2.7). Determine the maximal ideals in $\mathbb{Z}/(n)$.

EXERCISE 2.1.17. An element x of a ring is said to be *nilpotent* if $x^n = 0$ for some $n > 0$. If R is a commutative ring, let $\operatorname{Rad}_R(0)$ denote the set of all nilpotent elements of R. We call $\operatorname{Rad}_R(0)$ the *nil radical* of R.

(1) Show that $\operatorname{Rad}_R(0)$ is an ideal.
(2) Let I be an ideal of R contained in $\operatorname{Rad}_R(0)$. Show that the nil radical of R/I is $\operatorname{Rad}_R(0)/I$, hence the nil radical of $R/\operatorname{Rad}_R(0)$ is the trivial ideal $(0+\operatorname{Rad}_R(0))$.

EXERCISE 2.1.18. Let $\theta\colon R \to S$ be a homomorphism of rings. Prove that θ induces a homomorphism $\theta\colon \operatorname{Units}(R) \to \operatorname{Units}(S)$ on the groups of units.

EXERCISE 2.1.19. Let R be a commutative ring, $\operatorname{Rad}_R(0)$ the nil radical of R, and $\eta\colon R \to R/\operatorname{Rad}_R(0)$ the natural map. Prove:

(1) If x is a nilpotent element of R, then $1+x$ is a unit in R.
(2) If $\eta(r)$ is a unit in $R/\operatorname{Rad}_R(0)$, then r is a unit in R.
(3) If I is an ideal of R contained in $\operatorname{Rad}_R(0)$, then the natural map $\eta\colon \operatorname{Units}(R) \to \operatorname{Units}(R/I)$ is onto and the kernel of η is equal to the coset $1+I$.

EXERCISE 2.1.20. Let I and J be ideals in the commutative ring R. The *ideal quotient* is $I : J = \{x \in R \mid xJ \subseteq I\}$. Prove that $I : J$ is an ideal in R.

EXERCISE 2.1.21. For the following, let I, J and K be ideals in the commutative ring R. 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

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

EXERCISE 2.1.22. 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) A field is a local ring.
(2) If $(R,\mathfrak{m})$ is a local ring, then the group of units of R is equal to the set $R-\mathfrak{m}$.
(3) 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 2.1.23. Let R be a ring. If A and B are left ideals in R, then the product ideal AB is defined in Definition 2.1.14. The powers of A are defined recursively by the rule:

$$A^n = \begin{cases} R & \text{if } n=0,\\ A & \text{if } n=1,\\ AA^{n-1} & \text{if } n>1. \end{cases}$$

The left ideal A is *nilpotent* if for some $n>0$, $A^n=0$. Let A and B be nilpotent left ideals of R. Prove:

(1) Assume $A^n=0$. If $x_1,\dots,x_n$ are elements of A, then $x_1\cdots x_n=0$.
(2) Every element x of A is nilpotent.
(3) $A+B$ is a nilpotent left ideal. (Hint: For all p sufficiently large, if $x_1,\dots,x_p$ are elements of $A\cup B$, show that $x_1\cdots x_p=0$.)

EXERCISE 2.1.24. Let R be a commutative ring and $\{x_1,\dots,x_n\}$ a finite set of nilpotent elements of R. Show that $Rx_1+\cdots+Rx_n$ is a nilpotent ideal.

EXERCISE 2.1.25. Let R be a ring. We say that a left ideal M of R is *maximal* if M is not equal to R and if I is a left ideal such that $M \subseteq I \subsetneq R$, then $M = I$. Let I be a left ideal of R which is not the unit ideal. Show that there exists a maximal left ideal M such that $I \subseteq M \subsetneq R$.

EXERCISE 2.1.26. Show that the homomorphic preimage of a prime ideal is a prime ideal. That is, if $f : R \to S$ is a homomorphism of commutative rings and P is a prime ideal in S, then $f^{-1}(P)$ is a prime ideal in R.

2. Direct Products and Direct Sums of Rings

DEFINITION 2.2.1. Let $\{R_i \mid i \in I\}$ be a family of rings. 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 1.3.4. 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 $f(i) = 1$. By Exercise 1.5.9, for each $k \in I$ the canonical projection map

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

is defined by the rule $\pi_k(f) = f(k)$. The reader should verify that π_k is an onto homomorphism of rings. There is a canonical injection map

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

which maps $x \in R_k$ to $\iota_k(x)$ which is equal to x in coordinate k, and 0 elsewhere. The reader should verify that ι_k is a one-to-one homomorphism of additive groups. Moreover, ι_k is multiplicative and we have $\pi_k\iota_k = 1_{R_k}$.

DEFINITION 2.2.2. 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. Moreover, ι_k is multiplicative and we have $\pi_k\iota_k = 1_{R_k}$. These facts are verified as in Definition 2.2.1. The reader should verify that 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.

DEFINITION 2.2.3. Let $\{I_1, \dots, I_n\}$ be a set of ideals in a ring R. The ideal of R generated by the set $I_1 \cup I_2 \cup \cdots \cup I_n$ is called the *sum* of the ideals and is denoted $I_1 + I_2 + \cdots + I_n$. 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 $R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$.

DEFINITION 2.2.4. If R is a ring and I and J are ideals in R, then we say I and J are *comaximal* if $I + J = R$.

DEFINITION 2.2.5. Let R be a ring. An element e of R satisfying $e^2 = e$ is said to be *idempotent*. 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 $i \neq j$.

THEOREM 2.2.6. *If $A_1, \dots, A_n$ 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 $\{e_1, \dots, e_n\}$ 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 sum $A_1 \oplus \cdots \oplus A_n$.
(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.

PROOF. (1): Assume $x \in A_k \cap \left(\sum_{j \neq k} A_j\right)$. Let $x_k = -x$. Since $x \in \sum_{j \neq k} A_j$, write $x = \sum_{j \neq k} x_j$ where each $x_j \in A_j$. Subtracting, $0 = x - x = x_1 + \cdots + x_k + \cdots + x_n$. By the uniqueness of the representation of 0 in the internal direct sum, it follows that $x = 0$.

(2): Notice that xy and yx are both in $A_i \cap A_j$ since the ideals are two-sided.

(3): Because A_i is an ideal, it is enough to show that A_i has a multiplicative identity. Write $1 = e_1 + e_2 + \cdots + e_n$. If $x \in A_i$, then multiply by x from the left and use Part (2) to get $x = x1 = \sum_{j=1}^{n} x e_j = x e_i$. Now multiply by x from the right and use Part (2) to get $x = 1x = \sum_{j=1}^{n} e_j x = e_i x$. This shows e_i is the multiplicative identity for A_i. The the rest is left to the reader.

(4): Define a function $f : A_1 \oplus A_2 \oplus \cdots \oplus A_n \to R$ from the external ring direct sum to R by the rule $(x_1, x_2, \dots, x_n) \mapsto x_1 + x_2 + \cdots + x_n$. Then f is one-to-one and onto since R is the internal direct sum of the ideals A_i. Clearly f is additive. The reader should verify using Part (2) that f is multiplicative.

(5): Since each element r in $R = A_1 + A_2 + \cdots + A_n$ has a unique representation in the form $r = r_1 + r_2 + \cdots + r_n$, so does any element x in $I = I_1 + I_2 + \cdots + I_n$. So the sum is a direct sum and we can write $x = x_1 + x_2 + \cdots + x_n$ where each $x_k \in I_k$ is unique. Then $rx = r_1x_1 + r_2x_2 + \cdots + r_nx_n$ is in I, which shows I is a left ideal in R.

(6): By Part (3), for each k there is a central idempotent $e_k \in R$ such that $A_k = Re_k$. Let $I_k = e_kI$. Since e_k is central, $I_k = Ie_k$ is a left ideal in R. Since $I \subseteq R$ we have $I_k = Ie_k \subseteq Re_k = A_k$, so I_k is a left ideal in A_k. Since $1 = e_1 + \cdots + e_n$, we see that $I = I_1 + I_2 + \cdots + I_n$. The sum is a direct sum by Part (5). □

PROPOSITION 2.2.7. *Suppose $A_1, \dots, A_n$ are ideals in the ring R satisfying*

(1) $R = A_1 + A_2 + \cdots + A_n$ and

(2) for each k, $A_k \cap \left(\sum_{j \neq k} A_j\right) = (0)$.

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

PROOF. Assume $x_1 + x_2 + \cdots + x_n = 0$ where each $x_i \in A_i$. It is enough to show each $x_k = 0$. This follows from the observation $x_k = -\sum_{j \neq k} x_j$ is in $A_k \cap \left(\sum_{j \neq k} A_j\right) = (0)$. □

THEOREM 2.2.8. *(The Chinese Remainder Theorem). Let R be any ring. If $I_1, \dots, I_n$ are ideals in R and*

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

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

(1) The kernel of ϕ is equal to $I_1 \cap I_2 \cap \cdots \cap I_n$.

(2) ϕ is onto if and only if $n = 1$ or the ideals are pair-wise comaximal, (that is, $I_i + I_j = R$ if $i \neq j$).

PROOF. (1): Clearly the kernel of ϕ is the set of all x in R such that x is in I_k for all k.

(2): Assume ϕ is onto and $n > 1$. For each $1 \leq i \leq n$, consider the idempotent in $R/I_1 \oplus \cdots \oplus R/I_n$ which is 1 in coordinate i and 0 in every other coordinate. Since ϕ is onto, there exists an element $a_i \in R$ such that $b_i = 1 - a_i \in I_i$ and $a_i \in I_j$ whenever $j \neq i$. Therefore, $1 = a_i + b_i$ is in $I_j + I_i$.

Now we prove the converse of (2). If $n = 1$, we can apply Proposition 2.1.17. Therefore, assume $n > 1$ and the ideals are pairwise comaximal. Let $a_1, \dots, a_n$ be arbitrary elements of R. We show that there exists $a \in R$ such that a satisfies the set of linear congruences $a \equiv a_i \pmod{I_i}$.

For each $k = 2, \dots, n$ we have $I_1 + I_k = R$. Write $1 = x_k + y_k$, where $x_k \in I_1$ and $y_k \in I_k$. Multiplying and simplifying, we get

$$\begin{aligned} 1 &= (x_2 + y_2)(x_3 + y_3) \cdots (x_n + y_n) \\ &= (\text{all the terms with at least one } x_k) + y_2y_3 \cdots y_n. \end{aligned}$$

Since $y_2y_3 \cdots y_n \in \bigcap_{k=2}^n I_k$, we see that $1 \in I_1 + \bigcap_{k=2}^n I_k$. Therefore $R = I_1 + \bigcap_{k=2}^n I_k$. Similarly, for each $k \geq 2$, $R = I_k + \bigcap_{j \neq k} I_j$. There exist $u_k \in I_k$, $v_k \in \bigcap_{j \neq k} I_j$ such that $a_k = u_k + v_k$. Then $a_k \equiv u_k + v_k \equiv v_k \pmod{I_k}$. If $j \neq k$, then $v_j \equiv 0 \pmod{I_k}$. If we take $a = v_1 + v_2 + \cdots + v_n$, then we are done. □

2.1. Exercises.

EXERCISE 2.2.1. Suppose the ring R is the internal direct sum $R = A_1 \oplus \cdots \oplus A_n$ where each A_k is an ideal of R. Prove that for each k there exists a central idempotent $e_k \in R$ such that A_k is equal to the ideal generated by e_k.

EXERCISE 2.2.2. Suppose R is a ring and $e \in R$ is a central idempotent. Assume $e \neq 0$ and $e \neq 1$. Let I be the ideal generated by e. Prove that R is equal to the internal direct sum $I \oplus J$ for some ideal J.

EXERCISE 2.2.3. Let k be a field of characteristic different from 2. Let $f = x^2 - 1$. Show that $k[x]/(f)$ is isomorphic to a direct sum of fields.

EXERCISE 2.2.4. Consider the ring $R = \mathbb{Z}/(n)$.

(1) Suppose $n = 1105$.
  (a) Prove that R is isomorphic to a direct sum of fields.
  (b) Determine all maximal ideals in R.
  (c) Determine all idempotents in R.
(2) Suppose $n = 1800$.
  (a) Determine all maximal ideals in R.
  (b) Determine all idempotents in R.

EXERCISE 2.2.5. If $n > 1$, then we say n is squarefree if n is not divisible by the square of a prime number. Prove that the nil radical of $\mathbb{Z}/n$ is (0) if and only if n is squarefree.

EXERCISE 2.2.6. 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 2.2.7. 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 2.1.8.)

EXERCISE 2.2.8. Assume the ring R is the direct sum $R = R_1 \oplus \cdots \oplus R_n$. Let $e_1, \dots, e_n$ be the central idempotents corresponding to the direct summands (guaranteed by Theorem 2.2.6 (3)). Let D be a ring which has only two idempotents, namely 0 and 1. Let $\theta : R \to D$ be a homomorphism of rings. Prove that there exists e_j such that

$$\theta(e_i) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

3. Factorization in Commutative Rings

DEFINITION 2.3.1. Let R be a commutative ring. Suppose a and b are elements of R. We say *a divides b*, and write $a \mid b$, in case there exists $c \in R$ such that $b = ac$. We also say that a is a *factor* of b, or b is a *multiple* of a. If $a \mid b$ and $b \mid a$, then we say a and b are *associates*. The reader should verify that the relation "a is an associate of b" is an equivalence relation on R.

LEMMA 2.3.2. *Let R be a commutative ring. Let $a, b, r \in R$.*

(1) $a \mid b$ if and only if $(a) \supseteq (b)$.
(2) a and b are associates if and only if $(a) = (b)$.
(3) The following are equivalent.
  (a) u is a unit in R.
  (b) $(u) = R$.
  (c) $u \mid r$ for all r in R.
(4) If $a = bu$ and u is a unit, then a and b are associates.
(5) If R is an integral domain and a and b are associates, then $a = bu$ for some unit u.

PROOF. Is left to the reader. □

DEFINITION 2.3.3. Let R be a commutative ring and a an element of R which is not a unit and not a zero divisor. Then a is *irreducible* in case whenever $a = bc$, then either b is a unit or c is a unit. We say that a is *prime* in case whenever $a \mid bc$, then either $a \mid b$ or $a \mid c$.

LEMMA 2.3.4. *Let R be an integral domain.*

(1) *$p \in R$ is prime if and only if (p) is a prime ideal.*
(2) *$a \in R$ is irreducible if and only if (a) is maximal among nonunit principal ideals.*
(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.*

PROOF. (3): Suppose $a,b \in R$ and $p = ab$. So $p \mid ab$ and p is prime. We can assume $p \mid a$. Therefore a and p are associates. By Lemma 2.3.2 (5), b is a unit in R.

The rest is left to the reader. □

DEFINITION 2.3.5. A *unique factorization domain* is an integral domain R in which every nonzero nonunit a can be written as a product $a = p_1 p_2 \cdots p_n$ where each p_i is irreducible and up to order and associates this factorization is unique. Sometimes we say R is *factorial*, or R is a UFD.

PROPOSITION 2.3.6. *If R is a unique factorization domain, and p is irreducible, then p is prime.*

PROOF. Suppose p is irreducible and $p \mid ab$. Write $ab = pc$ for some c. Factor a,b,c into irreducibles. By uniqueness of factorization, p is an associate of one of the irreducible factors of a or b. □

3.1. Principal Ideal Domains. The fundamental properties of a principal ideal domain are derived in Theorem 2.3.7. In particular, every principal ideal domain is a unique factorization domain.

THEOREM 2.3.7. *Let R be a principal ideal domain (a PID, for short).*

(1) *If p is an irreducible element, then p is a prime element.*
(2) *R satisfies the* ascending chain condition *on ideals. That is, given a chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$, there exists $N \geq 1$ such that $I_N = I_{N+1} = \cdots$.*
(3) *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.
(4) (a) *If I is an ideal in R which is not the unit ideal, then $\bigcap_{n \geq 1} I^n = (0)$.*
 (b) *Suppose a is a nonzero element in R, p is irreducible and p is a factor of a. Then for some $n \geq 1$ we have $a \in (p^n)$ and $a \notin (p^{n+1})$.*
(5) *If $a \in R$ is a nonunit and a nonzero element, then there exists an irreducible element p such that $p \mid a$.*
(6) *R is a unique factorization domain.*

PROOF. (1): Since p is irreducible and R is a PID, by Lemma 2.3.4 (2), the principal ideal (p) is maximal. Assume $p \mid ab$ and $p \nmid a$. Then $(p,a) = R$ so there exist $x,y \in R$ such that $1 = ax + py$. Multiplying, $b = abx + pby$. Clearly p divides the right-hand side, so $p \mid b$.

(2): Let $I = \bigcup_{k=1}^{\infty} I_k$. By Exercise 2.1.13, I is an ideal in R. Since R is a PID, there exists $a \in R$ such that $I = (a)$. Given $a \in I$, we know $a \in I_N$ for some N. Then $I = (a) \subseteq I_N \subseteq I_{N+1} \subseteq \cdots$ and we are done.

(3): The proof is by contradiction. Assume $\{p_1, p_2, \dots\}$ is a sequence in $\mathscr{S}$ such that for each $n > 1$, p_n does not divide $p_1 p_2 \cdots p_{n-1}$. Write $a = p_1 a_1$. Then $p_2 \mid p_1 a_1$. By assumption, p_2 does not divide p_1. By Part (1), $p_2 \mid a_1$ and we write $a_1 = p_2 a_2$. Iteratively we arrive at the factorizations

$$a = p_1 a_1 = p_1 p_2 a_2 = \cdots = p_1 p_2 \cdots p_n a_n.$$

Applying one more step, we know $p_{n+1} \mid a$. Since p_{n+1} does not divide $p_1 p_2 \cdots p_n$, and p_{n+1} is prime, it follows that $p_{n+1} \mid a_n$. Write $a_n = p_{n+1} a_{n+1}$. Therefore $(a_n) \subseteq (a_{n+1})$ with equality if and only if a_n and a_{n+1} are associates. But p_{n+1} is not a unit, so by Lemma 2.3.2 (5), the chain of ideals

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \cdots$$

is strictly increasing. This contradicts Part (2).

(4): Because R is a PID, $I = (b)$ for some $b \in R$. If $I = 0$, then Part (a) is trivial, so we assume $b \neq 0$. Let $M = \bigcap_{n=1}^{\infty} I^n$. Then M is an ideal in R, so $M = (r)$ for some $r \in R$. Since M is an ideal, $bM \subseteq M$. To show that $bM = M$, assume $x \in M$. Then $x \in M \subseteq I$ implies $x = by$ for some $y \in R$. Let $n \geq 1$. Then $x \in M \subseteq I^{n+1} = (b^{n+1})$ implies $x = b^{n+1} z$ for some $z \in R$. Since R is an integral domain and $b \neq 0$, $x = by = b^{n+1} z$ implies $y = b^n z \in I^n = (b^n)$. This proves $y \in \bigcap_{n \geq 1} I^n = M$. Therefore $x \in bM$, and $bM = M$. Since $bM = (br)$, Lemma 2.3.2 says br and r are associates. But b is not a unit, so $r = 0$, which proves (a). For (b), take $I = (p)$. By assumption, $a \in (p)$ and $a \neq 0$. For some $n \geq 1$ we have $a \notin (p^{n+1})$ and $a \in (p^n)$.

(5): The proof is by contradiction. Suppose $a \in R$ is not a unit, and not divisible by an irreducible. Then a is not irreducible. There are nonunits a_1, b_1 in R such that $a = a_1 b_1$. By our assumption, a_1 and b_1 are not irreducible. By Lemma 2.3.2, $(a) \subsetneq (a_1)$. Since a_1 is not irreducible, there are nonunits a_2, b_2 in R such that $a_1 = a_2 b_2$. Since a_2 and b_2 are divisors of a, they are both irreducible. By Lemma 2.3.2, $(a) \subsetneq (a_1) \subsetneq (a_2)$. Recursively construct a strictly increasing sequence of ideals $(a_i) \subsetneq (a_{i+1})$, contradicting Part (2).

(6): This proof is left to the reader. □

3.2. Euclidean Domains.

DEFINITION 2.3.8. A *euclidean domain* is an integral domain R together with a function $\phi : R - (0) \to \mathbb{N}$, satisfying the following.

(1) If $a, b \in R - (0)$, then $\phi(a) \leq \phi(ab)$.
(2) If $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$, or $\phi(r) < \phi(b)$.

EXAMPLE 2.3.9. Here are two standard examples of euclidean domains.

(1) The ring of integers $\mathbb{Z}$ is a euclidean domain, where ϕ is the absolute value function. Property (2) is the Division Algorithm (Proposition 1.2.3).
(2) The ring of gaussian integers, denoted $\mathbb{Z}[i]$, is the subring of $\mathbb{C}$ consisting of all complex numbers of the form $a + bi$ where $a, b \in \mathbb{Z}$. Define $\phi : \mathbb{Z}[i] \to \mathbb{N}$ by $\phi(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$. If $y \neq 0$, then $\phi(y) \geq 1$. Since $\phi(xy) = \phi(x)\phi(y) \geq \phi(x)$, Property (1) is satisfied. Assume $x = a + bi$ and $N = a^2 + b^2 \neq 0$. Let $y = c + di$. Then $x^{-1} = (a - bi)/N$, so $yx^{-1} = ((c_d i)(a - bi))/N = (e + fi)/N$. Divide in $\mathbb{Z}$ to get $yx^{-1} = (q_1 + r_1/N) + (q_2 + r_2/N)i$. If we assume

$0 \le |r_i| \le N/2$, then $r_1^2 + r_2^2 \le N^2/4 < N^2$. Let $q = q_1 + q_2 i$. Then

$$\begin{aligned}
yx^{-1} &= q + (r_1 + r_2)/N \\
y(a-bi) &= qN + (r_1 + r_2) \\
y(a-bi) &= qx(a-bi) + (r_1 + r_2) \\
(y-qx)(a-bi) &= (r_1 + r_2) \\
\phi(y-qx)(a^2+b^2) &= r_1^2 + r_2^2 < (a^2+b^2)^2 \\
\phi(y-qx) &< a^2 + b^2 = \phi(x)
\end{aligned}$$

Set $r = y - qx$. Then $\phi(r) < \phi(x)$, hence Property (2) is satisfied. Therefore, $\mathbb{Z}[i]$ is a euclidean domain.

THEOREM 2.3.10. *If R is a euclidean domain, then R is a principal ideal domain.*

PROOF. Let I be a nonzero ideal in R. Let M be the least element of the set $\{\phi(x) \mid x \in I - (0)\}$. Let $a \in I - (0)$ such that $\phi(a) = M$. Let $u \in I$. Dividing, $u = qa + r$ and either $r = 0$, or $\phi(r) < \phi(a)$. Since $r = u - qa \in I$ we conclude that $r = 0$. □

3.3. Greatest Common Divisors.

DEFINITION 2.3.11. Let R be a commutative ring and X a nonempty subset of R. An element $d \in R$ is said to be the GCD (short for *greatest common divisor*) of X, if the following are satisfied.

(1) $d \mid x$ for all $x \in X$.
(2) If $c \mid x$ for all $x \in X$, then $c \mid d$.

If d is the GCD of X, we write $d = \mathrm{GCD}(X)$. If $d = \mathrm{GCD}(X)$ exists and $d = 1$, then we say the elements of X are *relatively prime*.

PROPOSITION 2.3.12. *Let R be a commutative ring and X a nonempty subset of R.*

(1) If the ideal generated by X is principal and d is a generator for (X), then $d = \mathrm{GCD}(X)$.
(2) If $d = \mathrm{GCD}(X)$ exists and d is in the ideal (X), then $(d) = (X)$.
(3) If R is a PID, then $d = \mathrm{GCD}(X)$ exists and $(d) = (X)$.
(4) If R is a UFD, and $X = \{x_1, \dots, x_n\}$ is a finite nonempty subset of R, then $d = \mathrm{GCD}(X)$ exists and is unique up to associates.

PROOF. (1) and (2): Are left to the reader.

(3): Since R is a PID, $(X) = (d)$ for some $d \in (X)$. Then $d \mid x$ for all $x \in X$ and $d = r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$ for some finite subset $\{x_1, \dots, x_n\} \subseteq X$. If $c \mid x$ for all $x \in X$, then clearly $c \mid d$.

(4): Factor each x_i into a product of irreducibles. By allowing exponents of zero, we can assume $x_i = p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_m^{e_{im}}$ where the p_i are distinct irreducibles (up to associates) and each $e_{ij} \ge 0$. Let ℓ_j be the least element in the set $\{e_{1j}, e_{2j}, \dots, e_{nj}\}$ and set $d = p_1^{\ell_1} p_2^{\ell_2} \cdots p_m^{\ell_m}$. The reader should verify that $d = \mathrm{GCD}(x_1, \dots, x_n)$. □

4. Ring of Quotients

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 2.4.1. Here are some typical examples of multiplicative sets.

(1) If P is a prime ideal in R, then Proposition 2.1.22 says that $R-P$ is a multiplicative set.
(2) If R is an integral domain, then $W=R-(0)$ is a multiplicative set.
(3) If $f\in R$, then $\{1,f,f^2,f^3,\dots\}$ is a multiplicative set.
(4) The set of all $x\in R$ such that x is not a zero divisor is a multiplicative set.

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 2.4.2. *Let R be a commutative ring and W a multiplicative subset of R.*

(1) $W^{-1}R$ 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 $1/1$.

(2) 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 $W^{-1}R$.

(3) If R is an integral domain and $W\subseteq R-(0)$, then the following are true.
  (a) The map θ of Part (2) is one-to-one.
  (b) If R is a field, then the map θ of Part (2) is an isomorphism.
  (c) $r/v=s/w$ if and only if $rw=sv$.
  (d) $W^{-1}R$ is an integral domain.
  (e) If $W=R-(0)$, then $W^{-1}R$ is a field, which we call the quotient field *of R.*

PROOF. Is left to the reader. □

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.

THEOREM 2.4.3. *(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 $f(W)\subseteq$ Units(S), then there exists a unique homomorphism $\bar f:W^{-1}R\to S$*

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\theta"'] & & S \\ & W^{-1}R \arrow[ur, dotted, "\exists\bar f"'] & \end{tikzcd}$$

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 $g(x/y) = g(\theta(x))g(\theta(y))^{-1} = f(x)f(y)^{-1} = \bar{f}(x/y)$. □

COROLLARY 2.4.4. *Let R be an integral domain with quotient field K and natural map $\theta : R \to K$. If F is a field and $f : R \to F$ is a monomorphism, then there exists a unique $\bar{f} : K \to F$ such that $f = \bar{f}\theta$.*

4.1. Exercises.

EXERCISE 2.4.1. Let R be a commutative ring and $f \in R$. As remarked in Example 2.4.1 (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 $R[(\alpha\beta)^{-1}]$ and $R[\alpha^{-1}][(\beta/1)^{-1}]$ are isomorphic as rings.
(2) If $i > 0$, then $R[\alpha^{-1}]$ and $R[\alpha^{-i}]$ are isomorphic as rings.

EXERCISE 2.4.2. 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 2.4.3. 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 $W \subseteq \text{Units}(R)$.

5. Polynomial Rings

Let R be any ring. The *polynomial ring* in one variable x with coefficients in R,

$$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid n \geq 0, a_i \in R \right\}$$

is constructed in the usual way. It is assumed that the *indeterminate* x commutes with elements of R. The ring $R[x]$ is commutative if and only if R is commutative. If $a \in R - (0)$, the *degree* of the *monomial* ax^n is n. For convenience, the degree of 0 is taken to be $-\infty$. The *degree* of a polynomial $f = \sum_{i=0}^{n} a_i x^i$ in $R[x]$ is the maximum of the degrees of the the terms $a_0x^0, \dots, a_nx^n$. If f is nonzero of degree n, the *leading coefficient* of f is a_n. We say that f is *monic* if the leading coefficient of f is 1. If $f = \sum_{i=0}^{m} a_i x^i$ has degree m and $g = \sum_{i=0}^{n} b_i x^i$ has degree n, then

$$\begin{aligned} fg &= \left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + \left(\sum_{j=0}^{k} a_j b_{k-j}\right) x^k + \cdots + a_m b_n x^{m+n}. \end{aligned}$$

It follows that $\deg(fg) = \deg(f) + \deg(g)$ in case one of the leading coefficients a_m or b_n is not a zero divisor in R.

LEMMA 2.5.1. *If R is a domain, then $R[x]$ is a domain.*

PROOF. The proof is left to the reader. □

The natural mapping $R \to R[x]$ which maps $a \in R$ to the polynomial of degree zero is a monomorphism. The polynomial ring over R in several variables $x_1, \dots, x_n$ is defined by iterating the one-variable construction: $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$.

THEOREM 2.5.2. *Let $\sigma : R \to S$ be a homomorphism of rings.*

1. *The definition $\bar{\sigma}(\sum r_i x^i) = \sum \sigma(r_i) x^i$ extends σ to a homomorphism on the polynomial rings $\bar{\sigma} : R[x] \to S[x]$. If $K = \ker(\sigma)$, then the kernel of $\bar{\sigma}$ is the set $K[x]$ consisting of those polynomials $f \in R[x]$ such that every coefficient of f is in K.*
2. *(Universal Mapping Property) Let s be an element of S such that $s\sigma(r) = \sigma(r)s$ for every $r \in R$. Then there is a unique homomorphism $\bar{\sigma}$ such that $\bar{\sigma}(x) = s$ and the diagram*

$$\begin{tikzcd} R \arrow[rr, "\sigma"] \arrow[dr] & & S \\ & R[x] \arrow[ur, "\bar{\sigma}"'] & \end{tikzcd}$$

commutes. We say $\bar{\sigma}$ is the evaluation homomorphism *defined by $x \mapsto s$.*

PROOF. The proof is left to the reader. □

THEOREM 2.5.3. *(The Division Algorithm) Let R be any ring. Let $f, g \in R[x]$ and assume the leading coefficient of g is a unit of R. There exist unique polynomials $q, r \in R[x]$ such that $f = qg + r$ and* $\deg r < \deg g$.

PROOF. If $\deg f < \deg g$, then set $q = 0$ and $r = f$. Otherwise assume $f = \sum_{i=0}^{m} a_i x^i$ where $a_m \neq 0$ and $g = \sum_{i=0}^{n} b_i x^i$ where $b_n \neq 0$ and b_n is a unit in R. If $m = 0$, then $n = 0$ so $q = a_0 b_0^{-1}$ and $r = 0$. Proceed by induction on m. Divide g into f to get

$$\left(a_m b_n^{-1} x^{m-n}\right) g = f + h$$

where $\deg h < \deg f$. By induction, $h = q_1 g + r$ where $\deg r < \deg g$. Now

$$\begin{aligned} f &= \left(a_m b_n^{-1} x^{m-n}\right) g + q_1 g + r \\ &= \left(a_m b_n^{-1} x^{m-n} + q_1\right) g + r \end{aligned}$$

so take $q = a_m b_n^{-1} x^{m-n} + q_1$. The reader should verify that the quotient and remainder are unique. □

COROLLARY 2.5.4. *(Synthetic Division) If R is any ring, $f = \sum_{i=0}^{m} r_i x^i \in R[x]$ and $a \in R$, then there exists a unique polynomial $q \in R[x]$ such that $f = q(x-a) + f(a)$ where $f(a) = \sum_{i=0}^{m} r_i a^i \in R$.*

PROOF. If a is in the center of R, then upon dividing $x - a$ into f, this follows straight from Theorem 2.5.3. If $\deg f \leq 0$, then take $q = 0$. Otherwise assume $m = \deg f \geq 1$. Notice that

$$x^{k+1} - a^{k+1} = \left(x^k + a x^{k-1} + \cdots + a^{k-1} x + a^k\right)(x - a).$$

Multiply by r_{k+1} to get

$$r_{k+1}\left(x^{k+1} - a^{k+1}\right) = r_{k+1}\left(x^k + a x^{k-1} + \cdots + a^{k-1} x + a^k\right)(x - a),$$

which can be written

$$r_{k+1} x^{k+1} - r_{k+1} a^{k+1} = q_{k+1}(x - a).$$

Add over all k in the range $0, 1, \dots, n-1$:

$$\sum_{i=1}^{n} r_i x^i - \sum_{i=1}^{n} r_i a^i = \left(\sum_{i=1}^{n} q_i \right) (x-a) = q(x-a).$$

To get $f - f(a) = q(x-a)$, simply add $r_0 - r_0$ to the left-hand side. The quotient q and remainder $f(a)$ are unique by Theorem 2.5.3. □

COROLLARY 2.5.5. *If k is a field, then $k[x]$ is a euclidean domain with the degree function* $\deg : k[x] - (0) \to \mathbb{N}$. *It follows that $k[x]$ is a PID and a UFD.*

If k is a field, and $R = k[x]$, then the quotient field of $k[x]$, denoted $k(x)$, is called thefield of rational functions over k. If S is a ring and R a subring, then by Theorem 2.5.2 we can view $R[x]$ as a subring of $S[x]$.

DEFINITION 2.5.6. Let R be any ring, $u \in R$, and $f = \sum_{i=0}^{m} r_i x^i \in R[x]$. We say that u is a *root* of f in case $f(u) = \sum_{i=0}^{m} r_i u^i = 0$.

LEMMA 2.5.7. *Let R be a commutative ring, $u \in R$, and $f \in R[x]$. The following are equivalent.*

(1) u is a root of f.
(2) f is in the kernel of the evaluation homomorphism $R[x] \to R$ defined by $x \mapsto u$.
(3) There exists $q \in R[x]$ such that $f = (x-u)q$.

PROOF. The proof is left to the reader. □

COROLLARY 2.5.8. *If R is an integral domain, and $f \in R[x]$ has degree $d \geq 0$, then*

(1) If u is a root of f in R, then there exists $m \geq 1$ such that $f = (x-u)^m q$ and $q(u) \neq 0$.
(2) f has at most d roots in R.

PROOF. (1): Apply Lemma 2.5.7 and induction on the degree.

(2): If $d = 0$, then f has no root. Inductively assume $d \geq 1$ and that the result holds for any polynomial of degree in the range $0, \dots, d-1$. If f has no root, then we are done. Suppose u is a root of f. By Part (2) we can write $f = (x-u)^m q$, where $\deg q = d - m$. If $v \neq u$ is another root of f, then $0 = f(u) = (v-u)^m q(u)$. Since R is an integral domain, this means u is a root of q. By induction, there are at most $d - m$ choices for v. □

PROPOSITION 2.5.9. *(The Rational Root Theorem) Suppose R is a UFD with quotient field K and $u = b/c$ is an element of K such that* $\operatorname{GCD}(b,c) = 1$. *If $f = a_0 + a_1 x + \cdots + a_d x^d \in R[x]$ and u is a root of f, then $b \mid a_0$ and $c \mid a_d$.*

PROOF. If $f(b/c) = 0$, then

$$a_0 + \frac{a_1 b}{c} + \frac{a_2 b^2}{c^2} + \cdots + \frac{a_d b^d}{c^d} = 0.$$

Multiply by c^d

$$a_0 c^d + a_1 b c^{d-1} + a_2 b^2 c^{d-2} + \cdots + a_d b^d = 0.$$

Since b divides the last d terms, it follows that $b \mid a_0 c^d$. Since c divides the first d terms, it follows that $c \mid a_d b^d$. Since $\operatorname{GCD}(b,c) = 1$ and R is a UFD, it follows that $b \mid a_0$ and $c \mid a_d$. □

DEFINITION 2.5.10. If R is an integral domain, $f \in R[x]$, and u is a root of f, then the *multiplicity* of u as a root of f is the positive number m given by Corollary 2.5.8 (1). We say that u is a *simple root* if $m = 1$. If $m > 1$, then u is called a *multiple root*.

DEFINITION 2.5.11. If R is any ring and $f = \sum_{i=0}^{n} a_i x^i \in R[x]$, then the *formal derivative* of f is defined to be

$$f' = \sum_{i=1}^{n} i a_i x^{i-1}$$

which is also in $R[x]$. The reader should verify the usual identities satisfied by the derivative operator. In particular, $(af+bg)' = af' + bg'$ and $(fg)' = f'g + fg'$. If R is commutative, then $(f^n)' = nf^{n-1}f'$.

PROPOSITION 2.5.12. *Suppose S is an integral domain and R is a subring of S. Let f be a nonconstant polynomial in $R[x]$ and $u \in S$. Then u is a multiple root of f if and only if $f'(u) = f(u) = 0$.*

PROOF. Suppose u is a multiple root of f. Write $f = (x-u)^2 q$ for some $q \in S[x]$ and compute $f' = 2(x-u)q + (x-u)^2 q'$. It is immediate that $f'(u) = 0$. Conversely, assume $f(u) = f'(u) = 0$. Write $f = (x-u)q$ for some $q \in S[x]$ and compute $f' = q + (x-u)q'$. It is immediate that $q(u) = 0$, so $f = (x-u)^2 q_2$ for some $q_2 \in S[x]$. □

THEOREM 2.5.13. *Let k be a subfield of the integral domain S and f a nonconstant polynomial in $k[x]$.*

(1) Assume
   (a) $\mathrm{GCD}(f, f') = 1$, or
   (b) f is irreducible in $k[x]$ and $f' \neq 0$ in $k[x]$, or
   (c) f is irreducible in $k[x]$ and k has characteristic zero.
   Then f has no multiple root in S.

(2) Suppose p denotes the characteristic of k. Assume u is a root of f in S.
   (a) If f is irreducible in $k[x]$ and u is a multiple root of f, then $p > 0$ and $f \in k[x^p]$.
   (b) If $p > 0$ and $f \in k[x^p]$, then u is a multiple root of f.

PROOF. (1): Assuming $\mathrm{GCD}(f, f') = 1$, by Proposition 2.3.12 there exist $s, t \in k[x]$ such that $1 = fs + f't$. It is clear that f and f' do not have a common root in S. By Proposition 2.5.12, f has no multiple root in S. Case (b) reduces immediately to case (a). Case (c) reduces immediately to case (b).

(2) (a): If $u \in S$ is a multiple root of f, then because f is irreducible in $k[x]$, Part (1) implies $p > 0$ and $f' = 0$. The reader should verify that under these conditions $f \in k[x^p]$.

(2) (b): If k has characteristic $p > 0$ and $f \in k[x^p]$, then clearly $f' = 0$. If $u \in S$ is a root of f, then by Proposition 2.5.12, u is a multiple root of f. □

5.1. Exercises.

EXERCISE 2.5.1. 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 2.5.2. Let $f = x^3 + 1$. Prove that there is an isomorphism $\theta : \mathbb{Q}[x]/(f) \to F_1 \oplus F_2$ where F_1 and F_2 are fields. Carefully describe the fields F_1 and F_2, and the map θ.

EXERCISE 2.5.3. Let k be a field. Let $R = k[x^2, x^3]$ be the subring of $k[x]$ consisting of all polynomials such that the coefficient of x is zero. Prove:

(1) R is an integral domain.
(2) R is not a UFD. (Hint: x^2 and x^3 are both irreducible.)
(3) R is not a PID. (Hint: Neither x^2 nor x^3 is prime.)

(4) The converse of Lemma 2.3.4 (3) is false.

EXERCISE 2.5.4. Let F be a field of positive characteristic p. Let $\theta : F[y] \to F[y]$ be the evaluation mapping given by $y \mapsto y^p$. Let $F[y^p]$ denote the image of θ. Prove that θ extends to a homomorphism $\chi : F(y) \to F(y)$ and let $F(y^p)$ be the image of χ. Prove that $F(y^p)$ is the quotient field of $F[y^p]$ and that the diagram

$$\begin{tikzcd}
F[y] \arrow[r] & F(y) \\
F[y^p] \arrow[u] \arrow[r] & F(y^p) \arrow[u]
\end{tikzcd}$$

commutes where each of the four maps is the set inclusion homomorphism.

EXERCISE 2.5.5. Let $K = F(y^p)$ be the subfield of $L = F(y)$ defined as in Exercise 2.5.4. We say that L/K is an extension of fields. Show that the polynomial $f = x^p - y^p$ is irreducible in $K[x]$, but that $f = (x-y)^p$ in $L[x]$.

EXERCISE 2.5.6. Prove that if R is an integral domain, then the homomorphism $R \to R[x]$ induces an isomorphism on the groups of units $\text{Units}(R) \to \text{Units}(R[x])$.

EXERCISE 2.5.7. Prove that if R is a commutative ring and $\text{Rad}_R(0) = (0)$, then the homomorphism $R \to R[x]$ induces an isomorphism on the groups of units $\text{Units}(R) \to \text{Units}(R[x])$.

EXERCISE 2.5.8. Let R be a commutative ring. Prove:

(1) The nil radical of $R[x]$ is equal to $\text{Rad}_R(0)[x]$. That is, a polynomial is nilpotent if and only if every coefficient is nilpotent.
(2) The kernel of $R[x] \to (R/\text{Rad}_R(0))[x]$ is equal to the nil radical of $R[x]$.
(3) The group of units of $R[x]$ consists of those polynomials of the form $f = a_0 + a_1x + \cdots + a_nx^n$, where a_0 is a unit in R and $f - a_0 \in \text{Rad}_R(0)[x]$.

EXERCISE 2.5.9. (GCD is invariant under a change of base field) Let $k \subseteq F$ be a tower of fields such that k is a subfield of F. In this case we view $k[x]$ as a subring of $F[x]$. Let $f, g \in k[x]$. Prove that if d is the greatest common divisor of f and g in $k[x]$, then d is the greatest common divisor of f and g in $F[x]$.

EXERCISE 2.5.10. Let R be an integral domain and $a \in R$. Prove that the linear polynomial $x - a$ is a prime element in $R[x]$.

EXERCISE 2.5.11. Let R be a commutative ring and $a \in R$. Show that there is an automorphism $\theta : R[x] \to R[x]$ such that $\theta(x) = x + a$ and for all $r \in R$, $\theta(r) = r$.

EXERCISE 2.5.12. Let R be an integral domain and a an irreducible element of R. Prove that a is an irreducible element in $R[x]$.

EXERCISE 2.5.13. Let k be a field and $A = k[x]$. Prove:

(1) If $I = (x)$ is the ideal in A generated by x, then $I^n = (x^n)$.
(2) Let $n \geq 1$. The nil radical of $k[x]/(x^n)$ consists of those cosets represented by polynomials of the form $\alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$.
(3) The group of units of $k[x]/(x^n)$ consists of those cosets represented by polynomials of the form $\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$, where α_0 is a unit in k.

EXERCISE 2.5.14. Let R be an integral domain.

(1) A polynomial f in $R[x]$ defines a function $f : R \to R$. If R is infinite, show that f is the zero function (that is, $f(a) = 0$ for all $a \in R$) if and only if f is the zero polynomial.
(2) A polynomial f in $R[x_1,\dots,x_r]$ defines a function $f : R^r \to R$. If R is infinite, use induction on r to show f is the zero function if and only if f is the zero polynomial.

EXERCISE 2.5.15. Let R be a commutative ring and $S = R[x]$ the polynomial ring in one variable over R. If $W = \{1, x, x^2, \dots\}$, then the localization $W^{-1}S$ is called the *Laurent polynomial ring* over R. Usually, the ring of Laurent polynomials over R is denoted $R[x, x^{-1}]$.

(1) Let $G = (a)$ be the infinite cyclic group generated by a and $R(G)$ the group ring over R. Prove that $R[x, x^{-1}] \cong R(G)$.
(2) Prove that $R[x, x^{-1}] \cong R[x,y]/(xy-1)$.

EXERCISE 2.5.16. Let R be a commutative ring, A an R-algebra, and $a \in A$. Let $\sigma : R[x] \to A$ be the evaluation map defined by $x \mapsto a$. Let $R[a]$ denote the image of σ. Show that $R[a]$ is the smallest subring of A containing $R \cdot 1$ and a. Show that $R[a]$ is commutative.

EXERCISE 2.5.17. 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 $x \mapsto \zeta x$.

6. Polynomials over a Unique Factorization Domain

Let R be a unique factorization domain, or UFD for short. Suppose f is a nonzero polynomial in $R[x]$. If we write $f = a_0 + a_1 x + \cdots + a_n x^n$, then the *content* of f, written $C(f)$, is defined to be $\mathrm{GCD}(a_0, a_1, \dots, a_n)$. By Proposition 2.3.12 (4), $C(f)$ is unique up to associates, which means $C(f)$ is unique up to multiplication by a unit of R. If $C(f) = 1$, then we say f is *primitive*. If we factor out the content, then $f = C(f) f_1$ where f_1 is primitive.

LEMMA 2.6.1. *Let R be a UFD with quotient field K. Let $f, g \in R[x]$.*

(1) If f and g are primitive, then fg is primitive.
(2) $C(fg) = C(f)C(g)$.
(3) Suppose f and g are primitive. Then f and g are associates in $R[x]$ if and only if they are associates in $K[x]$.

PROOF. (1): Assume p is an irreducible element of R and p divides $C(fg)$. Under the natural map $\eta : R[x] \to R/(p)[x]$, we have $\eta(fg) = \eta(f)\eta(g) = 0$. By Proposition 2.3.6, p is prime, so $R/(p)$ is an integral domain. Thus $R/(p)[x]$ is an integral domain, which implies one of $\eta(f)$ or $\eta(g)$ is zero. That is, p divides the content of f or the content of g.

(2): Factor $f = C(f) f_1$, $g = C(g) g_1$, where f_1 and g_1 are primitive. Then $fg = C(f)C(g) f_1 g_1$. By Part (1), $f_1 g_1$ is primitive.

(3): By Exercise 2.5.6, a unit in $K[x]$ is a nonzero constant polynomial. Suppose $f = ug$ where $u = r/s$ is a unit in K and $\mathrm{GCD}(r,s) = 1$. Then $sf = rg$ implies $sC(f) = rC(g)$, which implies r and s are associates. Therefore $u = 1$. The converse is trivial, since $R \subseteq K$. □

THEOREM 2.6.2. *(Gauss' Lemma) Suppose f is primitive. Then f is irreducible in $R[x]$ if and only if f is irreducible in $K[x]$.*

PROOF. If f has a nontrivial factorization in $R[x]$, then this factorization still holds in $K[x]$. Assume $f = pq$ is a factorization in $K[x]$, where we assume $m = \deg p \geq 1$, and $n = \deg q \geq 1$. Write

$$p = \sum_{i=0}^{m} \frac{a_i}{b_i} x^i, \quad q = \sum_{i=0}^{n} \frac{c_i}{d_i} x^i$$

and set $b = b_0 b_1 \cdots b_m$, $d = d_0 d_1 \ldots d_m$. Then $b(a_i/b_i) = \alpha_i \in R$ and $d(c_i/d_i) = \gamma_i \in R$ for each i, so we get

$$bp = \sum_{i=0}^{m} \alpha_i x^i, \quad dq = \sum_{i=0}^{n} \gamma_i x^i$$

are both in $R[x]$. Let $\alpha = C(bp)$ and factor $bp = \alpha p_1$, where p_1 is primitive. Set $\gamma = C(dq)$ and factor $dq = \gamma q_1$ where q_1 is primitive. Combining all of this, we have $(bd)f = (\alpha\gamma)(p_1 q_1)$. By Lemma 2.6.1, it follows that bd and $\alpha\gamma$ are associates in R. Up to a unit in R, $f = p_1 q_1$. □

THEOREM 2.6.3. *Let R be a UFD. Then $R[x_1, \ldots, x_n]$ is a UFD.*

PROOF. By finite induction, it is enough to show $R[x]$ is a UFD.

(Existence.) Let $f \in R[x]$ be a nonunit nonzero. If f has degree zero, then we can view f as an element of R and factor f into irreducibles in R. This is a factorization into irreducibles in $R[x]$.

Assume $\deg f \geq 1$ and factor $f = C(f) f_1$ where f_1 is primitive and $C(f) \in R$. Since $C(f)$ can be factored into irreducibles, we can reduce to the case where f is primitive. Let K be the quotient field of R. We know that $K[x]$ is a UFD, by Corollary 2.5.5. In $K[x]$ we Theorem 2.6.2, for each i we can write

$$p_i = \frac{a_i}{b_i} q_i$$

where $a_i, b_i \in R$, and $q_i \in R[x]$ is primitive and irreducible. Multiplying,

$$f = \frac{\alpha}{\beta} q_1 q_2 \cdots q_n.$$

By Lemma 2.6.1 (3) we conclude that α and β are associates in R. Up to associates, we have factored $f = q_1 q_2 \cdots q_n$ into irreducibles in $R[x]$.

(Uniqueness.) Let f be a nonzero nonunit element of $R[x]$. Then f can be factored into a product of irreducibles $f = (c_1 \cdots c_m)(p_1 p_2 \cdots p_n)$ where each p_i is a primitive irreducible polynomial in $R[x]$ and each c_i is an irreducible element of R. Up to associates, $C(f) = c_1 c_2 \cdots c_m$ is uniquely determined by f. Since R is a UFD, the factorization $C(f) = c_1 c_2 \cdots c_m$ is unique in R. In $K[x]$ the factorization $p_1 p_2 \cdots p_n$ is uniquely determined up to associates. By Lemma 2.6.1 (3), the factorization is unique in $R[x]$. □

THEOREM 2.6.4. *Let R be a commutative ring and $f = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n$ a polynomial of degree $n \geq 1$ in $R[x]$. Let P be a prime ideal in R such that $a_n \notin P$ and $a_i \in P$ for $i = 0, 1, \ldots, n-1$. Suppose $f = gh$ is a factorization in $R[x]$ where* $\deg g = s \geq 1$, $\deg h = t \geq 1$, *and $s + t = n$. Then $a_0 \in P^2$.*

PROOF. Assume $a_n \notin P$, $(a_0, \ldots, a_{n-1}) \subseteq P$ and there is a factorization $f = gh$, where $\deg g = s \geq 1$, $\deg h = t \geq 1$, and $s + t = n$. By Theorem 2.5.2 (1) the natural map $\eta : R \to R/P$ induces $\bar{\eta} : R[x] \to R/P[x]$. Under this homomorphism, $\bar{\eta}(f) = \bar{\eta}(g)\bar{\eta}(h)$. By hypothesis, $\bar{\eta}(f) = \eta(a_n)x^n$ has degree n. If we write $g = b_0 + b_1 x + \cdots + b_s x^s$ and $h = c_0 + c_1 x + \cdots + c_t x^t$, then

$$\eta(a_n)x^n = (\eta(b_0) + \eta(b_1)x + \cdots + \eta(b_s)x^s)(\eta(c_0) + \eta(c_1)x + \cdots + \eta(c_t)x^t) \tag{2.1}$$

holds in $R/P[x]$. Since P is prime, R/P is an integral domain. Let K denote the quotient field of R/P. The factorization of $\bar{\eta}(f)$ in (2.1) holds in $K[x]$. By Corollary 2.5.5, $K[x]$ is a UFD. We conclude that $(b_0, b_1, \dots, b_{s-1}) \subseteq P$ and $(c_0, c_1, \dots, c_{t-1}) \subseteq P$. The constant term of f is equal to $a_0 = b_0 c_0 \in P^2$. □

COROLLARY 2.6.5. *Let R be an integral domain and $f = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ a monic polynomial of degree $n \geq 1$ in $R[x]$. Let P be a prime ideal in R such that $a_i \in P$ for $i = 0, 1, \dots, n-1$, and $a_0 \notin P^2$. Then f is irreducible in $R[x]$.*

COROLLARY 2.6.6. *(Eisenstein's Irreducibility Criterion) Let R be UFD and $f = a_0 + a_1 x + \cdots + a_n x^n$ a primitive polynomial of degree $n \geq 1$ in $R[x]$. Let p be a prime in R such that $p \nmid a_n$, $p \mid a_i$ for $i = 0, 1, \dots, a_{n-1}$, and $p^2 \nmid a_0$. Then f is irreducible.*

6.1. Exercises.

EXERCISE 2.6.1. Let k be a field and $K = k(x)$ the field of rational functions over k in the variable x. Let y be an indeterminate. Show that for any $d \geq 1$, the polynomial $y^d - x$ is irreducible in $K[y]$.

CHAPTER 3

Linear Algebra

1. Modules and Algebras

1.1. Definitions and Fundamental Results.

DEFINITION 3.1.1. If R is a ring, an *R-module* is a nonempty set M with an addition operation making M an abelian group 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.

EXAMPLE 3.1.2. Standard examples of modules are listed here.

(1) Let M be any additive abelian group. Then $\mathbb{Z}$ acts on M. If $x \in M$ and $n \in \mathbb{Z}$, then
$$nx = \begin{cases} 0 & \text{if } n = 0 \\ \sum_{i=1}^{n} x = x+x+\cdots+x & \text{if } n > 0 \\ -\sum_{i=1}^{|n|} x = -(x+x+\cdots+x) & \text{if } n < 0 \end{cases}$$
This action makes M into a $\mathbb{Z}$-module.

(2) If R is any ring, and I is a left ideal in R, then R acts on I from the left. If $x \in I$ and $r \in R$, then $rx \in I$. The associative and distributive laws in R apply. Thus I is an R-module.

(3) Let $\phi : R \to S$ be a homomorphism of rings. Then R acts on S by the multiplication rule $rx = \phi(r)x$, for $r \in R$ and $x \in S$. By this action, S is an R-module.

DEFINITION 3.1.3. Let R be a ring and M an R-module. 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
$$\left\{ \sum_{i=1}^{n} r_i x_i \mid n \geq 1, r_i \in R, x_i \in X \right\}.$$
The reader should verify that the submodule generated by X is equal to 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 $X = \{x_1, x_2, \ldots, x_n\}$ is finite, we sometimes write $(X) = Rx_1 + Rx_2 + \cdots + Rx_n$.

DEFINITION 3.1.4. If I is a left ideal of R and M is an R-module, then IM denotes the R-submodule of M generated by the set $\{rx \mid r \in I, x \in M\}$.

DEFINITION 3.1.5. Let R be a ring and M an R-module. We say that M is *finitely generated* if there exists a finite subset $\{x_1, \ldots, x_n\} \subseteq M$ such that $M = Rx_1 + \cdots + Rx_n$.

DEFINITION 3.1.6. If M and N are R-modules, a *homomorphism* from M to N is a function $f : M \to N$ satisfying

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

for all $x \in M$ and $r \in R$. The *kernel* of the homomorphism f is $\ker(f) = \{x \in M \mid f(x) = 0\}$. The reader should verify that the kernel of f is a submodule of M and that f is one-to-one if and only if $\ker f = (0)$. The *image* of the homomorphism f is $\operatorname{im}(f) = \{f(x) \in N \mid x \in M\}$. The reader should verify that the image of f is a submodule of N. 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 set $\operatorname{Hom}_R(M,M)$ is a ring (see Example 3.3.1) which is called the *endomorphism ring* of M.

DEFINITION 3.1.7. Let R be a ring, M an R-module and S a submodule. The *factor* module of M modulo S is the set $M/S = \{a+S \mid a \in M\}$ of all left cosets of S in M. We sometimes call M/S the quotient module of M modulo S. We define addition and scalar multiplication of cosets by the rules

$$(a+S) + (b+S) = (a+b) + S$$
$$r(a+S) = ra + S.$$

The reader should verify that M/S is an R-module. Let $\eta : M \to M/S$ be the natural map defined by $x \mapsto x + S$. Then η is a homomorphism, $\operatorname{im}\eta = M/S$, and $\ker\eta = S$.

DEFINITION 3.1.8. The *cokernel* of a homomorphism $f : M \to N$ is defined to be

$$\operatorname{coker}(f) = N/\operatorname{im}(f)$$

which is a homomorphic image of N under the natural map.

PROPOSITION 3.1.9. *Let $\theta : M \to N$ be a homomorphism of R-modules. Let S be a submodule of M contained in $\ker\theta$. There exists a homomorphism $\varphi : M/S \to N$ satisfying the following.*

(a) $\varphi(a+S) = \theta(a)$*, or in other words* $\theta = \varphi\eta$.
(b) φ *is the unique homomorphism from* $M/S \to N$ *such that* $\theta = \varphi\eta$.
(c) $\operatorname{im}\theta = \operatorname{im}\varphi$.
(d) $\ker\varphi = \eta(\ker\theta) = \ker(\theta)/S$.
(e) φ *is one-to-one if and only if* $S = \ker\theta$.
(f) φ *is onto if and only if* θ *is onto.*
(g) There is a unique homomorphism $\phi : M/S \to M/\ker\theta$ *such that the diagram*

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

commutes.

PROOF. Is left to the reader. □

PROPOSITION 3.1.10. *Let M be an R-module with submodules A and B.*

(a) The natural map

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

sending the coset $x + A \cap B$ to the coset $x + B$ is an isomorphism.

(b) If $A \subseteq B$, then B/A is a submodule of M/A and the natural map

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

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

PROOF. Is left to the reader. □

PROPOSITION 3.1.11. *Let M be an R-module and A a submodule of M. 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 $B \mapsto B/A$.*

DEFINITION 3.1.12. Let R be a ring and M an R-module. The *annihilator* of M in R is

$$\operatorname{annih}_R M = \{r \in R \mid rm = 0 \text{ for all } m \in M\}.$$

The reader should verify that $\operatorname{annih}_R M$ is a two-sided ideal in R. If $\operatorname{annih}_R M = (0)$, then we say M is *faithful*.

DEFINITION 3.1.13. Let R be a commutative ring. 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. Then A is an R-module with action $ra = \theta(r)a$. For all $r \in R$, $a, b \in A$, it follows that $\theta(r)(ab) = (\theta(r)a)b = (a\theta(r))b = a(\theta(r)b)$. Therefore

$$r(ab) = (ra)b = a(rb). \tag{3.1}$$

We call θ the *structure homomorphism* of A. Conversely, if A is a ring and R is a commutative ring and A is an R-module satisfying (3.1), then $\theta : R \to Z(A)$ given by $\theta(r) = r1$ is a homomorphism of rings, so A is an R-algebra. 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.

DEFINITION 3.1.14. 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 $\operatorname{Aut}_R(A)$.

EXAMPLE 3.1.15. Let R be any ring and $\chi : \mathbb{Z} \to R$ the unique homomorphism of Example 2.1.13. The reader should verify that the image of χ is in the center of R, hence R is a $\mathbb{Z}$-algebra.

1.2. Exercises.

EXERCISE 3.1.1. 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 3.1.2. (Module version of Finitely Generated over Finitely Generated is Finitely Generated) Let $R \to S$ be a homomorphism of rings such that S is finitely generated as an R-module. If M is a finitely generated S-module, prove that M is finitely generated as an R-module.

EXERCISE 3.1.3. 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 3.1.4. 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 3.1.5. 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 3.1.6. 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 3.1.7. Let R be a commutative ring and A an R-algebra. Let G be a finite group and $R(G)$ the group ring.

(1) If $h : G \to A^*$ is a homomorphism from G to the group of units of A, show that there is a homomorphism of R-algebras $R(G) \to A$ which maps $rg \mapsto rh(g)$ for $r \in R$ and $g \in G$.
(2) There is an isomorphism of R-algebras $R(G) \cong R(G)^o$ which maps $g \in R(G)$ to $g^{-1} \in R(G)^o$.

1.3. Direct Sums of Modules.

DEFINITION 3.1.16. Let R be a ring and $\{M_i \mid i \in I\}$ a family of R-modules. The *direct product* is

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

The product of R-modules is an R-module, if addition and multiplication are defined coordinate-wise

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

For each $k \in I$ there is the canonical injection map

$$\iota_k : M_k \to \prod_{i\in I} M_i$$

which maps $x \in M_k$ to $\iota_k(x)$ which is equal to x in coordinate k, and 0 elsewhere. The reader should verify that ι_k is a one-to-one homomorphism of R-modules. The canonical projection map

$$\pi_k : \prod_{i\in I} M_i \to M_k$$

is defined by the rule $\pi_k(f) = f(k)$ as in Exercise 1.5.9. The reader should verify that π_k is an onto homomorphism of R-modules. We have $\pi_k\iota_k = 1_{M_k}$.

DEFINITION 3.1.17. Let R be a ring and $\{M_i \mid i \in I\}$ a family of R-modules. The *direct sum* is

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

which is a submodule of the product. For each $k \in I$ the image of the injection map ι_k of Definition 3.1.16 is contained in the direct sum $\bigoplus_{i\in I} M_i$ and is a one-to-one homomorphism of R-modules. The reader should verify that 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 $\pi_k\iota_k = 1_{M_k}$.

DEFINITION 3.1.18. If the index set is finite, the product and the direct sum are equal. If $I = \{1,2,\dots,n\}$ then $\bigoplus_{i=1}^n M_i$ is the usual (external) direct sum $M_1 \oplus M_2 \oplus \cdots \oplus M_n = \{(x_1,\dots,x_n) \mid x_i \in M_i\}$.

DEFINITION 3.1.19. Let $\{S_1,\dots,S_n\}$ be a set of submodules in the R-module M. The submodule of M generated by the set $S_1 \cup S_2 \cup \cdots \cup S_n$ is called the *sum* of the submodules and is denoted $S_1 + S_2 + \cdots + S_n$. We say that M is the *internal direct sum* of the submodules in case

(1) $M = S_1 + S_2 + \cdots + S_n$, and
(2) for each $x \in M$, x has a unique representation as a sum $x = x_1 + x_2 + \cdots + x_n$ where $x_i \in S_i$.

We denote the internal direct sum by $M = S_1 \oplus S_2 \oplus \cdots \oplus S_n$. 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 3.1.20. *If $S_1,\dots,S_n$ are submodules in the R-module M, and $M = S_1 \oplus \cdots \oplus S_n$, then the following are true.*

(1) For each k, $S_k \bigcap \left(\sum_{j\neq k} S_j\right) = (0)$.
(2) M is isomorphic to the (external) direct sum $S_1 \oplus \cdots \oplus S_n$.

PROOF. Left to the reader. □

PROPOSITION 3.1.21. *Suppose $S_1, \dots, S_n$ are submodules in the R-module M satisfying*

(1) $M = S_1 + S_2 + \cdots + S_n$ and
(2) for each k, $S_k \cap \left(\sum_{j \neq k} S_j\right) = (0)$.

Then $M = S_1 \oplus S_2 \oplus \cdots \oplus S_n$.

PROOF. Left to the reader. □

1.4. Free Modules.

DEFINITION 3.1.22. Let R be a ring and I any index set. For $i \in I$, let $R_i = R$ as R-modules. 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 $\phi_X(r_1, \dots, r_n) = r_1 x_1 + \dots r_n x_n$. 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

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \tag{3.2}$$

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 3.1.23. *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 set $I' \subseteq I$. Because X generates M and is linearly independent, this ϕ is one-to-one and onto. The converse is left to the reader. □

LEMMA 3.1.24. *Let R be a ring and M an R-module.*

(1) (Universal Mapping Property) 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

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

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.

PROOF. Part (1) is left to the reader.

(2) and (3): Let X be a generating set for M and F the free R-module on X. Map the basis elements of R^X to the generators for M. If M is finitely generated, X can be taken to be finite. □

DEFINITION 3.1.25. 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

$$M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \xrightarrow{\phi_3} \cdots. \tag{3.3}$$

Then (3.3) 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 (3.3) 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

$$0 \to M_2 \xrightarrow{\phi_2} M_3 \xrightarrow{\phi_3} M_4 \to 0 \tag{3.4}$$

where $M_1 = 0 = M_5$ and $\phi_1 = 0 = \phi_4$. The short exact sequence (3.4) 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 3.1.10, (3.4) 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 3.1.26. 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.

DEFINITION 3.1.27. 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.

1.5. Exercises.

EXERCISE 3.1.8. 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 3.1.9. 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 3.1.10. 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 3.1.11. 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 3.1.12. 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 $\text{GCD}(m,n) = 1$.

EXERCISE 3.1.13. 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 3.1.14. 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 3.1.15. Let R be a commutative ring and F a free R-module with basis $\{b_i\}_{i \in I}$. Prove that if J is a proper ideal of R and $\pi : F \to F/JF$ is the natural homomorphism, then F/JF is a free R/J-module with basis $\{\pi(b_i)\}_{i \in I}$.

EXERCISE 3.1.16. Let R be any ring. Show that the ring of polynomials $R[x]$ is a free R-module and the set $\{1, x, x^2, \dots, x^i, \dots\}$ is a free basis.

EXERCISE 3.1.17. Let R be a commutative ring and $f \in R[x]$ a monic polynomial of degree n. Show that $S = R[x]/(f)$ is a free R-module of rank n and the set $\{1, x, x^2, \dots, x^{n-1}\}$ is a free basis.

EXERCISE 3.1.18. Let R be a ring, and M an R-module with submodules S and T. If ϕ is the subtraction mapping $(x,y) \mapsto (x-y) + (S+T)$, and ψ is the diagonal $z \mapsto (z+S, z+T)$, then

$$0 \to S \cap T \to M \xrightarrow{\psi} M/S \oplus M/T \xrightarrow{\phi} M/(S+T) \to 0$$

is an exact sequence of R-modules.

EXERCISE 3.1.19. 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.

EXERCISE 3.1.20. Let R be a ring and M a free R-module. Prove that M is faithful.

EXERCISE 3.1.21. Let R be a ring. Let x be an element of R that is not a right zero divisor in R. Prove that Rx, the left ideal generated by x, is a free R-module.

EXERCISE 3.1.22. 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 rings induced by the set inclusion man $H \to G$ (see Example 2.1.13 (3)). Show that $R(G)$ is a free $R(H)$-module.

1.6. Vector Spaces. 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*.

THEOREM 3.1.28. *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 $X \subseteq Y$. The union of any chain in S is also in S. By Zorn's Lemma, Proposition 1.3.3, S contains a maximal member, say B. Assume $v \in V$ and v is not in the span of B. Assume there is a dependence relation

$$\sum_i \beta_i b_i + \alpha v = 0$$

where $\alpha, \beta_i \in D$ and $b_i \in B$. If $\alpha = 0$, then each $\beta_i = 0$. Otherwise, we can solve

$$v = -\alpha^{-1} \sum_i \beta_i b_i.$$

This contradicts the choice of v, hence $B \cup \{v\}$ is a linearly independent set which contradicts the choice of B as a maximal element of S. This proves that the span of B is equal to 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. The union of any chain in S is also in S. By Zorn's Lemma, Proposition 1.3.3, S contains a maximal member, say B. By the previous argument, we show that every $v \in X$ is in the span of B. Therefore B is a basis for V. □

THEOREM 3.1.29. *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.

PROOF. Step 1: Write $y_1 = \alpha_1 b_1 + \cdots + \alpha_n b_n$ where each $\alpha_i \in D$. For some i, $\alpha_i \neq 0$. Re-order the basis elements and assume $\alpha_1 \neq 0$. Solve for b_1 to get $b_1 = \alpha_1^{-1} y_1 -$

$\sum_{i=2}^{n}\alpha_1^{-1}\alpha_i b_i$. Therefore $B \subseteq Dy_1 + Db_2 + \cdots + Db_n$, hence $\{y_1, b_2, \ldots, b_n\}$ is a spanning set for V. Suppose $0 = \beta_1 y_1 + \beta_2 b_2 + \cdots + \beta_n b_n$. Then

$$\begin{aligned} 0 &= \beta_1(\alpha_1 b_1 + \cdots + \alpha_n b_n) + \beta_2 b_2 + \cdots + \beta_n b_n \\ &= \beta_1\alpha_1 b_1 + (\beta_1\alpha_2 + \beta_2)b_2 + \cdots + (\beta_1\alpha_n + \beta_n)b_n, \end{aligned}$$

from which it follows that $\beta_1\alpha_1 = 0$, hence $\beta_1 = 0$. Now $0 = \beta_2 b_2 + \cdots + \beta_n b_n$ implies $0 = \beta_2 = \cdots = \beta_n$. We have shown that $\{y_1, b_2, \ldots, b_n\}$ is a basis for V.

Step j: Inductively, assume $j \geq 2$ and that $\{y_1, y_2, \ldots, y_{j-1}, b_j, \ldots, b_n\}$ is a basis for V. Write $y_j = \alpha_1 y_1 + \cdots + \alpha_{j-1}y_{j-1} + \alpha_j b_j + \cdots + \alpha_n b_n$ where each $\alpha_i \in D$. Since the set $\{y_1, \ldots, y_j\}$ is linearly independent, for some $i \geq j$, $\alpha_i \neq 0$. Re-order the basis elements and assume $\alpha_j \neq 0$. Solve for b_j and by a procedure similar to that used in Step 1, we see that $\{y_1, \ldots, y_j, b_{j+1}, \ldots, b_n\}$ is a basis for V.

By finite induction, Part (1) is proved. For Part (2), assume $\{c_1, \ldots, c_m\}$ is another basis for V. By applying Part (1) from both directions, it follows that $m \leq n$ and $n \leq m$. □

DEFINITION 3.1.30. Suppose D is a division ring and V is 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 $\dim_D(V) = \infty$.

DEFINITION 3.1.31. Let R be a commutative ring and M a free R-module with a finite basis $\{b_1, \ldots, b_n\}$. By Exercise 3.1.23, any other basis of M has n elements. We call n the *rank* of M and write $\operatorname{Rank}_R M = n$.

DEFINITION 3.1.32. 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 $m \in M$, $m = \sum_{i \in I} f_i(m)m_i$.

PROPOSITION 3.1.33. *(Free over Free is Free) Let $\theta : R \to S$ be a homomorphism of rings such that S is free as an R-module. Let M be a free S-module.*

(1) Then M is a free R module.
(2) 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 $\operatorname{Rank}_R(M) = \operatorname{Rank}_S(M)\operatorname{Rank}_R(S)$.
(3) 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. 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 3.1.17 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. Consider the set $\{(s_j m_i, g_j f_i) \mid (i, j) \in I \times J\}$. 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 $x \in M$, $g_j f_i(x) = 0$ for all but finitely many choices of (i,j). For each $x \in M$ we have

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

This shows $\{(s_j m_i, g_j f_i)\}$ is a dual basis for M over R. To show that $\{s_j m_i\}$ is a free basis, assume there is a finite dependence relation

$$0 = \sum_{(i,j)\in I\times J} \alpha_{i,j} s_j m_i = \sum_{i\in I}\left(\sum_{j\in J}\alpha_{i,j}s_j\right)m_i.$$

Because $\{m_i \mid i \in I\}$ is a free basis, for each i we have $\sum_j \alpha_{i,j}s_j = 0$. Because $\{s_j \mid j \in J\}$ is a free basis, each $\alpha_{i,j}$ is zero. The rest of the proof is left to the reader. □

1.7. Exercises.

EXERCISE 3.1.23. 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 3.1.24. Suppose D is a division ring, V is a finite dimensional vector space over D, and W is a subspace of V. Prove:

(1) W is finite dimensional and $\dim_D(W) \le \dim_D(V)$.
(2) There is a subspace U of V such that $V = U \oplus W$ is an internal direct sum.

EXERCISE 3.1.25. Suppose $\phi \in \operatorname{Hom}_D(V,W)$, where V and W are vector spaces over the division ring D. Prove:

(1) If V is finite dimensional, then the kernel of ϕ is finite dimensional and the image of ϕ is finite dimensional.
(2) If the kernel of ϕ is finite dimensional and the image of ϕ is finite dimensional, then V is finite dimensional.

EXERCISE 3.1.26. (The Rank-Nullity Theorem) Suppose $\phi \in \operatorname{Hom}_D(V,W)$, where V and W are vector spaces over the division ring D. The *rank* of ϕ, written $\operatorname{Rank}(\phi)$, is defined to be the dimension of the image of ϕ. The *nullity* of ϕ, written $\operatorname{Nullity}(\phi)$, is defined to be the dimension of the kernel of ϕ. Prove that if V is finite dimensional, then $\dim_D(V) = \operatorname{Rank}(\phi) + \operatorname{Nullity}(\phi)$.

EXERCISE 3.1.27. Suppose $\phi \in \operatorname{Hom}_D(V,V)$, where V is a finite dimensional vector space over the division ring D. Prove that the following are equivalent:

(1) ϕ is invertible.
(2) $\operatorname{Nullity}(\phi) = 0$.
(3) $\operatorname{Rank}(\phi) = \dim_D(V)$.

EXERCISE 3.1.28. Let R be a UFD with quotient field K. Let a be an element of R which is not a square in R and let $f = x^2 - a \in R[x]$.

(1) Show that $S = R[x]/(f)$ is an integral domain and $L = K[x]/(f)$ is a field.
(2) Show that S is a free R-module, $\operatorname{Rank}_R(S) = 2$, and $\dim_K(L) = 2$.

EXERCISE 3.1.29. Let V be a finite dimensional vector space over a division ring D. Let ϕ, ψ be elements of $\operatorname{Hom}_D(V,W)$. Prove:

(1) $\operatorname{Rank}(\phi\psi) \le \operatorname{Rank}(\phi)$.
(2) $\operatorname{Rank}(\phi\psi) \le \operatorname{Rank}(\psi)$.
(3) $\operatorname{Rank}(\phi\psi) \le \min(\operatorname{Rank}(\phi), \operatorname{Rank}(\psi))$.
(4) If ϕ is invertible, $\operatorname{Rank}(\phi\psi) = \operatorname{Rank}(\psi\phi) = \operatorname{Rank}(\psi)$.

EXERCISE 3.1.30. Let D be a division ring and V and W finitely generated vector spaces over D. Suppose U is a subspace of V and $\phi : U \to W$ an element of $\operatorname{Hom}_D(U,W)$. Show that there exists an element $\bar{\phi}$ of $\operatorname{Hom}_D(V,W)$ such that the diagram

$$\begin{tikzcd}
U \arrow[rr, "\phi"] \arrow[dr, "\subseteq"'] & & W \\
& V \arrow[ur, dotted, "\bar{\phi}"'] &
\end{tikzcd}$$

commutes. That is, $\bar{\phi}$ is an extension of ϕ.

EXERCISE 3.1.31. 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 subrings $R \subseteq S \subseteq T$, prove:

(1) T is free over R of rank n.
(2) S is free over R of rank n.
(3) T is not free over S.

2. Finitely Generated Modules over a Principal Ideal Domain

Throughout this section, R is a principal ideal domain, or PID for short. A commutative ring R is called a *semilocal ring* if R has only a finite number of maximal ideals. A local ring has only one maximal ideal, hence is a semilocal ring.

PROPOSITION 3.2.1. *Let R be a PID.*

(1) Every nonzero ideal of R is a free R-module of rank 1.
(2) Let π be an irreducible element of R, $e > 0$ and $A = R/(\pi^e)$. The following are true.
  (a) A is a principal ideal ring which is a field if and only if $e = 1$.
  (b) A is a local ring, the unique maximal ideal is generated by π.
  (c) A has exactly $e+1$ ideals, namely

$$(0) \subseteq (\pi^{e-1}) \subseteq \cdots \subseteq (\pi^2) \subseteq (\pi) \subseteq A$$

(3) Let $\pi_1, \dots, \pi_n$ be irreducible elements of R that are pairwise nonassociates. Let $e_1, \dots, e_n$ be positive integers. If $x = \pi_1^{e_1}\pi_2^{e_2}\cdots\pi_n^{e_n}$, then the following are true.
  (a) $A = R/(x)$ is a semilocal ring with exactly n maximal ideals.
  (b) $A = R/(x)$ is isomorphic to the direct sum of the local rings $\bigoplus_i R/(\pi_i^{e_i})$.

PROOF. Is left to the reader. □

Let F be a free module over R with a finite basis. By Exercise 3.1.23, every basis of F over R has the same number of elements, namely $\operatorname{Rank}_R(F)$.

THEOREM 3.2.2. *Let R be a PID and let F be a free R-module with a finite basis. If M is a submodule of F, then M is a free R-module and* $\operatorname{Rank}_R(M) \le \operatorname{Rank}_R(F)$.

PROOF. Let $\{x_1, \dots, x_n\}$ be a basis for F over R. Let Rx_1 be the submodule of F spanned by x_1. The assignment $1 \mapsto x_1$ defines an isomorphism of R-modules $\theta : R \to Rx_1$. If $M_1 = M \cap Rx_1$, then M_1 is an R-submodule of the free R-module Rx_1. Then M_1 is equal to the image under θ of an ideal $I = Ra$ for some $a \in R$. In other words, $M_1 = Rax_1$. If

$a = 0$, then $M_1 = 0$. Otherwise, there is an isomorphism $R \cong M_1$ given by the assignment $1 \mapsto ax_1$. For each j in the range $1 \leq j \leq n$ define $M_j = M \cap (Rx_1 + \cdots + Rx_j)$. The proof is by induction on n. If $n = 1$, we are done. Assume $j \geq 1$ and that M_j is a free R-module on j or fewer generators. We now prove that $M_{j+1} = M \cap \left(Rx_1 + \cdots + Rx_{j+1}\right)$ is free of rank $j+1$ or less. Let $\psi : Rx_1 + \cdots + Rx_{j+1} \to Rx_{j+1}$ be the projection onto the last summand. The image of M_{j+1} under ψ is a submodule of the free R-module Rx_{j+1}. Therefore, $\psi\left(M_{j+1}\right) = Rax_{j+1}$ for some $a \in R$. If $a \neq 0$, then Rax_{j+1} is free of rank 1. The exact sequence

$$M_{j+1} \xrightarrow{\psi} Rax_{j+1} \to 0$$

splits and the kernel is $M_{j+1} \cap (Rx_1 + \cdots + Rx_j) = M_j$. □

COROLLARY 3.2.3. *Let R be a PID and M a finitely generated R-module. Then*

(1) M is of finite presentation, and
(2) every submodule of M is finitely generated.

PROOF. By Lemma 3.1.24, there is is a surjection $\psi : R^{(n)} \to M$. By Theorem 3.2.2, the kernel of ψ is free of rank $m \leq n$, so there is an exact sequence

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

which shows M is of finite presentation. If N is a submodule of M, then $\psi^{-1}(N)$ is a submodule of $R^{(n)}$, which is free of rank n or less. This shows N is the homomorphic image of a finitely generated R-module. □

DEFINITION 3.2.4. 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 the annihilator of x in R is nonzero. So x is torsion if 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, denoted M_t. If $M_t = 0$, then we say M is *torsion free*.

PROPOSITION 3.2.5. *Let R be a PID and M a finitely generated R-module. The following are equivalent.*

(1) M is torsion free.
(2) M is free.

PROOF. (2) implies (1): Is left to the reader.

(1) implies (2): Assume $M = Ry_1 + \cdots + Ry_n$. Let $\{v_1, \ldots, v_m\}$ be a linearly independent subset of $\{y_1, \ldots, y_n\}$ such that m is maximal. If $N = Rv_1 + \cdots + Rv_m$, then N is a free R-module. By the choice of $\{v_1, \ldots, v_m\}$, for each $j = 1, \ldots, n$, there is a nontrivial dependence relation

$$c_j y_j = \sum_{i=1}^{m} a_{ij} v_i$$

such that $c_j, a_{1j}, \ldots, a_{mj}$ are in R and $c_j \neq 0$. Since R is a domain, if $c = c_1 c_2 \cdots c_n$, then $c \neq 0$. For each j, c factors into $c = c_j d_j$. Consider the submodule $cM = \{cx \mid x \in M\}$ of

M. A typical element of $cM = c(Ry_1 + \cdots + Ry_n)$ looks like

$$\begin{aligned} cx &= c\sum_{j=1}^{n} r_j y_j \\ &= \sum_{j=1}^{n} r_j c y_j \\ &= \sum_{j=1}^{n} r_j d_j c_j y_j \\ &= \sum_{j=1}^{n} \left(r_j d_j \sum_{i=1}^{m} a_{ij} y_j \right) \end{aligned}$$

which is in N. Since N is free of rank m, Theorem 3.2.2 says that cM is free of rank no more than m. Because c is nonzero and M is torsion free, the assignment $x \mapsto cx$ defines an isomorphism $M \to cM$. □

In Example 5.2.6 we prove that a finitely generated projective module over a principal ideal domain is free.

COROLLARY 3.2.6. *Let R be a PID and M a finitely generated R-module. Let M_t denote the submodule consisting of all torsion elements of M. 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.*

PROOF. The reader should verify that M/M_t is torsion free. Therefore, the sequence

$$0 \to M_t \to M \to M/M_t \to 0$$

is split-exact. The rank of F is equal to the rank of M/M_t, which is uniquely determined by M. □

Let M be an R-module and $x \in M$. The *cyclic submodule generated by x* is Rx. Denote by I_x the annihilator of Rx in R. That is,

$$I_x = \operatorname{annih}_R(x) = \{r \in R \mid rx = 0\}$$

which is an ideal in R, hence is principal. So $I_x = Ra$ and up to associates in R, a is uniquely determined by x. We call a the *order of x*. The sequence of R-modules

$$0 \to I_x \to R \to Rx \to 0$$

is exact, so $Rx \cong R/(I_x) \cong R/Ra$.

The left regular representation of R in $\operatorname{Hom}_R(M,M)$ maps $r \in R$ to $\ell_r : M \to M$, where ℓ_r is "left multiplication by r" (see Example 3.3.2). 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

$$\begin{aligned} M(\pi) &= \bigcup_{n>0} \ker(\ell_{\pi^n}) \\ &= \{x \in M \mid \exists n > 0 : \pi^n x = 0\} \end{aligned}$$

is a submodule of M.

LEMMA 3.2.7. *Assume R is a PID, π is a prime in R, and M is an R-module.*

(1) If $(\pi, q) = 1$, then $\ell_q : M(\pi) \to M(\pi)$ is one-to-one.

(2) If $M \cong R/(\pi^e R)$ is a cyclic R-module of order π^e, where $e \geq 1$, then

(a) πM is cyclic of order π^{e-1}, and

(b) $M/\pi M$ is a vector space of dimension one over the field $R/\pi R$.

PROOF. (1): Suppose $x \in \ker(\ell_q)$ and $\pi^n x = 0$. Then $(\pi^n, q) = 1$, so there exist $a, b \in R$ such that $1 = qa + \pi^n b$. Therefore, $x = aqx + b\pi^n x = 0$.

(2): Is left to the reader. □

THEOREM 3.2.8. *Let R be a PID and M a torsion R-module. Then M is the internal direct sum of the submodules $M(\pi)$*

$$M = \bigoplus_{\pi} M(\pi)$$

where the sum is over all primes π in R. If M is finitely generated, then there exists a finite set $\pi_1, \dots, \pi_n$ of primes in R such that $M = M(\pi_1) \oplus \cdots \oplus M(\pi_n)$.

PROOF. Let $x \in M$ and let a be the order of x. Since M is torsion, $a \neq 0$. Since R is a UFD, we factor a into primes, $a = \pi_1^{e_1} \cdots \pi_n^{e_n}$ where each $e_i > 0$. For each π_i, let $q_i = a/\pi_i^{e_i}$. Then $Rq_1 + \cdots + Rq_n = 1$. There exist $s_1, \dots s_n \in R$ such that $1 = s_1 q_1 + \cdots + s_n q_n$. This means $x = s_1 q_1 x + \cdots + s_n q_n x$. Note that $\pi_i^{e_i} q_i x = ax = 0$ so $q_i x \in M(\pi_i)$. This proves $x \in M(\pi_1) + \cdots + M(\pi_n)$ and that M is spanned by the submodules $M(\pi_i)$. If M is finitely generated, then clearly only a finite number of primes are necessary in the sum.

To show that the sum is direct, assume π is a prime in R and

$$x \in M(\pi) \bigcap \Big(\sum_{q \neq \pi} M(q) \Big)$$

where the second summation is over all primes different from π. In the sum, only finitely many summands are nonzero. Assume $q_1, \dots, q_n$ are primes different from π and that x is in $M(\pi) \cap (M(q_1) + \cdots + M(q_n))$. Because x is in the sum $M(q_1) + \cdots + M(q_n)$, for some large integer m, if $s = (q_1 \cdots q_n)^m$, then $sx = 0$. But $(s, \pi) = 1$ and Lemma 3.2.7 says $\ell_s : M(\pi) \to M(\pi)$ is one-to-one. This implies $x = 0$. □

LEMMA 3.2.9. *Let R be a PID and M a torsion R-module such that the annihilator of M in R is $R\pi^n$, where π is a prime and $n > 0$. Then there exists an element $a \in M$ of order π^n such that the cyclic submodule Ra is a direct summand of M.*

PROOF. There exists $a \in M$ such that $\pi^n a = 0$ and $\pi^{n-1} a \neq 0$. If $Ra = M$, then we are done. Otherwise continue.

Step 1: There exists $b \in M$ such that $\pi b = 0$, $b \neq 0$ and $Ra \cap Rb = 0$. Start with any element c in $M - Ra$. Pick the least positive integer j such that $\pi^j c \in Ra$. Then $1 \leq j \leq n$. Let $\pi^j c = r_1 a$. Since R is factorial, write $r_1 = r\pi^k$ and assume $(r, \pi) = 1$. Now $0 = \pi^n c = \pi^{n-j} \pi^j c = r\pi^{n-j} \pi^k a$. By Lemma 3.2.7, $\pi^{n-j+k} a = 0$. Since the order of a is π^n, this implies $0 \leq -j + k$, so we have $1 \leq j \leq k$. Set $b = \pi^{j-1} c - r\pi^{k-1} a$. Since $\pi^{j-1} c \notin Ra$ but $r\pi^{k-1} a \in Ra$ we know $b \neq 0$. Also, $\pi b = \pi^j c - r\pi^k a = 0$. Now check that $Ra \cap Rb = 0$. Assume otherwise. Then for some $s \in R$ we have $sb \in Ra$ and $sb \neq 0$. Since the order of b is π, this implies $(s, \pi^n) = 1$. For some $x, y \in R$ we can write $xs + y\pi^n = 1$. In this case $b = xsb + y\pi^n b = xsb \in Ra$ which is a contradiction.

Step 2: Ra is a direct summand of M. Let $\mathscr{S}$ be the set of all submodules S of M such that $S \cap Ra = 0$. By Step 1, $\mathscr{S}$ is nonempty. Order $\mathscr{S}$ by set inclusion. Zorn's Lemma, Proposition 1.3.3, says there is a maximal member, C. To complete the proof, it suffices to show $C + Ra = M$, which is equivalent to showing M/C is generated by $a + C$. For contradiction's sake, assume $M \neq C + Ra$. Since $C \cap Ra = 0$, the order of $a + C$ in M/C is π^n. By Step 1, there exists $b + C \in M/C$ such that $b + C \neq C$, $\pi b + C = C$, and $(Ra + C) \cap (Rb + C) = C$. It suffices to show that $Rb + C$ is in $\mathscr{S}$. Suppose $x \in$

$(Rb+C)\cap Ra$. We can write x in two ways, $x = rb+c \in Rb+C$, and $x = sa \in Ra$. Hence $rb \equiv sa \pmod{C}$. The choice of b implies $\pi \mid r$. Then $x = (r/\pi)\pi b + c$ is an element of C. So $x \in C \cap Ra = 0$, which says $x = 0$. This says $Rb+C$ is in $\mathscr{S}$, which contradicts the choice of C. □

2.1. Exercises.

EXERCISE 3.2.1. 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 $i = 1, \dots, e$, 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 $i = 1, \dots, e-1$, 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 2.1.19 to prove that

$$1 \to U_i \to (R/(\pi^e))^* \to \left(R/(\pi^i)\right)^* \to 1$$

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 5.7.2) to the commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & U_i \arrow[r] \arrow[d] & (R/(\pi^e))^* \arrow[r] \arrow[d] & \left(R/(\pi^i)\right)^* \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & U_{i-1} \arrow[r] & (R/(\pi^e))^* \arrow[r] & \left(R/(\pi^{i-1})\right)^* \arrow[r] & 1
\end{tikzcd}$$

EXERCISE 3.2.2. Let k be a field and $n \geq 1$. Show that there is a series of subgroups

$$\operatorname{Units}(k[x]/(x^n)) = U_0 \supseteq U_1 \supseteq \cdots \supseteq U_{n-1} \supseteq U_n = (1),$$

where $U_0/U_1 = \operatorname{Units}(k)$, and for each $i = 1, \dots, n-1$, the factor group U_i/U_{i+1} is isomorphic to the additive group of k.

2.2. The Basis Theorems.

THEOREM 3.2.10. *(Basis Theorem – Elementary Divisor Form) Let R be a PID and M a finitely generated R-module. In the notation established above, the following are true.*

(1) $M = F \oplus M_t$, where F is a free submodule of finite rank. The rank of F is uniquely determined by M.

(2) $M_t = \bigoplus_\pi M(\pi)$ where π runs through a finite set of primes in R.

(3) *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 $e_1 \geq e_2 \geq \cdots \geq e_m$.*

(4) *M_t 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.*

PROOF. (1): is Corollary 3.2.6.

(2): is Theorem 3.2.8.

(3): Since $M(\pi)$ is a direct summand of M, it follows from Corollary 3.2.3 that $M(\pi)$ is finitely generated. Let $x_1, \dots, x_n$ be a generating set. Let k be the maximum integer in the set $\{k_i \mid x_i \text{ has order } \pi^{k_i}\}$. Then $\pi^k M(\pi) = 0$. There exists $e_1 > 0$ such that $\pi^{e_1} M(\pi) = 0$ and $\pi^{e_1 - 1} M(\pi) \neq 0$. By Lemma 3.2.9, there exists $a_1 \in M(\pi)$ such that a_1 has order π^{e_1} and $M = Ra_1 \oplus C_1$. If $C_1 \neq 0$, then we can apply Lemma 3.2.9 and find $a_2 \in C_1$ such that a_2 has order π^{e_2}, where $e_1 \geq e_2 \geq 1$ and $C_1 = Ra_2 \oplus C_2$. Notice that $R/\pi R$ is a field, and

$$M(\pi)/\pi M(\pi) = (Ra_1)/(\pi Ra_1) \oplus (Ra_2)/(\pi Ra_2) \oplus C_2/\pi C_2.$$

is a finite dimensional vector space. Since $(Ra_i)/(\pi Ra_i)$ is a vector space of dimension one, the number of times we can apply Lemma 3.2.9 is bounded by the dimension of the vector space $M/\pi M$. After a finite number of iterations we arrive at (3).

(4): Fix a prime π in R such that $M(\pi)$ is nonzero. In the proof of Step (3) we saw that the integer m is uniquely determined since it is equal to the dimension of the vector space $M/\pi M$ over the field $R/\pi R$. Suppose there are two decompositions of $M(\pi)$ into direct sums of cyclic submodules

$$M(\pi) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_m = Rb_1 \oplus Rb_2 \oplus \cdots \oplus Rb_m,$$

where the order of a_i is equal to π^{e_i} where $e_1 \geq e_2 \geq \cdots \geq e_m$, and the order of b_i is equal to π^{f_i}, where $f_1 \geq f_2 \geq \cdots \geq f_m$. We must show that $e_i = f_i$ for each i. Consider the submodule

$$\pi M(\pi) = \pi Ra_1 \oplus \pi Ra_2 \oplus \cdots \oplus \pi Ra_m = \pi Rb_1 \oplus \pi Rb_2 \oplus \cdots \oplus \pi Rb_m.$$

By Lemma 3.2.7, the order of the cyclic module πRa_i is $\pi^{e_i - 1}$. If $e_1 = 1$, then $\pi M(\pi) = 0$ which implies $f_1 = 1$. The proof follows by induction on e_1. □

THEOREM 3.2.11. *(Basis Theorem – Invariant Factor Form) Let R be a PID and M a finitely generated R-module. The following are true.*

(1) *$M = F \oplus M_t$, where F is a free submodule of finite rank. The rank of F is uniquely determined by M.*

(2) *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*

$$M_t \cong R/(r_1 R) \oplus \cdots \oplus R/(r_\ell R).$$

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.*

PROOF. By Theorem 3.2.10, there is a finite set of primes $\{\pi_i \mid 1 \leq i \leq k\}$ and a finite set of nonnegative integers $\{e_{ij} \mid 1 \leq i \leq k,\, 1 \leq j \leq \ell\}$ such that

$$M_t \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\ell} R/(\pi_i^{e_{ij}} R).$$

For each i we assume $e_{i1} \geq e_{i2} \geq \cdots \geq e_{i\ell} \geq 0$. Also assume for at least one of the primes π_i that $e_{i\ell} \geq 1$. For each j such that $1 \leq j \leq \ell$, set $r'_j = \prod_{i=1}^{k} \pi_i^{e_{ij}}$. Then $r'_\ell \mid \cdots \mid r'_2 \mid r'_1$. Reverse the order by setting $r_1 = r'_\ell, r_2 = r'_{\ell-1}, \dots, r_\ell = r'_1$. By Proposition 3.2.1 (3),

$$R/(r'_j) \cong \bigoplus_{i=1}^{k} R/(\pi_i^{e_{ij}} R)$$

from which it follows that $M_t \cong R/(r_1 R) \oplus \cdots \oplus R/(r_\ell R)$. This proves the existence claim of Part (2).

For the uniqueness claim, suppose we are given the elements $r_1, \dots, r_\ell$ in R. By unique factorization in R, $r_\ell = \pi_1^{e_{1\ell}} \cdots \pi_k^{e_{k\ell}}$. Likewise, factor each of the other r_i. By stepping through the existence proof backwards, we get

$$M_t \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\ell} R/(\pi_i^{e_{ij}} R).$$

The uniqueness of the primes and the exponents follows from Theorem 3.2.10. This gives the uniqueness of the r_i. □

3. Matrix Theory

3.1. The Matrix of a Linear Transformation.

EXAMPLE 3.3.1. Let R be any ring. Let M and N be R-modules. By $\operatorname{Hom}_R(M,N)$ we denote the set of all R-module homomorphisms from M to N. We can turn $\operatorname{Hom}_R(M,N)$ into an additive abelian group. For $\phi, \psi \in \operatorname{Hom}_R(M,N)$ and $x \in M$, define

$$(\phi + \psi)(x) = \phi(x) + \psi(x).$$

If $M = N$, we define multiplication in $\operatorname{Hom}_R(M,M)$ to be composition of functions

$$(\phi\psi)(x) = \phi(\psi(x))$$

which turns $\operatorname{Hom}_R(M,M)$ into a ring. In fact, $\operatorname{Hom}_R(M,M)$ is a subring of $\operatorname{Hom}_{\mathbb{Z}}(M,M)$ (see Example 2.1.8). 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. Four such possibilities are given in Lemma 5.5.1.

EXAMPLE 3.3.2. Let R be a commutative ring and M an R-module. If $r \in R$, then "left multiplication by r" is $\ell_r : M \to M$, where $\ell_r(x) = rx$. The mapping $r \mapsto \ell_r$ defines a homomorphism of rings $\theta : R \to \operatorname{Hom}_R(M,M)$, which we call the *left regular representation* of R in $\operatorname{Hom}_R(M,M)$. The homomorphism θ turns $\operatorname{Hom}_R(M,M)$ into an R-algebra. The proofs are left to the reader.

EXAMPLE 3.3.3. Let R be a commutative ring and A an R-algebra. Then A acts on itself as a ring of R-module homomorphisms. That is, if $a \in A$, then "left multiplication by a" is $\ell_a : A \to A$, where $\ell_a(x) = ax$. The mapping $a \mapsto \ell_a$ defines an R-algebra homomorphism $\theta : A \to \operatorname{Hom}_R(A,A)$ which is called the *left regular representation* of A in $\operatorname{Hom}_R(A,A)$. Because $\ell_\alpha(1) = \alpha$, the map θ is one-to-one. The proofs are left to the reader.

EXAMPLE 3.3.4. 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 as a ring of R-module homomorphisms of M. That is, if $a \in A$, then "left multiplication by a" is $\ell_a : M \to M$, where $\ell_a(x) = ax$. The mapping $a \mapsto \ell_a$ defines an R-algebra homomorphism $\varphi : A \to \operatorname{Hom}_R(M,M)$ which is called the *left regular representation* of A in $\operatorname{Hom}_R(M,M)$. The proofs are left to the reader.

DEFINITION 3.3.5. Let R be any ring and m,n positive integers. By $M_{nm}(R)$ we denote the set of all n-by-m matrices over R. If $m=n$, then we simply write $M_n(R)$ instead of $M_{nn}(R)$. Addition of matrices is coordinate-wise $(\alpha_{ij})+(\beta_{ij})=(\alpha_{ij}+\beta_{ij})$. We can multiply by elements of R from the left $r(\alpha_{ij})=(r\alpha_{ij})$, or from the right $(\alpha_{ij})r=(\alpha_{ij}r)$. Therefore, in the terminology of Definition 5.4.8, $M_{nm}(R)$ is a left R right R bimodule. If $(\alpha_{ij})\in M_{nm}(R)$ and $(\beta_{jk})\in M_{mp}(R)$, then the matrix product is defined by $(\alpha_{ij})(\beta_{jk})=(\gamma_{ik})\in M_{np}(R)$, where $\gamma_{ik}=\sum_{j=1}^{m}\alpha_{ij}\beta_{jk}$.

DEFINITION 3.3.6. Let e_{ij} be the matrix with 1 in position (i,j) and 0 elsewhere. The matrix e_{ij} is called an *elementary* matrix.

LEMMA 3.3.7. *For any ring R, the set $M_{nm}(R)$ of n-by-m matrices over R is a free R-module. The set $\{e_{ij} \mid 1\le i\le n,\ 1\le j\le m\}$ of elementary matrices is a free basis with nm elements.*

PROOF. The proof is left to the reader. □

DEFINITION 3.3.8. 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 $M_{nm}(R)$.

PROPOSITION 3.3.9. *Let R be any ring. If M is a free R-module of rank m, and N is a free R-module of rank n, then there is a $\mathbb{Z}$-module isomorphism* $\operatorname{Hom}_R(M,N)\cong M_{nm}(R)$. *If R is a commutative ring, then* $\operatorname{Hom}_R(M,N)$ *is a free R-module of rank mn.*

PROOF. Let $X=\{x_1,\dots,x_m\}$ be a basis for M and $Y=\{y_1,\dots,y_n\}$ a basis for N. The assignment $\phi\mapsto M(\phi,X,Y)$ defines an $\mathbb{Z}$-module homomorphism

$$M(\cdot,X,Y):\operatorname{Hom}_R(M,N)\to M_{nm}(R).$$

Conversely, if $(\alpha_{ij})\in M_{nm}(R)$, define α in $\operatorname{Hom}_R(M,N)$ by

$$\alpha(x_j)=\sum_{i=1}^{n}\alpha_{ij}y_i.$$

The rest is left to the reader. □

PROPOSITION 3.3.10. *Let R be any ring. Let M, N, and P denote free R-modules, each of finite rank. Let X, Y and Z be bases for M, N, and P respectively. Let $\phi\in$* $\operatorname{Hom}_R(M,N)$ *and $\psi\in$* $\operatorname{Hom}_R(N,P)$. *If the matrices $M(\psi,Y,Z)$ and $M(\phi,X,Y)$ are treated as having entries from the ring R^o, the opposite ring of R, then*

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

PROOF. The opposite ring R^o is defined as in Definition 2.1.9. Let $X=\{x_1,\dots,x_m\}$, $Y=\{y_1,\dots,y_n\}$, and $Z=\{z_1,\dots,z_p\}$. Let $M(\phi,X,Y)=(\phi_{ij})$, $M(\psi,Y,Z)=(\psi_{ij})$. It follows from

$$\psi\phi(x_j)=\psi\left(\sum_{i=1}^{n}\phi_{ij}y_i\right)=\sum_{i=1}^{n}\phi_{ij}\sum_{k=1}^{p}\psi_{ki}z_k=\sum_{k=1}^{p}\left(\sum_{i=1}^{n}\phi_{ij}\psi_{ki}\right)z_k$$

that $M(\psi\phi, X, Z) = (\gamma_{kj})$, where $\gamma_{kj} = \sum_{i=1}^{n} \phi_{ij}\psi_{ki}$. Computing the product of the two matrices over R^o, we get $M(\psi, Y, Z)M(\phi, X, Y) = (\tau_{kj})$, where

$$\tau_{kj} = \sum_{i=1}^{n} \psi_{ki} * \phi_{ij} = \sum_{i=1}^{n} \phi_{ij}\psi_{ki}.$$

□

COROLLARY 3.3.11. *Let R be any ring. With the binary operations defined in Definition 3.3.5, $M_n(R)$ is a ring with identity element $I_n = e_{11} + \cdots + e_{nn}$. The set $R \cdot I_n$ of all scalar matrices in $M_n(R)$ is a subring which is isomorphic to R. The center of the ring $M_n(R)$ is equal to the center of the subring $R \cdot I_n$. If R is commutative, $M_n(R)$ is an R-algebra and the center of $M_n(R)$ is equal to $R \cdot I_n$.*

PROOF. Use Proposition 3.3.10 to show that matrix multiplication is associative. The rest is left to the reader. □

PROPOSITION 3.3.12. *Let R be any ring. If M is a free R-module of rank n, then 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.*

PROOF. Pick a basis for M. The map of Proposition 3.3.9 defines an isomorphism of abelian groups. It is multiplicative by Proposition 3.3.10. □

DEFINITION 3.3.13. Let R be a commutative ring and $n \geq 1$. If A, B are matrices in $M_n(R)$ and P is an invertible matrix in $M_n(R)$ such that $A = P^{-1}BP$, then we say A and B are *similar*. The reader should verify that this defines an equivalence relation on $M_n(R)$.

PROPOSITION 3.3.14. *Let R be a commutative ring and M a free R-module of rank n. Let X and Y be two bases for M. If $\phi \in \operatorname{Hom}_R(M, M)$, then the matrix $M(\phi, X, X)$ of ϕ with respect to X and the matrix $M(\phi, Y, Y)$ of ϕ with respect to Y are similar. In fact, if $1 \in \operatorname{Hom}_R(M, M)$ is the identity map, then $M(1, X, Y)^{-1} = M(1, Y, X)$ and $M(\phi, X, X) = M(1, Y, X)M(\phi, Y, Y)M(1, X, Y)$.*

PROOF. Let $I \in M_n(R)$ be the identity matrix. It follows from Proposition 3.3.10 that $I = M(1, X, X) = M(1, Y, Y)$, $M(1, X, Y)M(1, Y, X) = I$, and $M(1, Y, X)M(1, X, Y) = I$. Also $M(\phi, X, Y) = M(1, X, Y)M(\phi, X, X) = M(\phi, Y, Y)M(1, X, Y)$. □

EXAMPLE 3.3.15. Let R be a commutative ring and $A \in M_{mn}(R)$. Elements of R^n can be viewed as n-by-1 column matrices in M_{n1}. As in Proposition 3.3.9, multiplication by A from the left defines an element in $\operatorname{Hom}_R(R^n, R^m)$. In particular, if k is a field and $A \in M_n(k)$, then left multiplication by A defines a linear transformation from k^n to k^n. We define the rank of A and the nullity of A as in Exercise 3.1.26. Define the *column space* of A to be the subspace of k^n spanned by the columns of A. The rank of A is seen to be the dimension of the column space of A.

3.2. The Dual of a Module.

DEFINITION 3.3.16. Let R be any ring. Let M be a left R-module. The *dual of M* is defined to be $M^* = \operatorname{Hom}_R(M, R)$. We turn M^* into a right R-module by the action $(fr)(x) = (f(x))r$, for $r \in R$, $f \in M^*$, $x \in M$. The reader should verify that this is a well defined right R-module action on M^*. If N is another left R-module, and $\psi \in \operatorname{Hom}_R(M, N)$, define $\psi^* : N^* \to M^*$ by the rule $\psi^*(f) = f \circ \psi$, for any $f \in N^*$.

LEMMA 3.3.17. *Let R be any ring. Let M and N be left R-modules. If $\psi : M \to N$ is a homomorphism of left R-modules, then $\psi^* : N^* \to M^*$ is a homomorphism of right R-modules. If L is another R-module, and $\phi \in \operatorname{Hom}_R(L,M)$, then $(\psi\phi)^* = \phi^*\psi^*$.*

PROOF. Let $f, g \in N^*$ and $a \in R$. The reader should verify that $\psi^*(f+g) = \psi^*(f) + \psi^*(g)$. If $x \in M$, then

$$(\psi^*(fa))(x) = (fa)(\psi(x)) = (f(\psi(x)))a = (\psi^*(f)(x))a = (\psi^*(f)a)(x).$$

Lastly, $\phi^*\psi^*(f) = (\psi\phi)^*(f)$. □

DEFINITION 3.3.18. Let M be a left R-module which is free of finite rank. If $B = \{v_1, \dots, v_n\}$ is a basis for M, then define $v_1^*, \dots, v_n^*$ in M^* by the rules

$$v_i^*(v_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

PROPOSITION 3.3.19. *If M is a free left R-module with basis $B = \{v_1, \dots, v_n\}$, then M^* is a free right R-module with basis $B^* = \{v_1^*, \dots, v_n^*\}$.*

PROOF. By Proposition 3.3.9, M^* is isomorphic to $M_{1n}(R)$ as $\mathbb{Z}$-modules. Under this isomorphism, v_i^* is mapped to the row matrix e_{1i} which has 1 in position i and zeros elsewhere. This is therefore a homomorphism of right R-modules. □

THEOREM 3.3.20. *Let R be any ring. Let M and N be free R-modules, each of finite rank. Let X be a basis for M, and Y a basis for N. Let X^* and Y^* be the corresponding bases for M^* and N^*. Given $\phi \in \operatorname{Hom}_R(M,N)$,*

$$M(\phi^*, Y^*, X^*) = M(\phi, X, Y)^T.$$

That is, the matrix of ϕ^* with respect to Y^* and X^* is the transpose of the matrix of ϕ with respect to X and Y.

PROOF. Let $X = \{u_1, \dots, u_m\}$ and $Y = \{v_1, \dots, v_n\}$. Let $M(\phi, X, Y) = (\phi_{ij})$. Consider $\phi^*(v_l^*)(u_j) = v_l^*(\phi(u_j)) = v_l^*(\sum_{i=1}^n \phi_{ij} v_i) = \phi_{lj}$. Now consider $(\sum_{i=1}^m \phi_{li} u_i^*)(u_j) = \phi_{lj}$. Therefore, $\phi^*(v_l^*) = \sum_{i=1}^m \phi_{li} u_i^*$ as elements of $M^* = \operatorname{Hom}_R(M,R)$ because they agree on a basis of M. This also shows that column l of the matrix $M(\phi^*, Y^*, X^*)$ is the transpose of $(\phi_{l1}, \phi_{l2}, \dots, \phi_{lm})$, which is row l of $M(\phi, X, Y)$ □

DEFINITION 3.3.21. If k is a field, the space $V^{**} = \operatorname{Hom}_k(V^*, k)$ is called the *double dual* of V. Given $v \in V$, let $\varphi_v : V^* \to k$ be the "evaluation at v" map. That is, if $f \in V^*$, then $\varphi_v(f) = f(v)$. The reader should verify that φ_v is an element of V^{**}, and that the assignment $v \mapsto \varphi_v$ is a homomorphism of k-vector spaces $V \to V^{**}$.

THEOREM 3.3.22. *Let V be a vector space over a field k. The map $V \to V^{**}$ which sends a vector $v \in V$ to φ_v is one-to-one. If V is finite dimensional, this is a vector space isomorphism.*

PROOF. Let v be a nonzero vector in V. By Theorem 3.1.28 we can extend $\{v\}$ to a basis for V, say $B = \{v, v_2, \dots, v_n\}$. Define $f \in V^*$ to be the projection mapping onto the v-coordinate. Then $f(v) = 1$, and $f(v_i) = 0$ for $2 \le i \le n$. Then $\varphi_v(f) = f(v) = 1$. This proves $V \to V^{**}$ is one-to-one. If V is finite dimensional, then $V \to V^{**}$ is onto since $\dim_k(V) = \dim_k(V^{**})$. □

Exercise 5.5.8 extends Theorem 3.3.22 to finitely generated projective modules over any ring.

THEOREM 3.3.23. *Let D be a division ring and V and W finitely generated D-vector spaces. Let $\phi \in \operatorname{Hom}_D(V,W)$. Let $\phi^* : W^* \to V^*$ be the associated homomorphism of right D-vector spaces.*

(1) If ϕ is one-to-one, then ϕ^* is onto.
(2) If ϕ is onto, then ϕ^* is one-to-one.
(3) The rank of ϕ is equal to the rank of ϕ^*.

PROOF. (1): Assume ϕ is one-to-one. Let $f : V \to D$ be in V^*. By Exercise 3.1.30 there is $\bar{f} : W \to D$ in W^* such that $f = \bar{f}\phi = \phi^*(\bar{f})$.

(2): Assume ϕ is onto. A typical element of W is of the form $w = \phi(v)$, for some $v \in V$. Assume $g \in W^*$ and $g\phi = 0$. Then $g(w) = g(\phi(v)) = 0$.

(3): Let $n = \dim_D(V)$. By Proposition 3.3.9, $\dim_D(V^*) = n$. Let $U = \ker\phi$. Let $\psi : U \to V$ be the inclusion map. By (1), ψ^* is onto. Then $\operatorname{Rank}(\psi^*) = \dim(U^*) = \dim(U) = \operatorname{Nullity}(\phi) = n - \operatorname{Rank}\phi$. By Lemma 3.3.17, $\operatorname{im}\phi^* \subseteq \ker\psi^*$. We prove the reverse inclusion. Suppose $f \in V^*$ and $\psi^*(f) = f\psi = 0$. Then f factors through $V/\ker\phi = \operatorname{im}\phi$. There is $\bar{f} : \operatorname{im}\phi \to D$ such that $f = \bar{f}\phi$. By Exercise 3.1.30, $\bar{f}$ extends to W, so f is in the image of ϕ^*. This proves $\operatorname{Rank}\phi^* = \operatorname{Nullity}\psi^* = n - \operatorname{Rank}\psi^* = \operatorname{Rank}\phi$. □

COROLLARY 3.3.24. *Let D be a division ring and $A \in M_{nm}(D)$. The row rank of A is equal to the column rank of A.*

PROOF. As in Proposition 3.3.9, define α in $\operatorname{Hom}_D(D^m, D^n)$ to be "left multiplication by A". Let α^* be the associated map on dual spaces. By Theorem 3.3.20 the matrix of α^* is A^T. The column rank of A is equal to $\operatorname{Rank}\alpha$ which is equal to $\operatorname{Rank}\alpha^*$, by Theorem 3.3.23. But $\operatorname{Rank}\alpha^*$ is equal to the column rank of A^T, which is the row rank of A. □

3.3. Exercises.

EXERCISE 3.3.1. Let k be a field and V a finite dimensional vector space over k. Show that $\operatorname{Hom}_k(V,V)$ is a commutative ring if and only if $\dim_k(V) \le 1$.

EXERCISE 3.3.2. Suppose $\phi \in \operatorname{Hom}_D(V,V)$, where V is a finite dimensional vector space over the division ring D. Prove:

(1) There is a chain of subspaces $\ker(\phi) \subseteq \ker(\phi^2) \subseteq \ker(\phi^3) \subseteq \cdots$.
(2) There is a chain of subspaces $\phi(V) \supseteq \phi^2(V) \supseteq \phi^3(V) \supseteq \cdots$.
(3) The kernel of $\phi : \phi(V) \to \phi^2(V)$ is equal to $\ker(\phi) \cap \phi(V)$. More generally, if $m \ge 1$, the kernel of $\phi^m : \phi^m(V) \to \phi^{2m}(V)$ is equal to $\ker(\phi^m) \cap \phi^m(V)$.
(4) If $m \ge 1$ and $\phi^m(V) = \phi^{m+1}(V)$, then $\phi^m(V) = \phi^{m+i}(V)$ for all $i \ge 1$.
(5) If $n = \dim_D(V)$, then there exists m such that $1 \le m \le n$ and $\phi^m(V) = \phi^{m+1}(V)$.
(6) If $n = \dim_D(V)$, then there exists m such that $1 \le m \le n$ and $\ker(\phi^m) \cap \phi^m(V) = (0)$.

EXERCISE 3.3.3. Let R be a commutative ring. Let $A \in M_{nm}(R)$ and $B, C \in M_{ml}(R)$. Prove:

(1) $(A^T)^T = A$.
(2) $(B+C)^T = B^T + C^T$.
(3) $(AB)^T = B^T A^T$.

EXERCISE 3.3.4. If R is a commutative ring, show that the mapping $M_n(R) \to M_n(R)^o$ defined by $A \mapsto A^T$ is an isomorphism of R-algebras.

EXERCISE 3.3.5. If R is any ring, show that the mapping $M_n(R) \to M_n(R^o)^o$ defined by $A \mapsto A^T$ is an isomorphism of rings. Using the Morita Theorems, a very general version of this is proved in Corollary 5.9.3 (4).

3.4. Minimal Polynomial. Let k be a field and A a finite dimensional k-algebra. Given $\alpha \in A$, the evaluation homomorphism (Theorem 2.5.2) is a k-algebra homomorphism $\sigma : k[x] \to A$ determined by $x \mapsto \alpha$. The image of σ is denoted $k[\alpha]$ (Exercise 2.5.16). Since $k[\alpha]$ is a subspace of the finite dimensional vector space A, $k[\alpha]$ is finite dimensional. Since $k[x]$ is infinite dimensional, we know that the kernel of σ is nonzero. Since $k[x]$ is a principal ideal domain, there exists a monic polynomial $p \in k[x]$ which generates the kernel of σ. Clearly p is the unique polynomial in $k[x]$ satisfying

(1) p is monic,
(2) $p(\alpha) = 0$, and
(3) if $f \in k[x]$ and $f(\alpha) = 0$, then p divides f.

We call p the *minimal polynomial of α over k*, and write $p = \operatorname{min.poly}_k(\alpha)$. We view k as a subring of the center of A. Therefore the ring $k[\alpha]$ is a commutative subring of A. Since $k[\alpha]$ is a homomorphic image of the principal ideal domain $k[x]$, it follows that $k[\alpha]$ is a principal ideal ring. Since $k[\alpha]$ is a subring of A, we can view A as a module over $k[\alpha]$. Let $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be the minimal polynomial of α. Since $k[\alpha] \cong k[x]/(p)$, Exercise 3.1.17 says $k[\alpha]$ is a k-vector space of dimension n spanned by $1, \alpha, \dots, \alpha^{n-1}$.

EXAMPLE 3.3.25. Since $M_n(k)$ is finite dimensional over k, every matrix $A \in M_n(k)$ has a minimal polynomial $\operatorname{min.poly}_k(A)$. The evaluation homomorphism $x \mapsto A$ maps $k[x]$ onto the commutative subring $k[A]$ of $M_n(R)$.

EXAMPLE 3.3.26. If V is a finite dimensional vector space over k, then $\operatorname{Hom}_k(V,V)$ is finite dimensional by Proposition 3.3.9, so every ϕ in $\operatorname{Hom}_k(V,V)$ has a minimal polynomial $p = \operatorname{min.poly}_k(\phi)$. By Proposition 3.3.12, $M_n(k)$ and $\operatorname{Hom}_k(V,V)$ are isomorphic as k-algebras. If X is a basis for V, and $A = M(\phi, X, X)$, then $\operatorname{min.poly}_k(\phi) = \operatorname{min.poly}_k(A)$. The evaluation homomorphism $\sigma : k[x] \to \operatorname{Hom}_k(V,V)$ defined by $x \mapsto \phi$ maps $k[x]$ onto the commutative subring $k[\phi]$. There is a k-algebra isomorphism $k[x]/(p) \cong k[\phi]$ and $k[\phi]$ is a principal ideal ring which is a semilocal ring. The ideals in $k[\phi]$ correspond up to associates to the divisors of p in $k[x]$ (see Proposition 3.2.1).

Using the k-algebra homomorphism σ, $k[x]$ acts as a ring of k-vector space homomorphisms on V. Given a polynomial $f \in k[x]$, and a vector $u \in V$ the action is given by $fu = \sigma(f)u = f(\phi)u$. This makes V into a $k[x]$-module, which is denoted by V_ϕ. Since V is finitely generated as a vector space over k, it is immediate that V_ϕ is finitely generated as a module over $k[x]$. The structure theory of Section 3.2 applies to the $k[\phi]$-module V_ϕ. If $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is the minimal polynomial of ϕ, then a k-basis for $k[\phi]$ is $\{\phi^{n-1}, \dots, \phi, 1\}$. If $u \in V$, the cyclic $k[x]$-submodule of V generated by u is therefore equal to

$$k[\phi]u = \{f(\phi)u \mid f \in k[x]\} = k\phi^{n-1}u + \cdots + k\phi u + k.$$

Since ϕ maps this subspace to itself, we say $k[\phi]u$ is *ϕ-invariant*. If u is nonzero, the $k[x]$-module homomorphism $k[x] \to k[\phi]u$ is onto and the kernel is a principal ideal $I_u = (q)$,

$$k[\phi]u \cong k[x]/(q).$$

The polynomial q is the order of u. Since u is nonzero and $k[\phi]u$ is finite dimensional over k, we can assume q is a monic polynomial of positive degree. In fact, q is the polynomial of minimal degree such that $q(\phi)u = 0$. By Exercise 3.3.8, q is a divisor of the minimal polynomial p of ϕ. It is clear that q is the minimal polynomial of the restriction of ϕ to the ϕ-invariant subspace $k[\phi]u$.

LEMMA 3.3.27. *Let V be a finite dimensional vector space over the field k. Let ϕ and ψ be linear transformations in $\operatorname{Hom}_k(V,V)$. The $k[x]$-modules V_ϕ and V_ψ are isomorphic if and only if there exists an invertible linear transformation ρ in $\operatorname{Hom}_k(V,V)$ such that $\phi = \rho^{-1}\psi\rho$.*

PROOF. Let $f : V_\phi \to V_\psi$ be an isomorphism of $k[x]$-modules. Then f is an isomorphism of k-vector spaces. That is, $f = \rho$ for some invertible element ρ in $\operatorname{Hom}_k(V,V)$. For each $u \in V$ we have $f(\phi u) = \psi f(u)$. Therefore, $\phi = \rho^{-1}\psi\rho$. Conversely, if $\phi = \rho^{-1}\psi\rho$, define $f : V_\phi \to V_\psi$ by $f(u) = \rho u$. For $i \geq 1$, we have $\rho\phi^i = \psi^i\rho$. Then $f(\phi^i u) = \rho\phi^i u = \psi^i\rho u = \psi^i f(u)$. The rest follows from the fact that ρ is k-linear. □

3.5. Rational Canonical Form.

THEOREM 3.3.28. *If V is a finite dimensional vector space over the field k, and $\phi \in \operatorname{Hom}_k(V,V)$, then there is a basis $\{u_1, u_2, \dots, u_r\}$ for the $k[\phi]$-module V such that the following are true.*

1. *The $k[\phi]$-module V is equal to the internal direct sum $U_1 \oplus U_2 \oplus \cdots \oplus U_r$ where $U_i = k[\phi]u_i$ is the cyclic submodule of V spanned by u_i.*
2. *$U_i \cong k[x]/(q_i)$ where q_i is the order of u_i and $q_1 \mid q_2 \mid \cdots \mid q_r$.*
3. *U_i is a ϕ-invariant subspace of V and the minimal polynomial of $\phi|_{U_i}$ is q_i.*
4. *The minimal polynomial of ϕ is q_r.*
5. *The sequence of polynomials $(q_1, q_2, \dots, q_r)$ is uniquely determined by ϕ.*

The polynomials $q_1, \dots, q_r$ are called the invariant factors *of ϕ.*

PROOF. Apply Theorem 3.2.11 to the finitely generated $k[x]$-module V. □

If V and ϕ are as in Theorem 3.3.28, then $V = U_1 \oplus \cdots \oplus U_r$ where each $\phi(U_i) \subseteq U_i$. Then each U_i is a k-subspace of V. We can pick a k-basis B_i for each subspace U_i and concatenate to get a basis $B = B_1 + \cdots + B_r$ for V. It is clear that the matrix of ϕ with respect to B is the block diagonal matrix (see Exercise 3.4.3)

$$M(\phi,B) = \operatorname{diag}(M(\phi|_{U_1},B_1),\dots,M(\phi|_{U_r},B_r))$$

where there are r blocks and block i is the matrix with respect to B_i of the restriction of ϕ to U_i.

Now we determine a canonical form for the matrix of ϕ. In other words, we try to find a basis B of V for which the matrix $M(\phi,B)$ is simplified. Based on the previous paragraph, we consider the case where $V = k[\phi]u$ is a cyclic module over the ring $k[\phi]$. Suppose the minimal polynomial of ϕ is $\operatorname{min.poly}_k(\phi) = p = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. The $k[x]$-module homomorphism $k[x] \to k[\phi]u$ defined by $1 \mapsto u$ is surjective and the kernel is the principal ideal $I_u = (p)$ generated by p. Therefore, as a $k[x]$-module, V is isomorphic to $k[x]/(p)$. Applying the division algorithm, we see that $1, x, x^2, \dots, x^{n-1}$ is a k-basis for $k[x]/(p)$. Therefore, a k-basis for V is $B = \{u, \phi u, \phi^2 u, \dots, \phi^{n-1}u\}$. Introduce the notation $x_i = \phi^{i-1}u$. The action of ϕ on $B = \{x_1, x_2, \dots, x_n\}$ determines the matrix $M(\phi,B)$.

Computing, we get

$$\begin{aligned}
\phi x_1 &= \phi u = x_2 \\
\phi x_2 &= \phi\phi u = x_3 \\
&\vdots \\
\phi x_{n-1} &= \phi^{n-1} u = x_n \\
\phi x_n &= \phi^n u = -a_{n-1}\phi^{n-1}u - \cdots - a_1\phi^1 u - a_0 u = -a_0 x_1 - a_1 x_2 - \cdots - a_{n-1}x_n
\end{aligned}$$

so the matrix is

$$M(\phi,B) = \begin{bmatrix}
0 & 0 & 0 & \dots & 0 & 0 & -a_0 \\
1 & 0 & 0 & \dots & 0 & 0 & -a_1 \\
0 & 1 & 0 & \dots & 0 & 0 & -a_2 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \\
0 & 0 & 0 & \dots & 0 & 0 & -a_{n-3} \\
0 & 0 & 0 & \dots & 1 & 0 & -a_{n-2} \\
0 & 0 & 0 & \dots & 0 & 1 & -a_{n-1}
\end{bmatrix}. \tag{3.5}$$

We call (3.5) the *companion matrix* of the polynomial $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. If $p \in k[x]$ is a polynomial of degree $n \geq 1$, denote the companion matrix of p in $M_n(k)$ by $C(p)$. Conversely, by Exercise 3.4.1, the minimal polynomial of (3.5) is again $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

COROLLARY 3.3.29. *If V is a finite dimensional vector space over the field k, $\phi \in \operatorname{Hom}_k(V,V)$, and $q_1, q_2, \dots, q_r$ are the invariant factors of ϕ, then there is a basis B for V such that the matrix of ϕ with respect to B is the block diagonal matrix*

$$M(\phi,B) = \operatorname{diag}\left(C(q_1), C(q_2), \dots, C(q_r)\right)$$

where block i is the companion matrix of q_i. The matrix $M(\phi,B)$ is called the rational canonical form *for ϕ.*

3.6. Jordan Canonical Form.

THEOREM 3.3.30. *If V is a finite dimensional vector space over the field k, and $\phi \in \operatorname{Hom}_k(V,V)$, then there exist positive integers $s, \nu_1, \dots, \nu_s$ and a basis $\{u_{ij} \mid 1 \leq i \leq s; 1 \leq j \leq \nu_i\}$ for the $k[\phi]$-module V such that the following are true.*

1. *The $k[\phi]$-module V is equal to the internal direct sum*

$$V = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{\nu_i} U_{ij}$$

   where $U_i = k[\phi]u_{ij}$ is the cyclic submodule of V spanned by u_{ij}.

2. *$U_{ij} \cong k[x]/(\pi_i^{e_{ij}})$ where*
   - (a) *$\pi_1, \dots, \pi_s$ are distinct monic irreducible polynomials,*
   - (b) *the order of u_{ij} is $\pi_i^{e_{ij}}$, and*
   - (c) *$e_{i1} \geq e_{i2} \geq \cdots \geq e_{i\nu_i} \geq 1$.*
3. *U_{ij} is a ϕ-invariant subspace of V and the minimal polynomial of $\phi|_{U_{ij}}$ is $\pi_i^{e_{ij}}$.*
4. *The minimal polynomial of ϕ is*

$$\operatorname{min.poly}_k(\phi) = \prod_{i=1}^{s} \pi_i^{e_{i1}}$$

(5) *The sequence of irreducible polynomials* $(\pi_1, \pi_2, \dots, \pi_s)$ *and the positive integers* $\{e_{ij}\}$ *are uniquely determined by* ϕ.

The polynomials $\pi_i^{e_{ij}}$ *are called the* elementary divisors *of* ϕ.

PROOF. Apply Theorem 3.2.10 to the finitely generated $k[x]$-module V. □

Using the basis for V given by Theorem 3.3.30, we determine a canonical form for the matrix of ϕ. The minimal polynomial for ϕ restricted to U_{ij} is a power of the irreducible polynomial π_i. We assume each π_i is a linear polynomial, because the canonical form of ϕ in this case is particularly simplified. This case will occur if and only if the minimal polynomial of ϕ factors into a product of linear polynomials in $k[x]$. The k-bases for the individual ϕ-invariant subspaces U_{ij} can be concatenated for a basis of V. We now determine a canonical form for the matrix of ϕ under the following assumptions

(1) V is a cyclic $k[\phi]$-module spanned by u.
(2) $\min.\mathrm{poly}_k(\phi) = (x-b)^n$ is a power of a linear polynomial.

Notice that V is a cyclic $k[\phi]$-module, spanned by u. Since $k[\phi] = k[\phi - b]$, it follows that V is a cyclic $k[\phi - b]$-module, spanned by u. If $\theta : k[x] \to \mathrm{Hom}_k(V,V)$ is defined by $x \mapsto \phi$, then $\ker\theta$ is the principal ideal generated by $(x-b)^n$. If $\tau : k[x] \to \mathrm{Hom}_k(V,V)$ is defined by $x \mapsto \phi - b$, then the minimal polynomial of $\psi = \phi - b$ is the monic generator of $\ker\tau$, which is x^n. Therefore $B = \{u, \psi u, \psi^2 u, \dots, \psi^{n-1}u\}$ is a k-basis for V. The matrix of $\psi = \phi - b$ with respect to the basis B is

$$M(\phi - b, B) = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & & & \vdots & & & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{bmatrix}$$

which is the companion matrix of the polynomial x^n. The matrix of ϕ with respect to the basis B is equal to $M(\phi,B) = M(\phi - b, B) + M(b,B)$. Therefore,

$$M(\phi, B) = \begin{bmatrix} b & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & b & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & b & \dots & 0 & 0 & 0 \\ \vdots & & & \vdots & & & \vdots \\ 0 & 0 & 0 & \dots & b & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & b & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & b \end{bmatrix}. \tag{3.6}$$

We denote the n-by-n matrix (3.6) by $J_n(b)$ and refer to it as the basic *Jordan block* for the polynomial $(x-b)^n$.

COROLLARY 3.3.31. *Assume V is a finite dimensional vector space over the field k, $\phi \in \mathrm{Hom}_k(V,V)$, and that the minimal polynomial* $\min.\mathrm{poly}_k(\phi)$ *factors into a product of linear factors in $k[x]$. If $b_1, \dots, b_s$ are the distinct roots of* $\min.\mathrm{poly}_k(\phi)$ *and $\{e_{ij}\}$ is the set of exponents of the elementary divisors of ϕ, then there is a basis B for V such that the matrix of ϕ with respect to B is the block diagonal matrix*

$$M(\phi,B) = \mathrm{diag}\left(J_{e_{11}}(b_1), J_{e_{12}}(b_1), \dots, J_{e_{ij}}(b_i), \dots\right)$$

where the block corresponding to the ordered pair (i,j) is the Jordan matrix of $(x-b_i)^{e_{ij}}$. The matrix $M(\phi,B)$ is called the Jordan canonical form *for ϕ and B is called a* Jordan basis.

Let k be a field, and A a matrix in $M_n(k)$. With respect to the standard basis on $k^{(n)}$, left multiplication by A defines a linear transformation ℓ_A in $\operatorname{Hom}_k(k^{(n)},k^{(n)})$. The invariant factors, elementary divisors, rational canonical form, and the Jordan canonical form of A are defined to be the corresponding invariants of ℓ_A.

COROLLARY 3.3.32. *Let k be a field, and A and B two matrices in $M_n(k)$. The following are equivalent.*

(1) A and B are similar.
(2) A and B have the same invariant factors.
(3) A and B have the same rational canonical form.

PROOF. If A and B have the same invariant factors, say $q_1,q_2,\dots,q_r$, then they are both similar to the block diagonal matrix $C = \operatorname{diag}(C(q_1),C(q_2),\dots,C(q_r))$. The matrix C is in rational canonical form. The reader should verify that the invariant factors of C are $q_1,\dots,q_r$. If A and B are similar, then by Proposition 3.3.12 and Lemma 3.3.27, the $k[x]$-modules that they induce on k^n are isomorphic. So they have the same invariant factors. □

3.7. Exercises.

EXERCISE 3.3.6. Let k be a field and A a finite dimensional k-algebra. Let $\alpha \in A$ and $f = \operatorname{min.poly}_k(\alpha)$. Prove:

(1) α is invertible in A if and only if $f(0) \neq 0$.
(2) α is left invertible if and only if α is right invertible.

EXERCISE 3.3.7. Let R be a commutative ring and A an R-algebra. Suppose $\alpha \in A$ is a root of the polynomial $p \in R[x]$. Prove:

(1) If $\phi : A \to A$ is an R-algebra homomorphism, then $\phi(\alpha)$ is a root of p.
(2) If u is a unit in A, then $u^{-1}\alpha u$ is a root of p.

EXERCISE 3.3.8. Let k be a field, V a finite dimensional k-vector space, u a nonzero vector in V, and $\phi \in \operatorname{Hom}_k(V,V)$. Let $f \in k[x]$ be the monic polynomial of minimal degree such that $f(\phi)u = 0$. Prove that f divides $\operatorname{min.poly}_k(\phi)$.

EXERCISE 3.3.9. Let k be a field and A a finite dimensional k-algebra. Let $\alpha \in A$. The assignment $x \mapsto \alpha$ defines the evaluation homomorphism $k[x] \to A$ whose image is the commutative subalgebra $k[\alpha]$ of A (Exercise 2.5.16). Show that $k[\alpha]$ is a field if and only if $\operatorname{min.poly}_k(\alpha)$ is irreducible.

EXERCISE 3.3.10. 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) The k-algebra $k[x]/(x-a)$ is isomorphic to k.
(2) There is a k-algebra isomorphism $k[x]/(f) \cong k \oplus k$.
(3) There is a k-algebra isomorphism $k[x]/(g) \cong k[x]/(x^2)$.
(4) 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 3.3.11. Let k be a field and A a finite dimensional k-algebra. Prove that if $\dim_k(A) = 2$, then A is commutative.

EXERCISE 3.3.12. Classify up to isomorphism all finite rings of order four.

EXERCISE 3.3.13. Let k be a field and $A \in M_n(k)$. Let F be a field which contains k as a subfield. Prove:

1. A is invertible in $M_n(k)$ if and only if A is invertible in $M_n(F)$.
2. The rank of A over k is equal to the rank of A over F.
3. The invariant factors of A in $k[x]$ are the same as the invariant factors of A in $F[x]$.
4. If $A, B \in M_n(k)$, then A and B are similar in $M_n(k)$ if and only if A and B are similar in $M_n(F)$.

EXERCISE 3.3.14. Let k be a field and $A, B, C \in M_n(k)$. Prove:

1. If C is invertible, then $\operatorname{Rank}(AC) = \operatorname{Rank}(CA) = \operatorname{Rank}(A)$.
2. If A and B are similar, then $\operatorname{Rank}(A) = \operatorname{Rank}(B)$.

EXERCISE 3.3.15. Let R be any ring and $b \in R$. Let $B \in M_n(R)$ be the Jordan block corresponding to $(x-b)^n$. That is, B is the matrix which has main diagonal entries all equal to b, first lower subdiagonal entries all equal to 1 and 0 elsewhere. Prove that the transpose of B is similar to B.

EXERCISE 3.3.16. Assume A is an n-by-n matrix over the field $\mathbb{Q}$ such that the minimal polynomial of A in $\mathbb{Q}[x]$ is equal to $(x^2+1)(x+2)$. If $n = 7$, exhibit all possible rational canonical forms for A.

EXERCISE 3.3.17. Let R be any ring, and M an R-module. Prove that $\operatorname{Hom}_R(M, M)$ is the trivial ring (0) if and only if M is the trivial R-module (0).

EXERCISE 3.3.18. Let k be a field and A a finite-dimensional k-algebra. Prove that the following are equivalent.

1. A is a division ring.
2. A has no zero divisors.

4. The Determinant

4.1. Alternating Multilinear Forms. Throughout this section, R is a commutative ring. Let $J = \{1, \dots, n\}$ and $J^n = J \times \cdots \times J$ (n times). We view the symmetric group S_n as the subset of J^n consisting of n-tuples $\vec{j} = (j_1, \dots, j_n)$ that are permutations of J. The sign of a permutation $\sigma \in S_n$ is denoted $\operatorname{sign}(\sigma)$.

DEFINITION 3.4.1. Let R be a commutative ring, $n \geq 1$, and $(R^n)^n = \bigoplus_{i=1}^n R^n$. Consider a function $f : (R^n)^n \to R$. We say that f is a *multilinear form* if for each i,

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

We say that f is an *alternating form* if $f(x_1, , \dots, x_n) = 0$ whenever $x_i = x_j$ for some pair $i \neq j$.

LEMMA 3.4.2. *If $f : (R^n)^n \to R$ is an alternating multilinear form and $\sigma \in S_n$ is a permutation on the set $\{1, \dots, n\}$, then*

$$f(x_{\sigma 1}, \dots, x_{\sigma n}) = \operatorname{sign}(\sigma) f(x_1, , \dots, x_n).$$

We say that f is skew symmetric.

PROOF. Because σ factors into a product of transpositions, it is enough to show that acting on the variables by a transposition changes the sign of f. For simplicity's sake, assume $\sigma = (i,j) = (1,2)$. Look at

$$\begin{aligned}0 &= f(x_1+x_2,x_1+x_2,x_3,\dots,x_n)\\ &= f(x_1,x_1,x_3,\dots,x_n)+f(x_1,x_2,x_3,\dots,x_n)+\\ &\quad f(x_2,x_1,x_3,\dots,x_n)+f(x_2,x_2,x_3,\dots,x_n)\\ &= f(x_1,x_2,x_3,\dots,x_n)+f(x_2,x_1,x_3,\dots,x_n).\end{aligned}$$

This shows $f(x_1,x_2,x_3,\dots,x_n) = -f(x_2,x_1,x_3,\dots,x_n)$. □

LEMMA 3.4.3. *If R is a commutative ring and $r \in R$, there is a unique alternating multilinear form $f : (R^n)^n \to R$ such that $f(e_1,\dots,e_n) = r$, where $(e_1,\dots,e_n)$ is the standard basis for R^n.*

PROOF. (Uniqueness) Given $(x_1,\dots,x_n) \in (R^n)^n$, for each i we can write $x_i = a_{1i}e_1 + \cdots + a_{ni}e_n$. Since f is multilinear,

$$\begin{aligned}f(x_1,\dots,x_n) &= f\left(\sum_{j\in J} a_{j1}e_j,\dots,\sum_{j\in J} a_{jn}e_j\right)\\ &= \sum_{j_1\in J}\left(a_{j_1 1} f\left(e_{j_1},\sum_{j\in J} a_{j2}e_j,\dots,\sum_{j\in J} a_{jn}e_j\right)\right)\\ &= \sum_{j_1\in J}\sum_{j_2\in J}\left(a_{j_1 1}a_{j_2 2} f\left(e_{j_1},e_{j_2},\dots,\sum_{j\in J} a_{jn}e_j\right)\right)\\ &\vdots\\ &= \sum_{(j_1,\dots,j_n)\in J^n} a_{j_1 1}\cdots a_{j_n n} f\left(e_{j_1},\dots,e_{j_n}\right).\end{aligned}$$

Since f is alternating, if $\vec{j} = (j_1,\dots,j_n) \in J^n$ is not a permutation, then $f(e_{j_1},\dots,e_{j_n}) = 0$. We can restrict the latest summation to $\vec{j} \in S_n$. In this case, since f is skew symmetric, $f(e_{j_1},\dots,e_{j_n}) = \operatorname{sign}(j) f(e_1,\dots,e_n) = \operatorname{sign}(j)r$. This proves that

$$f(x_1,\dots,x_n) = r\sum_{\vec{j}\in S_n} \operatorname{sign}(\vec{j})a_{j_1 1}\cdots a_{j_n n} \tag{3.7}$$

is completely determined by r and $(x_1,\dots,x_n)$.

(Existence) The formula in (3.7) defines a function $f : (R^n)^n \to R$. Notice that

$$f(e_1,\dots,e_n) = r$$

since only for $\vec{j} = (1,2,\dots,n)$ is the product formula in the summation (3.7) nonzero. We need to prove f is an alternating multilinear form. Let $\alpha,\beta \in R$, $u,v \in R^n$. Write $u = \sum u_i e_i$

and $v = \sum v_i e_i$. Set $a_{ik} = \alpha u_i + \beta v_i$, so that $x_k = \sum a_{ik} e_i = \sum(\alpha u_i + \beta v_i)e_i = \alpha u + \beta v$. Then

$$\begin{aligned}
f(x_1,\dots,\alpha u+\beta v,\dots,x_n) &= r \sum_{\vec{j}\in S_n} \operatorname{sign}(j) a_{j_1 1}\cdots a_{j_k k}\cdots a_{j_n n} \\
&= r \sum_{\vec{j}\in S_n} \operatorname{sign}(j) a_{j_1 1}\cdots (\alpha u_{j_k} + \beta v_{j_k})\cdots a_{j_n n} \\
&= r\alpha \sum_{\vec{j}\in S_n} \operatorname{sign}(j) a_{j_1 1}\cdots u_{j_k}\cdots a_{j_n n} + \\
&\qquad r\beta \sum_{\vec{j}\in S_n} \operatorname{sign}(j) a_{j_1 1}\cdots v_{j_k}\cdots a_{j_n n} \\
&= \alpha f(x_1,\dots,u,\dots,x_n) + \beta f(x_1,\dots,v,\dots,x_n)
\end{aligned}$$

shows f is multilinear.

Now we show f is alternating. Suppose $i < j$ and let τ be the transposition that switches i and j. The alternating group A_n has index 2 in S_n, so every odd permutation is of the form $\sigma\tau$ for some $\sigma \in A_n$. Assume $x_i = x_j$ and show $f(x_1,\dots,x_n) = 0$. For all k we have $a_{ki} = a_{kj}$. Also, if $\sigma \in A_n$ then $\sigma\tau(i) = \sigma(j)$ and $\sigma\tau(j) = \sigma(i)$.

$$\begin{aligned}
f(x_1,\dots,x_n) &= r \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n} \\
&= r \sum_{\sigma\in A_n} \left(a_{\sigma(1)1}\cdots a_{\sigma(n)n} - a_{\sigma\tau(1)1}\cdots a_{\sigma\tau(n)n}\right) \\
&= r \sum_{\sigma\in A_n} \left(a_{\sigma(1)1}\cdots a_{\sigma(n)n} - a_{\sigma\tau(1)1}\cdots a_{\sigma\tau(i)i}\cdots a_{\sigma\tau(j)j}\cdots a_{\sigma\tau(n)n}\right) \\
&= r \sum_{\sigma\in A_n} \left(a_{\sigma(1)1}\cdots a_{\sigma(n)n} - a_{\sigma(1)1}\cdots a_{\sigma(j)i}\cdots a_{\sigma(i)j}\cdots a_{\sigma(n)n}\right) \\
&= r \sum_{\sigma\in A_n} \left(a_{\sigma(1)1}\cdots a_{\sigma(n)n} - a_{\sigma(1)1}\cdots a_{\sigma(j)j}\cdots a_{\sigma(i)i}\cdots a_{\sigma(n)n}\right) \\
&= 0.
\end{aligned}$$

□

DEFINITION 3.4.4. By viewing the columns of a matrix in $M_n(R)$ as vectors in R^n, we identify $M_n(R)$ with $(R^n)^n$. The *determinant* is the unique alternating multilinear form $\det : M_n(R) \to R$ such that $\det(I_n) = 1$. By Lemma 3.4.3,

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

LEMMA 3.4.5. *Let $A, B \in M_n(R)$.*

(1) $\det(AB) = \det(A)\det(B)$.
(2) A is invertible if and only if $\det(A)$ *is a unit in R.*
(3) If A and B are similar, then $\det(A) = \det(B)$.
(4) $\det(A) = \det(A^T)$.
(5) The determinant is an alternating multilinear form on the rows of matrices in $M_n(R)$.

PROOF. (1): Fix A. Taking $r = \det(A)$ in (3.7) defines an alternating multilinear form $g : M_n(R) \to R$, where $g(C) = \det(A)\det(C)$. Define another function $f : M_n(R) \to R$ by $f(C) = \det(AC)$. Since $f(I_n) = \det(A)$, by Lemma 3.4.3, it is enough to prove that f is alternating and multilinear. Assume $u, v \in R^n$ and $C = (x_1, \dots, x_n) \in M_n(R)$. Then

$$\begin{aligned} f(c_1, \dots, \alpha u + \beta v, \dots, c_n) &= \det(A(c_1, \dots, \alpha u + \beta v, \dots, c_n)) \\ &= \det(Ac_1, \dots, \alpha Au + \beta Av, \dots, Ac_n) \\ &= \alpha \det(Ac_1, \dots, Au, \dots, Ac_n) + \beta \det(Ac_1, \dots, Av, \dots, Ac_n) \\ &= \alpha f(c_1, \dots, u, \dots, c_n) + \beta f(c_1, \dots, v, \dots, c_n) \end{aligned}$$

If two columns of C are equal, then two columns of AC are equal, so f is alternating.

(2): If $AB = I_n$, then $\det(A)\det(B) = 1$. The converse follows from Lemma 3.4.9 because in this case $A^{-1} = \det(A)^{-1}A^a$.

(3): If $A = X^{-1}BX$, then

$$\begin{aligned} \det(A) &= \det(X^{-1})\det(B)\det(X) \\ &= \det(B)\det(X^{-1})\det(X) \\ &= \det(B)\det(X^{-1}X) \\ &= \det(B). \end{aligned}$$

(4): Since R is commutative, for every $\sigma \in S_n$ we have

$$a_{\sigma(1),1} \cdots a_{\sigma(n),n} = a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)}.$$

This together with the fact that $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma^{-1})$ lead to

$$\begin{aligned} \det(A) &= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n} \\ &= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} \\ &= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \\ &= \det(A^T). \end{aligned}$$

(5): Follows from (4). □

DEFINITION 3.4.6. 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 3.4.7. *For A in $M_n(R)$,*

(1) For each row i, $\det(A) = \sum_{j=1}^n a_{ij}(-1)^{i+j}\det(A_{ij})$, and

(2) For each column j, $\det(A) = \sum_{i=1}^n a_{ij}(-1)^{i+j}\det(A_{ij})$.

PROOF. We prove that the determinant can be computed by cofactor expansion of row i. The statement about column expansion follows from Lemma 3.4.5 (4). Define a function $f : M_n(R) \to R$ by the formula $f(A) = \sum_{j=1}^n a_{ij}(-1)^{i+j}\det(A_{ij})$. The reader should verify that $f(I_n) = 1$. By Lemma 3.4.3 it is enough to show that f is alternating and multilinear.

Assume the columns of A are $(A_1, \dots, A_n)$ and assume $A_k = A_\ell$ and $k < \ell$. Therefore $a_{ik} = a_{i\ell}$. If $j \neq k$ and $j \neq \ell$, then A_{ij} has two columns that are equal, so $\det(A_{ij}) = 0$. The formula for f reduces to

$$\begin{aligned} f(A) &= a_{ik}(-1)^{i+k}\det(A_{ik}) + a_{i\ell}(-1)^{i+\ell}\det(A_{i\ell}) \\ &= a_{ik}(-1)^{i+k}\det(A_{ik}) + a_{ik}(-1)^{i+\ell}\det(A_{i\ell}) \\ &= a_{ik}\left((-1)^{i+k}\det(A_{ik}) + (-1)^{i+\ell}\det(A_{i\ell})\right). \end{aligned}$$

But A_{ik} is obtained from $A_{i\ell}$ by permuting the columns. In fact, $\ell-k-1$ transpositions are sufficient. Since the determinant form is skew symmetric, $\det(A_{ik}) = (-1)^{\ell-k-1}\det(A_{i\ell})$. The reader should verify that $(-1)^{i+k}+(-1)^{i+\ell}(-1)^{\ell-k-1} = 0$, hence

$$\begin{aligned} f(A) &= a_{ik}\Big((-1)^{i+k}\det(A_{ik}) + (-1)^{i+\ell}\det(A_{i\ell})\Big) \\ &= a_{ik}\Big((-1)^{i+k}\det(A_{ik}) + (-1)^{i+\ell}(-1)^{\ell-k-1}\det(A_{ik})\Big) \\ &= a_{ik}\det(A_{ik})\Big((-1)^{i+k} + (-1)^{i+\ell}(-1)^{\ell-k-1}\Big) \\ &= 0 \end{aligned}$$

which proves f is alternating.

Assume the columns of A are $(A_1,\dots,A_n)$ where $A_k = \alpha u + \beta v$ for some $u,v \in R^n$. Let $B = (b_{ij})$ be the matrix obtained by replacing column k of A with the vector u. Let $C = (c_{ij})$ be the matrix obtained by replacing column k of A with the vector v. We show that $f(A) = \alpha f(B) + \beta f(C)$. Because they differ only in column k, we have $A_{ik} = B_{ik} = C_{ik}$. If $j \neq k$, then the determinant is multilinear, so $\det(A_{ij}) = \alpha\det(B_{ij}) + \beta\det(C_{ij})$. Therefore

$$\begin{aligned} f(A) &= \sum_{j=1}^{n} a_{ij}(-1)^{i+j}\det(A_{ij}) \\ &= \sum_{j\neq k} a_{ij}(-1)^{i+j}\left(\alpha\det(B_{ij}) + \beta\det(C_{ij})\right) + (\alpha b_{ik} + \beta c_{ik})(-1)^{i+k}\det(A_{ik}) \\ &= \alpha\sum_{j=1}^{n} b_{ij}(-1)^{i+j}\det(B_{ij}) + \beta\sum_{j=1}^{n} c_{ij}(-1)^{i+j}\det(C_{ij}) \\ &= \alpha f(B) + \beta f(C) \end{aligned}$$

□

DEFINITION 3.4.8. Let $A \in M_n(R)$. The *adjoint* of A, denoted A^a, is the transpose of the matrix of cofactors of A. Therefore, $A^a = \big((-1)^{i+j}\det(A_{ji})\big)$.

LEMMA 3.4.9. $A^aA = AA^a = \det(A)I_n$.

PROOF. Assume $i \neq j$. Let B be the matrix which is equal to A with column i replaced with a copy of column j. Compute $\det(B) = 0$ by column expansion down column i. Use the facts that $B_{ki} = A_{ki}$ and $b_{ki} = b_{kj} = a_{kj}$ for each k.

$$\begin{aligned} 0 &= \sum_{k=1}^{n} b_{ki}(-1)^{i+k}\det(B_{ki}) \\ &= \sum_{k=1}^{n} a_{kj}(-1)^{i+k}\det(A_{ki}) \end{aligned}$$

Let $A^aA = (c_{ij})$. Then

$$c_{ij} = \sum_{k=1}^{n}(-1)^{i+k}\det(A_{ki})a_{kj} = \begin{cases} \det(A) & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

□

The determinant is constant on similarity classes, by Lemma 3.4.5. If M is a finitely generated free R-module and $\phi \in \operatorname{Hom}_R(M,M)$, then the determinant of ϕ is defined to be the determinant of the matrix of ϕ with respect to any basis of M. If A is an R-algebra which is free of finite rank and $\alpha \in A$, then we have the left regular representation $\theta : A \rightarrow$

$\operatorname{Hom}_R(A,A)$ of A as a ring of R-module homomorphisms of A. Under θ, the element $\alpha \in A$ is mapped to ℓ_α, which is "left multiplication by α". The determinant of α is defined to be the determinant of ℓ_α.

4.2. The Characteristic Polynomial.

EXAMPLE 3.4.10. Let R be a commutative ring. 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.

DEFINITION 3.4.11. 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 (Lemma 3.4.7) 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, by Exercise 3.4.2. 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 $\theta : A \to \operatorname{Hom}_R(A,A)$ of A as a ring of R-module homomorphisms of A. Under θ, the element $\alpha \in A$ is mapped to ℓ_α, which is "left multiplication by α". The characteristic polynomial of α is defined to be the characteristic polynomial of ℓ_α.

THEOREM 3.4.12. *(Cayley-Hamilton Theorem) Let R be a commutative ring, M an n-by-n matrix over R, and $p(x) = \operatorname{char.poly}_R(M)$ the characteristic polynomial of M. Then $p(M) = 0$.*

PROOF. In the polynomial ring $M_n(R)[x]$, apply Corollary 2.5.4 to $p(x)$ and M. There is a unique $q(x) \in M_n(R)[x]$ such that $p(x) = q(x)(x - M) + p(M)$. Lemma 3.4.9 implies that $p(x)I_n = \det(xI_n - M)I_n = (xI_n - M)^a(xI_n - M)$ is a factorization of $p(x)$ in $M_n(R[x])$. As in Example 3.4.10, we identify the $R[x]$-algebras $M_n(R)[x]$ and $M_n(R[x])$. By the uniqueness part of The Division Algorithm 2.5.3, we conclude that $p(M) = 0$ and $q(x) = (xI_n - M)^a$. □

THEOREM 3.4.13. *Let k be a field and V a finite dimensional vector space over k. Let $\phi \in \operatorname{Hom}_k(V,V)$. As in Theorem 3.3.28, let $q_1, q_2, \dots, q_r$ be the invariant factors of ϕ.*

(1) $\operatorname{char.poly}_k(\phi) = q_1 q_2 \cdots q_r$.
(2) *(Cayley-Hamilton) If $p(x) = \operatorname{char.poly}_k(\phi)$, then $p(\phi) = 0$. In other words,* $\operatorname{min.poly}_k(\phi) \mid \operatorname{char.poly}_k(\phi)$.
(3) *If $f \in k[x]$ is irreducible, then $f \mid \operatorname{char.poly}_k(\phi)$ if and only if $f \mid \operatorname{min.poly}_k(\phi)$. The roots of* $\operatorname{min.poly}_k(\phi)$ *are precisely the roots of* $\operatorname{char.poly}_k(\phi)$.

PROOF. (1): By Corollary 3.3.29 there is a basis for V such that the matrix of ϕ is the block diagonal matrix $(C(q_1), C(q_2), \dots, C(q_r))$, where $C(q_i)$ is the companion matrix for

q_i. By Exercise 3.4.1, the characteristic polynomial of $C(q_i)$ is q_i. Apply Exercise 3.4.3 iteratively to show that $\operatorname{char.poly}_k(\phi) = q_1 q_2 \cdots q_r$.

(2): By Theorem 3.3.28, $\operatorname{min.poly}_k(\phi) = q_r$.

(3): By Theorem 3.3.28, $q_1 \mid q_2 \mid \cdots \mid q_r$. The irreducible factors of $\operatorname{char.poly}_k(\phi)$ are equal to the irreducible factors of $\operatorname{min.poly}_k(\phi)$. □

DEFINITION 3.4.14. Let k be a field, V a finite dimensional vector space over k and $\phi \in \operatorname{Hom}_k(V,V)$. We call $\lambda \in k$ an *eigenvalue* of ϕ if there exists a nonzero $v \in V$ satisfying $\phi(v) = \lambda v$. In this case we say v is an *eigenvector* corresponding to λ. The set $U(\lambda) = \{x \in V \mid \phi(x) = \lambda x\}$ is called the *eigenspace* of λ. The reader should verify that $U(\lambda)$ is a ϕ-invariant subspace of V.

THEOREM 3.4.15. *Let k be a field, V a finite dimensional vector space over k and $\phi \in \operatorname{Hom}_k(V,V)$.*

1. *The eigenvalues of ϕ are precisely the roots of the minimal polynomial of ϕ.*
2. *The following are equivalent.*
   (a) *There is a basis B for V such that $M(\phi, B)$ is diagonal.*
   (b) *There is a basis of V consisting of eigenvectors of ϕ.*
   (c) *The minimal polynomial* $\operatorname{min.poly}_k(\phi)$ *factors into a product of linear factors in $k[x]$ and has no multiple roots.*

PROOF. (1): Let $\lambda \in k$. Then λ is an eigenvalue of ϕ if and only if there exists a nonzero $v \in V$ such that $(\phi - \lambda I)(v) = 0$, which is true if and only if $\phi - \lambda I$ is not invertible, which is true if and only if $\det(\phi - \lambda I) = 0$, which is true if and only if λ is a root of $\operatorname{char.poly}_k(\phi)$.

(2): (a) is clearly equivalent to (b).

(a) is equivalent to (c): This follows from Corollary 3.3.31. The Jordan blocks are one-by-one if and only if the exponents e_{ij} are equal to 1, if and only if the matrix is diagonal. □

4.3. Exercises.

EXERCISE 3.4.1. Suppose k is a field and

$$M = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & 0 & -a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & 0 & \dots & 0 & 0 & -a_{n-3} \\ 0 & 0 & 0 & \dots & 1 & 0 & -a_{n-2} \\ 0 & 0 & 0 & \dots & 0 & 1 & -a_{n-1} \end{bmatrix}$$

is a matrix in $M_n(k)$.

1. Prove that $\operatorname{min.poly}_k(M) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.
2. Prove that $\operatorname{char.poly}_k(M) = \operatorname{min.poly}_k(M)$.
3. Prove that the rank of M is equal to the rank of the transpose of M.

EXERCISE 3.4.2. Let R be a commutative ring and A and B similar matrices in $M_n(R)$. Prove that $\operatorname{char.poly}_R(A) = \operatorname{char.poly}_R(B)$.

EXERCISE 3.4.3. Let R be a commutative ring, $A \in M_m(R)$, $B \in M_n(R)$. Define the *direct sum of A and B* by

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

which is a matrix in $M_{m+n}(R)$. The direct sum $A \oplus B$ is sometimes called a *block diagonal matrix* and is denoted $\operatorname{diag}(A,B)$. Prove:

(1) $\det(A \oplus B) = \det(A)\det(B)$.
(2) $\operatorname{char.poly}_R(A \oplus B) = \operatorname{char.poly}_R(A)\operatorname{char.poly}_R(B)$.
(3) $\operatorname{Rank}(A \oplus B) = \operatorname{Rank}(A) + \operatorname{Rank}(B)$.

EXERCISE 3.4.4. Let R be a commutative ring and $n \geq 1$. Define the *trace* of a matrix $\alpha = (\alpha_{ij}) \in M_n(R)$ by $\operatorname{trace}(\alpha) = \sum_{i=1}^n \alpha_{ii}$.

(1) Prove that the trace mapping is an R-module homomorphism from $M_n(R)$ to R.
(2) Prove that $\operatorname{trace}(\alpha\beta) = \operatorname{trace}(\beta\alpha)$. (Hint: First show $\operatorname{trace}(\alpha e_{ij}) = \operatorname{trace}(e_{ij}\alpha)$ if e_{ij} is an elementary matrix and α is arbitrary.)
(3) Prove that if α and β are similar, then $\operatorname{trace}(\alpha) = \operatorname{trace}(\beta)$.

EXERCISE 3.4.5. Let R be a commutative ring, M a finitely generated free R-module, and X a basis for M over R. Define the trace of $\phi \in \operatorname{Hom}_R(M,M)$ to be $\operatorname{trace}(\phi) = \operatorname{trace}(M(\phi,X))$. Show that this definition is independent of the choice for X. Show that the trace mapping is an R-module homomorphism from $\operatorname{Hom}_R(M,M)$ to R.

EXERCISE 3.4.6. 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 3.4.7. Let k be a field, $n \geq 1$, $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$ and $M = C(f)$ the companion matrix of f. Prove the following.

(1) $\det(M) = (-1)^n a_0$.
(2) $\operatorname{trace}(M) = -a_{n-1}$.

EXERCISE 3.4.8. 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 3.4.9. Let k be a field, V a finitely generated vector space over k, and $\phi \in \operatorname{Hom}_k(V,V)$. Suppose $q = \operatorname{min.poly}_k(\phi) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ is irreducible in $k[x]$. Prove the following.

(1) $\operatorname{char.poly}_k(\phi) = q^r$ for some integer r.
(2) $\det(\phi) = (-1)^{mr} a_0^r$.
(3) $\operatorname{trace}(\phi) = -ra_{m-1}$.

EXERCISE 3.4.10. Let k be a field and A a matrix in $M_n(k)$ such that $\operatorname{Rank}(A) = r < n$. Prove:

(1) $\det(A) = 0$.
(2) If B is an $r+1$-by-$r+1$ submatrix of A, then $\det(B) = 0$.

(3) A contains an r-by-r submatrix of rank r.

EXERCISE 3.4.11. (Cramer's Rule) Let R be a commutative ring. Suppose $A \in M_n(R)$, $x, b \in R^n$ such that $Ax = b$. Prove that $x_i \det(A) = \det(B_i)$, where $B_i = (a_1, \dots, b, \dots, a_n)$ is the matrix obtained by replacing column i of A with the column vector b. (Hint: If $A = (a_1, \dots, a_n)$ is written in columnar form, then $b = x_1 a_1 + \cdots + x_n a_n$. Use the multilinear and alternating properties when computing $\det(B_i)$.)

EXERCISE 3.4.12. Let k be a field and f an irreducible polynomial with coefficients in k. Show that if M is an n-by-n matrix over k such that $f(M) = 0$, then $\deg(f) \le n$.

EXERCISE 3.4.13. Let $\theta : R \to S$ be a homomorphism of commutative rings.

(1) Show that θ induces a homomorphism of rings $\theta : M_n(R) \to M_n(S)$.
(2) Show that $\theta(\det(M)) = \det(\theta(M))$, for every M in $M_n(R)$.
(3) We know from Theorem 2.5.2 that θ induces a homomorphism of rings $R[x] \to S[x]$. Show that $\theta(\operatorname{char.poly}_R(M)) = \operatorname{char.poly}_S(\theta(M))$.

EXERCISE 3.4.14. Let R be a commutative ring and $n \ge 1$. If $A \in M_n(R)$, show that the trace of A (see Exercise 3.4.4) satisfies:

$$\sum_{i=1}^{n} \sum_{j=1}^{n} e_{ij} A e_{ji} = \operatorname{trace}(A) I_n$$

where e_{ij} denotes the elementary matrix (Definition 3.3.6) and $I_n = e_{11} + \cdots + e_{nn}$ the identity matrix.

EXERCISE 3.4.15. Let R be a commutative ring and $A = M_n(R)$ the ring of n-by-n matrices over R. The so-called *trace pairing* $\tau : A \times A \to R$ is defined by $\tau(\alpha, \beta) = \operatorname{trace}(\alpha\beta)$, where the trace map is defined in Exercise 3.4.4. Show that τ satisfies these properties:

(1) $\tau(\alpha, \beta) = \tau(\beta, \alpha)$.
(2) $\tau(a_1\alpha_1 + a_2\alpha_2, \beta) = a_1\tau(\alpha_1, \beta) + a_2\tau(\alpha_2, \beta)$ for $a_1, a_2 \in R$.
(3) $\tau(\alpha, b_1\beta_1 + b_2\beta_2) = b_1\tau(\alpha, \beta_1) + b_2\tau(\alpha, \beta_2)$ for $b_1, b_2 \in R$.
(4) If $\alpha \ne 0$ is fixed, then $\tau(\alpha, \ ) : A \to R$ is nonzero. That is, there exists β such that $\tau(\alpha, \beta) \ne 0$.

We say that τ is a *symmetric nondegenerate bilinear form*.

5. Polynomial Functions

5.1. The Ring of Polynomial Functions on a Module. Let R be a commutative ring, M an R-module, and $M^* = \operatorname{Hom}_R(M, R)$ the dual of M. By $\operatorname{Map}(M, R)$ we denote the set of all functions $f : M \to R$. Then $\operatorname{Map}(M, R)$ can be turned into an R-algebra. The addition and multiplication operations are defined pointwise: $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$. An element a in R defines the constant function $a : M \to R$, where $a(x) = a$. We can view M^* as an R-submodule of $\operatorname{Map}(M, R)$. The R-subalgebra of $\operatorname{Map}(M, R)$ generated by the set M^* is denoted $R[M^*]$ and is called the *ring of polynomial functions* on M. If $d \ge 0$, then a polynomial function $f \in R[M^*]$ is said to be *homogeneous of degree d*, if $f(rx) = r^d f(x)$, for all $x \in M$ and $r \in R$. Proposition 3.5.1 shows that the ring $R[M^*]$ is in fact a coordinate-free way to generalize the usual ring of polynomial functions on a vector space.

PROPOSITION 3.5.1. *Let k be an infinite field, and V a finite dimensional k-vector space. If $\dim_k(V) = n$, then $k[V^*] \cong k[x_1, \dots, x_n]$ as k-algebras.*

PROOF. Let $\{(v_i, f_i) \mid 1 \le i \le n\}$ be a dual basis for V. As a k-vector space, $f_1, \dots, f_n$ is a basis for V^*. Define $\theta : k[x_1, \dots, x_n] \to k[V^*]$ by $x_i \mapsto f_i$. The reader should verify that θ is onto, and by Exercise 2.5.14 is one-to-one. □

LEMMA 3.5.2. *Let R be a commutative ring and P a free R-module with* $\operatorname{Rank}_R(P) = n$. *Let $\phi \in \operatorname{Hom}_R(P,P)$. If the characteristic polynomial of ϕ is $p(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, then for each $i = 1, \dots, n$, the assignment $\phi \mapsto (-1)^i a_i$ defines a polynomial function $N_i : \operatorname{Hom}_R(P,P) \to R$ which is homogeneous of degree i.*

PROOF. Fix a basis B for P. Let $\phi \in \operatorname{Hom}_R(P,P)$, and $(\phi_{ij}) = M(\phi, B)$ the matrix of ϕ. By Proposition 3.5.1, a polynomial function on $\operatorname{Hom}_R(P,P)$ corresponds to a polynomial in the n^2 indeterminates $\Phi = \{\phi_{ij} \mid 1 \le i \le n,\ 1 \le j \le n\}$. The characteristic polynomial of ϕ is given by the combinatorial formula for the determinant (Definition 3.4.4)

$$\det(xI_n - (\phi_{ij})) = \sum_{\vec{\ell} \in S_n} \operatorname{sign}(\ell) b_{\ell_1,1} \cdots b_{\ell_n,n} \tag{3.8}$$

where $b_{ii} = x - \phi_{ii}$ and $b_{ij} = -\phi_{ij}$ if $i \neq j$. A typical summand in (3.8) can be written in the form

$$\operatorname{sign}(\ell) b_{\ell_1,1} \cdots b_{\ell_n,n} = (x - a_{i_1 i_1}) \cdots (x - a_{i_d i_d}) m$$

where m is a monomial in $k[\Phi]$ of degree $n - d$. Therefore, $b_{\ell_1,1} \cdots b_{\ell_n,n}$ is a polynomial in x of degree d and for $0 \le k < n$, the coefficient of x^k is a homogeneous polynomial of degree $n - k$ in $k[\Phi]$. □

EXAMPLE 3.5.3. 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 $\operatorname{Hom}_k(A,A)$. As in Lemma 3.5.2, let $N_i : \operatorname{Hom}_k(A,A) \to k$ be the homogeneous polynomial function of degree i defined by the coefficient of x^{n-i} in the characteristic polynomial of ϕ. For each i, upon restriction to A, $N_i : A \to k$ defines a homogeneous polynomial function on A of degree i. In particular N_n is the norm $N^A_k : A \to k$ defined in Exercise 3.4.6, and N_1 the trace $T^A_k : A \to k$. Fix a k-basis $\alpha_1, \dots, \alpha_n$ for A. Then this basis can be extended to a basis for $\operatorname{Hom}_k(A,A)$ and N_i can be identified with a homogeneous polynomial in $k[x_1, \dots, x_n]$ of degree i.

5.2. Resultant of Two Polynomials. Assume $m \ge 0$, $n \ge 0$, and $m + n \ge 1$. Let $f = \sum_{i=0}^m f_i x^i$ and $g = \sum_{i=0}^n g_i x^i$ be two polynomials in $k[x]$, where k is a field. So the degree of f is at most m, and the degree of g is at most n. In the general case, m and n are both positive, and the *Sylvester matrix* of f and g is the $(m+n)$-by-$(m+n)$ matrix

$$\operatorname{Syl}(f,g) = \left[\begin{array}{cccccccccc}
f_m & f_{m-1} & f_{m-2} & \cdots & f_0 & & & & \cdots & \\
 & f_m & f_{m-1} & \cdots & f_1 & f_0 & & & \cdots & \\
 & & f_m & \cdots & f_2 & f_1 & f_0 & & \cdots & \\
 & & & \vdots & & & & & & \\
 & \cdots & & f_m & f_{m-1} & f_{m-2} & \cdots & f_0 & & \\
 & \cdots & & & f_m & f_{m-1} & \cdots & f_1 & f_0 & \\
 & \cdots & & & & f_m & \cdots & f_2 & f_1 & f_0 \\
g_n & g_{n-1} & g_{n-2} & \cdots & g_0 & & & & \cdots & \\
 & g_n & g_{n-1} & \cdots & g_1 & g_0 & & & \cdots & \\
 & & g_n & \cdots & g_2 & g_1 & g_0 & & \cdots & \\
 & & & \vdots & & & & & & \\
 & \cdots & & g_n & g_{n-1} & f_{m-2} & \cdots & g_0 & & \\
 & \cdots & & & g_n & g_{n-1} & \cdots & g_1 & g_0 & \\
 & \cdots & & & & g_n & \cdots & g_2 & g_1 & g_0
\end{array}\right]$$

where blank spaces consist of zeros. The top n rows are constructed from the coefficients of f, shifted and padded with zeros. The bottom m rows are constructed from shifting the coefficients of g, and padding with zeros. In the degenerate case when $m=0$, $\operatorname{Syl}(f,g)$ is defined to be the n-by-n diagonal matrix $f_0(E_{11}+\cdots+E_{nn})$. In the degenerate case when $n=0$, $\operatorname{Syl}(f,g)$ is defined to be the m-by-m diagonal matrix $g_0(E_{11}+\cdots+E_{mm})$. The *resultant* of f and g, written $\operatorname{Res}(f,g)$, is the determinant of $\operatorname{Syl}(f,g)$.

LEMMA 3.5.4. *In the above context, we view $f_0,\dots,f_m$, $g_0,\dots,g_n$ as variables. Then in the terminology of Section 3.5.1, $\operatorname{Res}(f,g)$ satisfies the following:*

(1) $\operatorname{Res}(f,g)$ is a polynomial in $\mathbb{Z}[f_0,\dots,f_m,g_0,\dots,g_n]$ which is homogeneous of degree $n+m$.

(2) For any constant $c\in\mathbb{Z}$,

$$\operatorname{Res}(cf,g) = c^n \operatorname{Res}(f,g)$$
$$\operatorname{Res}(f,cg) = c^m \operatorname{Res}(f,g)$$

Thus, $\operatorname{Res}(f,g)$ is homogeneous of degree n in $f_0,\dots,f_m$ and homogeneous of degree m in $g_0,\dots,g_n$.

PROOF. Is left to the reader. □

LEMMA 3.5.5. *In the above context, the following are true.*

(1) If $\deg(f)<m$ and $\deg(g)<n$, then $\operatorname{Res}(f,g)=0$.

(2) If $m=0$, then $\operatorname{Res}(f,g)=f_0^n$.

(3) If $n=0$, then $\operatorname{Res}(f,g)=g_0^m$.

(4) $\operatorname{Res}(f,g)=(-1)^{mn}\operatorname{Res}(g,f)$.

(5) If $\deg(f)=m$ and $d=\deg(g)<n$, then $\operatorname{Res}(f,g)=f_m^{n-d}\operatorname{Res}(f,h)$, where $h=g_dx^d+\cdots+g_1x+g_0$.

PROOF. (1) – (4): Are left to the reader.

(5): The Sylvester matrix has the form

$$\operatorname{Syl}(f,g) = \begin{bmatrix} T & * \\ 0 & \operatorname{Syl}(f,h) \end{bmatrix}$$

where T is an upper triangular matrix of size $(n-d)$-by-$(n-d)$ with diagonal $(f_m,\dots,f_m)$. $\square$

LEMMA 3.5.6. *In the context of Lemma 3.5.5, assume $m \le n$ and $\deg(f) = m$. Let q and r be the unique polynomials in $k[x]$ guaranteed by The Division Algorithm (Theorem 2.5.3) which satisfy: $q = \sum_{i=0}^{n-m} q_i x^i$, $r = \sum_{i=0}^{m-1} r_i x^i$, and $g = qf + r$. Then $\operatorname{Res}(f,g) = f_m^{n-m+1}\operatorname{Res}(f,r)$.*

PROOF. Write $c = -q_{n-m} = -g_n/f_m$, and set $h = g + cx^{n-m} f = \sum_{i=0}^{n-1} h_i x^i$. Let $I_m = E_{11} + \cdots + E_{mm} \in M_m(k)$, $I_n = E_{11} + \cdots + E_{nn} \in M_n(k)$, and $I_{mn} = E_{11} + \cdots + E_{mm} \in M_{mn}(k)$. The product

$$\begin{bmatrix} I_n & 0 \\ cI_{mn} & I_m \end{bmatrix} \operatorname{Syl}(f,g) = \begin{bmatrix} f_m & * \\ & \operatorname{Syl}(f,h) \end{bmatrix}$$

corresponds to elementary row operations. The determinant formulas in Lemma 3.4.5 and Lemma 3.4.7 imply that $\operatorname{Res}(f,g) = f_m \operatorname{Res}(f,h)$. By induction on $n-m$, we are done. $\square$

THEOREM 3.5.7. *In the context of Lemma 3.5.5, assume F/k is an extension of fields such that in the unique factorization domain $F[x]$ both polynomials f and g have no irreducible factor of degree greater than one.*

(1) If $m = \deg(f) \ge 1$ and $f = f_m(x-\alpha_1)\cdots(x-\alpha_m)$ is a factorization of f into a product of linear polynomials, then

$$\operatorname{Res}(f,g) = f_m^n \prod_{i=1}^{m} g(\alpha_i).$$

(2) If $\deg(g) = n \ge 1$ and $g = g_n(x-\beta_1)\cdots(x-\beta_n)$ is a factorization of g into a product of linear polynomials, then

$$\operatorname{Res}(f,g) = (-1)^{mn} g_n^m \prod_{j=1}^{n} f(\beta_j).$$

(3) Suppose $\deg(f) = m \ge 1$ and $\deg(g) = n \ge 1$. If $f = f_m(x-\alpha_1)\cdots(x-\alpha_m)$ and $g = g_n(x-\beta_1)\cdots(x-\beta_n)$ are factorizations of f and g into products of linear polynomials, then

$$\operatorname{Res}(f,g) = f_m^n g_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

PROOF. We prove (1) and (2) simultaneously. The reader should verify that Part (3) follows from Parts (1) and (2).

The proof is by induction on $m+n$. The basis for the induction, which follows from Lemma 3.5.5, is when $n = 0$ or $m = 0$. Assume from now on that $1 \le m$ and $1 \le n$.

Case 1: $\deg(f) = m \ge 1$, and $\deg(g) = d < n$. If we set $h = \sum_{i=0}^{d} g_i x^i$, then by Lemma 3.5.5 (5), $\operatorname{Res}(f,g) = f_m^{n-d}\operatorname{Res}(f,g)$. By the induction hypothesis, $\operatorname{Res}(f,g) = f_m^{n-d}\operatorname{Res}(f,g) = f_m^{n-d} f_m^d \prod_{i=1}^{m} g(\alpha_i)$. Which proves (1) in this case.

Case 2: $\deg(g) = n \ge 1$, and $\deg(f) = d < m$. In this case, Part (2) follows by Case 1 and Lemma 3.5.5 (4).

Case 3: Assume $\deg(f) = m \geq 1$ and $\deg(g) = n \geq 1$, and $m \leq n$. As in Lemma 3.5.6, write $g = fq + r$, where $r = \sum_{i=0}^{m-1} r_i x^i$. By Lemma 3.5.6 and the induction hypothesis,

$$\begin{aligned} \operatorname{Res}(f,g) &= f_m^{n-m+1} \operatorname{Res}(f,r) \\ &= f_m^{n-m+1} f_m^{m-1} \prod_{i=1}^{m} r(\alpha_i) \\ &= f_m^{n} \prod_{i=1}^{m} g(\alpha_i) \end{aligned}$$

where the last equation follows since $r(\alpha_i) = g(\alpha_i) - f(\alpha_i)q(\alpha_i)$. In this case, we have proved Part (1). By

$$\begin{aligned} \operatorname{Res}(f,g) &= f_m^{n} \prod_{i=1}^{m} g(\alpha_i) \\ &= f_m^{n} \prod_{i=1}^{m} g_n(\alpha_i - \beta_1) \cdots (\alpha_i - \beta_n) \\ &= g_n^{m} \prod_{j=1}^{n} f_m(\alpha_1 - \beta_j) \cdots (\alpha_m - \beta_j) \\ &= (-1)^{mn} g_n^{m} \prod_{j=1}^{n} f(\beta_j) \end{aligned}$$

we see that Part (2) holds in Case 3.

Case 4: Assume $\deg(f) = m \geq 1$ and $\deg(g) = n \geq 1$, and $n \leq m$. By Lemma 3.5.5 (4), this reduces to Case 3. □

COROLLARY 3.5.8. *In the above context,* $\operatorname{Res}(f,g) = 0$ *if and only if one of the following is satisfied:*

(1) $\deg(f) < m$ *and* $\deg(g) < n$.

(2) $(f,g) \neq k[x]$*, or equivalently, f and g have a common irreducible factor, or equivalently, f and g have a common root in some extension field F/k.*

PROOF. If (1) is true, then the first column of $\operatorname{Syl}(f,g)$ is made up of zeros, so $\operatorname{Res}(f,g) = 0$. Otherwise, by Lemma 3.5.5, we can reduce to the case where $\deg(f) = m$. By Theorem 3.5.7 (1), $\operatorname{Res}(f,g) = 0$ if and only if f and g have a common root in some extension field F/k. By Exercise 2.5.9, this is equivalent to (2). □

CHAPTER 4

Fields

If k is a field, there is a unique homomorphism $\eta : \mathbb{Z} \to k$ and the kernel of η is either (0), or (p) for some prime p. If η is one-to-one, then the characteristic of k is zero and k contains the quotient field of $\operatorname{im}\eta$, which is isomorphic to the field of rational numbers $\mathbb{Q}$. Otherwise, the characteristic of k is positive and the image of η is a finite field isomorphic to $\mathbb{Z}/p$, where $p = \operatorname{char} k$. The image of η is contained in every subring of k. The *prime subfield* of k is the smallest subfield P of k, it contains the image of η. If $\operatorname{char} k = 0$, then P is isomorphic to $\mathbb{Q}$. Otherwise, $\operatorname{char} k = p$ is positive and P is isomorphic to $\mathbb{Z}/p$.

1. Algebraic Extensions and Transcendental Extensions

Let k and F be fields. If k is a subring of F, then we say F is an *extension* of k, k is a *subfield* of F, or that F/k is an *extension of fields*.

Let F/k be an extension of fields. Then F is a k-algebra, and in particular F is a vector space over k. If $X \subseteq F$, then by $k[X]$ we denote the k-subalgebra of F generated by k and X. By $k(X)$ we denote the subfield of F generated by k and X. If $F = k(u_1, \ldots, u_n)$, then we say F is finitely generated over k. If $F = k(u)$, then we say F is a *simple extension* of k.

LEMMA 4.1.1. *Let F/k be an extension of fields and $X \subseteq F$.*

(1) $k[X] = \{g(u_1, \ldots, u_n) \mid n \geq 1, u_i \in X, g \in k[x_1, \ldots, x_n]\}$

(2) $k(X) = \left\{ \frac{g(u_1,\ldots,u_n)}{h(v_1,\ldots,v_n)} \mid n \geq 1, u_i, v_j \in X, g, h \in k[x_1, \ldots, x_n], h(v_1, \ldots, v_n) \neq 0 \right\}$

As k-algebras, the quotient field of $k[X]$ is isomorphic to $k(X)$.

PROOF. Is left to the reader. □

Let F/k be an extension of fields. Let L and M be intermediate fields. That is, $k \subseteq L \subseteq F$ and $k \subseteq M \subseteq F$. The *composite* of L and M, denoted LM, is $k(L \cup M)$.

DEFINITION 4.1.2. Let F/k be an extension of fields and $u \in F$. If there is a nonzero polynomial $f \in k[x]$ and $f(u) = 0$, then we say u is *algebraic* over k. Otherwise we say u is *transcendental* over k. We say F/k is an *algebraic extension* if each element of F is algebraic over k.

PROPOSITION 4.1.3. *Let F/k be an extension of fields and $u \in F$ a transcendental element. Let x be an indeterminate. Then $k(x) \cong k(u)$ by a k-algebra isomorphism which maps x to u.*

PROOF. Let $\phi : k[x] \to k(u)$. Since u is transcendental, if $h(x) \in k[x]$ is nonzero, the $h(u) \neq 0$ in $k(u)$. By Theorem 2.4.3, ϕ factors through $k(x)$. □

THEOREM 4.1.4. *Let F/k be an extension of fields. Let u be an element of F which is algebraic over k. Let x be an indeterminate.*

(1) $k[u] = k(u)$

(2) $k[u] \cong k[x]/(f)$ *where* $f \in k[x]$ *satisfies*
   (a) f *is monic, irreducible,*
   (b) $f(u) = 0$, *and*
   (c) *if* $g(u) = 0$ *for some* $g \in k[x]$, *then* f *divides* g.
   The polynomial f *is uniquely determined by* u. *We call* f *the* irreducible polynomial *for* u *over* k *and write* $f = \operatorname{Irr.poly}_k(u)$. *Sometimes* f *is called the* minimal polynomial *for* u *over* k, *in which case we write* $f = \operatorname{min.poly}_k(u)$.

(3) *If* f *is the irreducible polynomial of* u *and* $\deg f = n$, *then* $\{1, u, \dots, u^{n-1}\}$ *is a basis for* $k[u]$ *as a* k*-vector space.*

(4) $\dim_k(k[u])$ *is equal to the degree of the irreducible polynomial of* u.

PROOF. (2): Let $\phi : k[x] \to F$ be the k-algebra homomorphism determined by $x \mapsto u$. Since $k[x]$ is a principal ideal domain, the kernel of ϕ is a principal ideal, say $\ker(\phi) = (f)$. Then ϕ factors to give the isomorphism $k[x]/(f) \cong k[u]$. Since F is a field, the kernel of ϕ is a prime ideal. Since $k[x]$ is a principal ideal domain, the prime ideal (f) is maximal, f is irreducible, and we can assume f is monic. It follows that the image of ϕ is a field, so $k[u] = k(u)$. Notice that $g \in \ker(\phi)$ if and only if $g(u) = 0$ if and only if f divides g.

(2) implies (1): By (2), $k[u]$ is a field.

(2) implies (3): By Exercise 3.1.17.

(3) implies (4): Immediate. □

THEOREM 4.1.5. *Assume* F/k *is an extension of fields and* $u \in F$. *Assume* L/K *is another extension of fields and* $v \in L$. *Let* $\sigma : k \to K$ *be an isomorphism of fields and assume either*

(1) u *is transcendental over* k *and* v *is transcendental over* K, *or*

(2) u *is a root of the irreducible polynomial* $f \in k[x]$ *and* v *is a root of the irreducible polynomial* $\bar{\sigma}(f) \in K[x]$.

Then there is an isomorphism $\tau : k(u) \to K(v)$ *such that* $\tau|_k = \sigma$ *and* $\tau(u) = v$.

PROOF. (1): Follows straight from Proposition 4.1.3.

(2): Note that σ induces an isomorphism $\bar{\sigma} : k[x] \to K[x]$ and the image of the irreducible polynomial f is the irreducible polynomial $\bar{\sigma}(f)$. Consequently, the kernel of

$$k[x] \to \frac{K[x]}{(\bar{\sigma}(f))}$$

is the principal ideal (f). The rest follows from Theorem 4.1.4. □

COROLLARY 4.1.6. *Let* F/k *be an extension of fields and assume* $u, v \in F$. *Assume either*

(1) u *and* v *are transcendental over* k, *or*

(2) u *and* v *are algebraic and satisfy the same irreducible polynomial.*

Then there is a k*-algebra isomorphism* $\tau : k(u) \to k(v)$ *such that* $\tau(u) = v$.

COROLLARY 4.1.7. *Let* F/k *be an extension of fields. Assume* $u, v \in F$ *are algebraic over* k *and that there is a* k*-algebra isomorphism* $\tau : k(u) \to k(v)$ *such that* $\tau(u) = v$. *Then* u *and* v *satisfy the same irreducible polynomial.*

PROOF. Let $\phi : k[x] \to k[u]$ where $\phi(x) = u$. Let $\psi : k[x] \to k[v]$ where $\psi(x) = v$. The diagram of k-algebra homomorphisms

$$\begin{tikzcd} k[x] \arrow[r, "\phi"] \arrow[d, "="'] & k[u] \arrow[d, "\tau"] \\ k[x] \arrow[r, "\psi"] & k[v] \end{tikzcd}$$

commutes. Let $\ker(\phi) = (f)$, where f is the monic irreducible polynomial for u. The diagram commutes, so $f \in \ker(\psi)$. It follows that $f(v) = 0$. Since $\ker(\psi)$ is a principal ideal and maximal, it follows that $\ker(\psi)$ is generated by f. □

THEOREM 4.1.8. *(Kronecker's Theorem) Let k be a field and f a polynomial of positive degree in $k[x]$. There exists an extension field F of k and an element $u \in F$ satisfying*

(1) u is a root of f,
(2) $\dim_k(k[u]) \leq \deg(f)$, and
(3) if f is irreducible, then $\dim_k(k[u]) = \deg(f)$ and $k[u]$ is unique up to a k-algebra isomorphism.

PROOF. Let g be an irreducible factor of f, set $F = k[x]/(g)$ and take u to be the coset of x in F. The rest follows from Theorem 4.1.4 and Corollary 4.1.6. □

PROPOSITION 4.1.9. *Let F/k be an extension of fields.*

(1) If F is finite dimensional over k, then F is finitely generated and algebraic over k.
(2) (Finitely Generated and Algebraic is Finite Dimensional) If $X = \{u_1, \dots, u_n\} \subseteq F$ and each u_i is algebraic over k, then $\dim_k k(X) < \infty$.
(3) If $F = k(X)$ and every element of X is algebraic over k, then F is algebraic over k.
(4) (Algebraic over Algebraic is Algebraic) Let E be an intermediate field of F/k. If F/E is algebraic and E/k is algebraic, then F/k is algebraic.
(5) (Algebraic Closure of k in F) If $E = \{u \in F \mid u \text{ is algebraic over } k\}$, then E is an intermediate field of F/k.

PROOF. (1): Clearly F is finitely generated. Suppose $u \in F$, and $\dim_k(F) = n$. The set $\{u^n, u^{n-1}, \dots, u, 1\}$ is linearly dependent. A dependence relation $0 = a_n u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0$ over k shows that u is algebraic over k.

(2): By Theorem 4.1.4, $\dim_k k(u_1) < \infty$. Now use induction and Proposition 3.1.33.

(3): Let $u \in k(X)$. Then there exist $u_1, \dots, u_m, v_1, \dots, v_n$ in X and polynomials f, g over k such that

$$u = \frac{f(u_1, \dots, u_m)}{g(v_1, \dots, v_n)}.$$

This shows $u \in k(u_1, \dots, u_m, v_1, \dots, v_n)$. By Parts (2) and (1) this shows u is algebraic over k.

(4): Let $u \in F$. There is a polynomial $f = \sum_{i=0}^n a_i x^i$ in $E[x]$ such that $f(u) = 0$. Let $K = k(a_0, \dots, a_n)$. Then u is algebraic over K and $\dim_K K(u) < \infty$. Since each a_i is algebraic over k, by Part (2), $\dim_k K < \infty$. By Proposition 3.1.33, $\dim_k K(u) < \infty$. By Part (1), u is algebraic over k.

(5): Let u, v be algebraic over k. By Part (3), $k(u, v)$ is an algebraic extension of k. So $k(u, v) \subseteq E$. Therefore, $u + v$, $u - v$, uv, u/v are all in E. It follows that E is a field. □

THEOREM 4.1.10. *Let K/k be an extension of fields. Let E and F be intermediate fields. Assume $\dim_k F = n$ is finite and that $\{v_1, \dots, v_n\}$ is a basis for F as a k-vector space. The following are true.*

(a) As a vector space over E, EF is spanned by $\{v_1, \dots, v_n\}$.
(b) $\dim_E (EF) \le \dim_k F$.
(c) If $\dim_k E = m$ is finite and $\{u_1, \dots, u_m\}$ is a basis for E as a k-vector space, then $\dim_k EF \le \dim_k E \dim_k F$ and as a vector space over k, EF is spanned by $\{u_i v_j \mid 1 \le i \le m,\ 1 \le j \le n\}$.
(d) If $\dim_k E$ and $\dim_k F$ are finite and relatively prime, then $\dim_k EF = \dim_k F \dim_k E$.

PROOF. We have $F = k(v_1, \dots, v_n)$. Then $EF = k(E \cup F) = k(E)(F) = E(F) = E(k(v_1, \dots, v_n)) = E(v_1, \dots, v_n)$. By Lemma 4.1.1, a typical element u in EF is a linear combination $u = e_1 M_1 + \cdots + e_r M_r$ where each e_i is in E and each M_i is a monomial of the form $M_i = v_1^{\varepsilon_{i,1}} \cdots v_n^{\varepsilon_{i,n}}$, where $\varepsilon_{i,j} \ge 0$ for each i, j. In the field F, each monomial M_i can be written as a k-linear combination in the form $M_i = a_{i,1} v_1 + \cdots + a_{i,n} v_n$, where $a_{i,j} \in k$ for each i, j. Therefore,

$$\begin{aligned} u &= e_1 M_1 + \cdots + e_r M_r \\ &= \sum_{i=1}^{r} \left(e_i \sum_{j=1}^{n} a_{i,j} v_j \right) \end{aligned}$$

This proves (a). Part (b) follows from (a) and Proposition 3.1.28. Part (c) follows from (b), Proposition 3.1.33, and its proof. For (d), we have $\dim_k (E) = m$ and $\dim_k (F) = n$ both divide $\dim_k (EF)$. Since m and n are relatively prime, it follows that mn is the least common multiple of m and n. Thus $mn \le \dim_k (EF)$. □

1.1. Exercises.

EXERCISE 4.1.1. Let F/k be an extension of fields. Prove that F/k is an algebraic extension if and only if for every k-subalgebra R of F, R is a field.

EXERCISE 4.1.2. Let k be a field and F an extension field of k. Suppose α and β are elements of F that are algebraic over k. Using resultants (Section 3.5.2), show that $\alpha + \beta$ and $\alpha\beta$ are algebraic over k. Show how to find the minimal polynomials for $\alpha + \beta$ and $\alpha\beta$.

2. The Fundamental Theorem of Galois Theory

In this section we present a proof of the Fundamental Theorem of Galois Theory which is due to DeMeyer [**7**].

Let F/k be an extension of fields. As in Definition 3.1.14, by $\operatorname{Aut}_k(F)$ we denote the group of all k-algebra automorphisms of F. If G is a group and H is a subgroup, the index of H in G is denoted $[G : H]$. The order of G is $[G : 1]$.

DEFINITION 4.2.1. Let F/k be an extension of fields and G a finite subgroup of $\operatorname{Aut}_k(F)$. If $k = F^G$, then we say F/k is a *Galois* extension with Galois group G.

PROPOSITION 4.2.2. *Let F/k be an extension of fields.*

(1) Let $f \in k[x]$, $\sigma \in \operatorname{Aut}_k(F)$, and $u \in F$. If $f(u) = 0$, then $f(\sigma(u)) = 0$.
(2) Assume $u \in F$ is algebraic over k and $E = k[u]$. If $\sigma \in \operatorname{Aut}_k(E)$, then σ is completely determined by $\sigma(u)$.

(3) *If H is a subset of $G = \operatorname{Aut}_k(F)$, then*

$$F^H = \{v \in F \mid \sigma(v) = v, (\forall \sigma \in H)\}$$

is an intermediate field of F/k which is called the fixed field of H.

(4) *If $G = \operatorname{Aut}_k(F)$ and E is an intermediate field of F/k, then*

$$G_E = \{\sigma \in G \mid \sigma(v) = v, (\forall v \in E)\}$$

is a subgroup of G which is called the subgroup of G fixing E. Note that $G_E = \operatorname{Aut}_E(F)$.

PROOF. (1): If $f = \sum_{i=0}^n a_i x^i$, then $f(\sigma(u)) = \sum a_i(\sigma(u))^i = \sum \sigma(a_i u^i) = \sigma(\sum a_i u^i) = \sigma(0) = 0$.

(2): By Theorem 4.1.4, there is a k-basis for E of the form $1, u, u^2, \dots, u^{n-1}$ where $n = \dim_k(E)$.

(3) and (4): Proofs are left to the reader. □

LEMMA 4.2.3. *Let F be a field with automorphism group $\operatorname{Aut}(F)$. Let G be a finite subset of $\operatorname{Aut}(F)$, and set $k = F^G$. Let E be an intermediate field of F/k and $G_E = G \cap \operatorname{Aut}_E(F)$. Then there exist elements $a_1, \dots, a_n$ in E and $y_1, \dots, y_n$ in F such that for each $\sigma \in G$*

$$a_1\sigma(y_1) + \cdots + a_n\sigma(y_n) = \begin{cases} 1 & \text{if } \sigma \in G_E \\ 0 & \text{if } \sigma \notin G_E. \end{cases} \tag{4.1}$$

PROOF. If $G = G_E$, then simply take $n = 1$, $a_1 = y_1 = 1$. If $G \neq G_E$, pick σ in $G - G_E$ and let $S = G_E \cup \{\sigma\}$. There is an element $a \in E$ such that $\sigma(a) \neq a$. Since F is a field and σ is an automorphism, there is $b \in F$ such that $b(\sigma^{-1}(a) - a) = 1$. Set $a_1 = a$, $a_2 = 1$, $y_1 = -b$, $y_2 = b\sigma^{-1}(a)$. For any $\tau \in G_E$ we have

$$a_1\tau(y_1) + a_2\tau(y_2) = \tau(a_1y_1 + a_2y_2) = \tau(-ab + b\sigma^{-1}(a)) = \tau(1) = 1$$

and for $\sigma \in S - G_E$,

$$a_1\sigma(y_1) + a_2\sigma(y_2) = -a\sigma(b) + \sigma(b\sigma^{-1}(a)) = 0.$$

Now suppose S is a subset of G containing G_E such that there exist $a_1, \dots, a_m$ in E and $y_1, \dots, y_m$ in F satisfying (4.1) for all $\sigma \in S$. Also suppose S' is another subset of G containing G_E such that there exist $a'_1, \dots, a'_n$ in E and $y'_1, \dots, y'_n$ in F satisfying (4.1) for all $\sigma' \in S'$. For any $\tau \in S \cup S'$ we get

$$\begin{aligned} \sum_{i=1}^m \sum_{j=1}^n a_i a'_j \tau(y_i y'_j) &= \left(\sum_{i=1}^m a_i \tau(y_i)\right)\left(\sum_{j=1}^n a'_j \tau(y'_j)\right) \\ &= \begin{cases} 1 & \text{if } \tau \in G_E \\ 0 & \text{if } \tau \notin G_E. \end{cases} \end{aligned}$$

The sets of elements $\{a_i a'_j \mid 1 \le i \le m, 1 \le j \le n\}$ in E and $\{y_i y'_j \mid 1 \le i \le m, 1 \le j \le n\}$ in F satisfy (4.1) for all τ in $S \cup S'$. The proof is complete, by a finite induction argument, since G has a finite covering by the sets $G_E \cup \{\sigma\}$. □

LEMMA 4.2.4. *Let F be a field and G a subgroup of $\operatorname{Aut}(F)$. Let $k = F^G$ and let E be an intermediate field of F/k. Let $\sigma_1, \dots, \sigma_m$ be a set of left coset representatives for G_E in G. If $u_1, \dots, u_m$ are in F such that*

$$\sum_{i=1}^m u_i \sigma_i(x) = 0$$

for all $x \in E$, then each u_i is equal to zero.

PROOF. Fix an integer p such that $1 \leq p \leq m$. By Lemma 4.2.3 applied to the set $\{\sigma_1^{-1}\sigma_p, \dots, \sigma_m^{-1}\sigma_p\}$, there exist elements $a_1, \dots, a_n$ in E and elements $y_1, \dots, y_n$ in F such that for each $1 \leq j \leq m$,

$$a_1\sigma_j^{-1}\sigma_p(y_1) + \cdots + a_n\sigma_j^{-1}\sigma_p(y_n) = \begin{cases} 1 & \text{if } p = j \\ 0 & \text{if } p \neq j. \end{cases}$$

If $u_1\sigma_1(x) + \cdots + u_m\sigma_m(x) = 0$ for all $x \in E$, then

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} u_j\sigma_j(a_i) \right) \sigma_p(y_i) \\ &= \sum_{j=1}^{m} u_j \left(\sum_{i=1}^{n} \sigma_j(a_i)\sigma_p(y_i) \right) \\ &= \sum_{j=1}^{m} u_j\sigma_j \left(\sum_{i=1}^{n} a_i\sigma_j^{-1}\sigma_p(y_i) \right) \\ &= u_p. \end{aligned}$$

□

LEMMA 4.2.5. *If F is a field and G is a finite subgroup of $\operatorname{Aut}(F)$, then there exists $c \in F$ such that $\sum_{\sigma \in G} \sigma(c) = 1$.*

PROOF. By Lemma 4.2.4 with $E = F$, there exists an element $b \in F$ such that $x = \sum_{\sigma \in G} \sigma(b) \neq 0$. Since x is in $F^G = k$ and k is a field, $x^{-1} \in k$. Take $c = x^{-1}b$. Then

$$\sum_{\sigma \in G} \sigma(c) = \sum_{\sigma \in G} \sigma(x^{-1}b) = x^{-1} \sum_{\sigma \in G} \sigma(b) = 1.$$

□

LEMMA 4.2.6. *Let F/k be a Galois extension with finite group G. Let E be an intermediate field of F/k and let $\sigma_1, \dots, \sigma_m$ be a full set of left coset representatives for G_E in G. If $T \in \operatorname{Hom}_k(E, F)$, then there exist unique elements $u_1, \dots, u_m$ in F such that*

$$T(x) = \sum_{j=1}^{m} u_j\sigma_j(x)$$

for all $x \in E$.

PROOF. By Lemma 4.2.3 there exist $a_1, \dots, a_n$ in E and $y_1, \dots, y_n$ in F satisfying

$$a_1\sigma(y_1) + \cdots + a_n\sigma(y_n) = \begin{cases} 1 & \text{if } \sigma \in G_E \\ 0 & \text{if } \sigma \notin G_E. \end{cases}$$

By Lemma 4.2.5 there exists $c \in F$ such that $\sum_{\sigma \in G_E} \sigma(c) = 1$. If $x \in E$ and $\sigma \in G_E$, then $\sigma(x) = x$. It follows that

$$\begin{aligned} x &= \sum_{\sigma \in G_E} \sigma(c)\sigma(x) \\ &= \sum_{\sigma \in G_E} \left(\sigma(c)\sigma(x) \sum_{i=1}^{n} a_i \sigma(y_i) \right) \\ &= \sum_{\sigma \in G} \left(\sigma(cx) \sum_{i=1}^{n} a_i \sigma(y_i) \right) \\ &= \sum_{i=1}^{n} \sum_{\sigma \in G} a_i \sigma(y_i cx). \end{aligned}$$

For any $y \in F$, $\sum_{\sigma \in G} \sigma(y) \in k$. Applying T,

$$\begin{aligned} T(x) &= \sum_{i=1}^{n} T\left(a_i \sum_{\sigma \in G} \sigma(y_i cx) \right) \\ &= \sum_{i=1}^{n} T(a_i) \left(\sum_{\sigma \in G} \sigma(y_i cx) \right) \\ &= \sum_{\sigma \in G} \left(\sum_{i=1}^{n} T(a_i)\sigma(y_i c) \right) \sigma(x). \end{aligned}$$

The outer sum can be split over the cosets of G_E in G. Therefore, setting

$$u_j = \sum_{\sigma \in \sigma_j G_E} \sum_{i=1}^{n} T(a_i)\sigma(y_i c),$$

we have

$$T(x) = \sum_{j=1}^{m} u_j \sigma_j(x).$$

To prove that the coefficients are unique, assume

$$\sum_{j=1}^{m} u_j \sigma_j(x) = \sum_{j=1}^{m} v_j \sigma_j(x)$$

for all $x \in E$. Then

$$\sum_{j=1}^{m} (u_j - v_j)\sigma_j(x) = 0$$

and by Lemma 4.2.4, $u_j - v_j = 0$ for all j. □

THEOREM 4.2.7. *Let F/k be a finite Galois extension with group G. Let E be an intermediate field of F/k. If $\tau : E \to F$ is a k-algebra homomorphism, then τ is the restriction of some $\sigma \in G$. In particular,* $\operatorname{Aut}_k(F) = G$.

PROOF. Let $\sigma_1, \dots, \sigma_m$ be a full set of left coset representatives for G_E in G. By Lemma 4.2.6 there exist $u_1, \dots, u_m$ such that $\tau(x) = u_1\sigma_1(x) + \cdots + u_m\sigma_m(x)$ for all $x \in E$. For any $a, b \in E$ we have

$$\tau(ab) = \sum_{j=1}^{m} u_j \sigma_j(a)\sigma_j(b)$$

as well as

$$\tau(ab) = \tau(a)\tau(b) = \tau(a)\sum_{j=1}^{m} u_j\sigma_j(b) = \sum_{j=1}^{m} u_j\tau(a)\sigma_j(b).$$

Subtracting yields

$$0 = \sum_{j=1}^{m} u_j\left(\sigma_j(a) - \tau(a)\right)\sigma_j(b).$$

The uniqueness part of Lemma 4.2.6 says $u_j(\sigma_j(a) - \tau(a)) = 0$ for all $a \in E$ and for all j. There is at least one j such that $u_j \neq 0$. For that j we have $\tau(a) = \sigma_j(a)$ for all $a \in E$. □

THEOREM 4.2.8. *Let F be a field, G a subgroup of $\operatorname{Aut}(F)$ and $k = F^G$. Then G is finite if and only if $\dim_k(F)$ is finite and in this case the order of G is equal to $\dim_k(F)$.*

PROOF. If G is finite, then apply Lemma 4.2.3 to $E = F$. There are elements $a_1, \dots, a_n$, $y_1, \dots, y_n$ in F such that

$$\sum_{i=1}^{n} a_i y_i = 1 \tag{4.2}$$

and

$$\sum_{i=1}^{n} a_i\sigma(y_i) = 0 \tag{4.3}$$

for all $\sigma \neq 1$. Let x be an element of F. Multiply (4.2) by x, multiply (4.3) by $\sigma(x)$, and sum over all σ to get

$$\begin{aligned} x &= \sum_{i=1}^{n} a_i y_i x + \sum_{\sigma\neq 1}\sum_{i=1}^{n} a_i\sigma(y_i x) \\ &= \sum_{\sigma\in G}\left(\sum_{i=1}^{n} a_i\sigma(y_i x)\right) \\ &= \sum_{i=1}^{n} a_i\left(\sum_{\sigma\in G}\sigma(y_i x)\right). \end{aligned}$$

Since $\sum_{\sigma\in G}\sigma(y_i x) \in k$, it follows that $a_1, \dots, a_n$ is a spanning set for F as a k-vector space.

Conversely, assume $n = \dim_k(F)$ is finite. As in Example 3.3.3, the left regular representation of the k-algebra F is a one-to-one k-algebra homomorphism $F \to \operatorname{Hom}_k(F,F)$. By Proposition 3.3.9, $\dim_k(\operatorname{Hom}_k(F,F)) = n^2$. By Proposition 3.1.33,

$$\dim_k(\operatorname{Hom}_k(F,F)) = \dim_F(\operatorname{Hom}_k(F,F))\dim_k(F).$$

It follows that $\dim_F(\operatorname{Hom}_k(F,F)) = n$. By Lemma 4.2.4, with $E = F$, every finite subset of G is a linearly independent subset of the F-vector space $\operatorname{Hom}_k(F,F)$. This proves $[G : 1] \leq n$. By Lemma 4.2.6, the set G is a basis for $\operatorname{Hom}_k(F,F)$ as an F-vector space. This proves $[G : 1] = n$. □

THEOREM 4.2.9. *(The Fundamental Theorem of Galois Theory) Let F/k be a Galois extension of fields with finite group G. There is a one-to-one order inverting correspondence between the subgroups H of G and the intermediate fields E of F/k. A subgroup H corresponds to the fixed field F^H. An intermediate field E corresponds to the subgroup G_E. If E is an intermediate field of F/k, then*

(1) $\dim_E(F) = [G_E : 1]$, $\dim_k(E) = [G : G_E]$, $G_E = \operatorname{Aut}_E(F)$,

(2) F/E is a Galois extension with group G_E, and

(3) *E/k is a Galois extension if and only if G_E is a normal subgroup of G and in this case, $G/G_E \cong \operatorname{Aut}_k(E)$.*

PROOF. The reader should verify that the correspondences given are well defined and order inverting. Suppose H and K are two subgroups of G such that $F^H = F^K$. Apply Theorem 4.2.7 with $k = F^H = F^K$ and $E = F$. Then we get $H \subseteq K$ and $K \subseteq H$. Let E be an intermediate field of F/k. Then $E \subseteq F^{G_E}$. We show the reverse inclusion. Let $x \in F^{G_E}$. If $\sigma \in G_E$, then $\sigma(x) = x$. By the first part of the proof of Lemma 4.2.6, there exist $a_1, \dots, a_n$ in E, $y_1, \dots, y_n$ in F, and $c \in F$ such that

$$x = \sum_{i=1}^{n} \left(a_i \sum_{\sigma \in G} \sigma(y_i c x) \right),$$

which is in E. The correspondence between subgroups and intermediate fields is one-to-one. If E is an intermediate field, then F is a Galois extension of $E = F^{G_E}$ and (2) follows. By Theorem 4.2.8, $\dim_E(F) = [G_E : 1]$. Also $[G : 1] = [G : G_E][G_E : 1]$ and $\dim_k(F) = \dim_k(E)\dim_E(F)$ says $\dim_k(E) = [G : G_E]$. By Theorem 4.2.7 with $k = E$ and $E = F$, it follows that $G_E = \operatorname{Aut}_E(F)$ and (1) is done.

(3): Assume G_E is a normal subgroup of G. Given $\sigma \in G$, we show that $\sigma|_E \in \operatorname{Hom}_k(E,E)$. If not, there is some $x \in E$ such that $\sigma(x) \notin E$. Since $F^{G_E} = E$, there is $\tau \in G_E$ such that $\tau\sigma(x) \neq \sigma(x)$, which implies $\sigma^{-1}\tau\sigma(x) \neq x$. This contradicts the assumption that $\sigma^{-1}\tau\sigma \in G_E$. Consequently, the restriction map defines a homomorphism of groups $G \to \operatorname{Aut}_k(E)$ with kernel G_E. So G/G_E is isomorphic to a subgroup of $\operatorname{Aut}_k(E)$. Since $F^G = k$, it follows that $k = E^G = E^{G/G_E}$, so E/k is a Galois extension with group G/G_E. For the converse, assume E is an intermediate field of F/k which is a Galois extension of k with group $\operatorname{Aut}_k(E)$. By Theorem 4.2.7, every $\tau \in \operatorname{Aut}_k(E)$ is the restriction of some element $\sigma \in G$. So there is a subgroup G' of G such that the restriction map $\sigma \mapsto \sigma|_E$ defines a surjective homomorphism $\theta : G' \to \operatorname{Aut}_k(E)$. The kernel of θ contains G_E. Since $[\operatorname{Aut}_k(E) : 1] = [E : k] = [G : G_E]$, a finite counting argument shows that $G' = G$ and G_E is equal to the kernel of θ. Hence G_E is normal in G and $G/G_E \cong \operatorname{Aut}_k(E)$. □

3. Splitting Fields

DEFINITION 4.3.1. Let k be a field and p a polynomial in $k[x]$ of positive degree. If F/k is an extension of fields, then we say that p *splits* in F if each irreducible factor of p in $F[x]$ is linear. Equivalently, p factors in $F[x]$ into a product of linear polynomials.

LEMMA 4.3.2. *Let F be a field. The following are equivalent.*

(1) *Every nonconstant polynomial $p \in F[x]$ has a root in F.*
(2) *Every nonconstant polynomial $p \in F[x]$ splits in F.*
(3) *Every irreducible polynomial $p \in F[x]$ has degree 1.*
(4) *If K/F is an algebraic extension of fields, then $F = K$.*
(5) *F contains a subfield k such that F/k is algebraic and every polynomial in $k[x]$ splits in F.*

PROOF. (1), (2), and (3) are clearly equivalent.
To show (3) and (4) are equivalent, use Theorem 4.1.4.
(2) implies (5): Is trivial.
(5) implies (4): If K/F is algebraic, then by Proposition 4.1.9 (4), K/k is algebraic. If $u \in K$, then the irreducible polynomial of u over k splits in F. Therefore $u \in F$. □

DEFINITION 4.3.3. If F is a field that satisfies any of the equivalent statements of Lemma 4.3.2, then we say F is *algebraically closed*. If F/k is an extension of fields, we say F is an *algebraic closure* of k in case F is algebraic over k, and F is algebraically closed.

DEFINITION 4.3.4. Let F/k be an extension of fields and p a nonconstant polynomial in $k[x]$. We say that F is a *splitting field* of p if

(1) p splits in F, and
(2) $F = k(u_1, \dots, u_n)$ where $p(u_i) = 0$ for each i.

If S is a set of polynomials in $k[x]$, then we say F is a *splitting field* of S if

(1) every polynomial p in S splits in F, and
(2) if X is the set of all $u \in F$ such that $p(u) = 0$ for some $p \in S$, then $F = k(X)$.

The reader should verify that if $S = \{p_1, \dots, p_n\}$ is a finite subset of $k[x]$, then F is a splitting field for S if and only if F is a splitting field for $p_1 \cdots p_n$.

PROPOSITION 4.3.5. *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 $\dim_k(F) \le n!$.
(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 (Theorem 4.1.8), 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 $\dim_k(F_1) = \deg p_1 \le n$. Factor $f = (x-\alpha)g$ in $F_1[x]$. By induction on n, there exists a splitting field F/F_1 for g and $\dim_{F_1}(F) \le (n-1)!$. 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, $\dim_k(F) = \dim_k(F_1)\dim_{F_1}(F) \le n!$.

(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 1.3.2. By the Well Ordering Principle, Axiom 1.2.1, 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 $S(\gamma) = \{p_\alpha \in S \mid \alpha \le \gamma\}$. 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 4.3.6. *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 Theorem 4.1.5 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 σ to a root of $\sigma(f)$. Since f splits in F, $\sigma(f)$ splits in $\bar{\sigma}(F)$. By Corollary 2.5.8, $\sigma(f)$ 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 1.3.3, 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 4.3.7. *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 4.3.6.

(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 4.3.5, 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 4.3.6, 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 4.3.6, θ is an isomorphism. □

DEFINITION 4.3.8. Let F/k be an algebraic extension of fields. We say F/k is a *normal* extension if every irreducible polynomial over k that has a root in F actually splits over F.

THEOREM 4.3.9. *If F/k is an algebraic extension of fields, then the following are equivalent.*

1. *F/k is a normal extension.*
2. *F is the splitting field over k of a set of polynomials in $k[x]$.*
3. *If Ω is an algebraic closure of k containing F, then any k-algebra homomorphism $\theta: F\to\Omega$, maps F to F, hence θ restricts to a k-automorphism of F.*

PROOF. (1) implies (2): If B is a basis for F/k, then F is the splitting field of the set of polynomials $\{\operatorname{Irr.poly}_k(\beta)\mid\beta\in B\}$ over k.

(2) implies (3): Suppose S is a set of polynomials in $k[x]$ and F is the splitting field for S over k. Let Ω be an algebraic closure for k containing F and $\theta: F\to\Omega$ a k-algebra homomorphism. Suppose $f\in S$ and that α is a root of f in Ω. Then $\theta(\alpha)=\beta$ is another root of f in Ω. But F contains every root of f. Moreover, F is generated by roots of polynomials in S. Therefore, θ maps F onto F.

(3) implies (1): Suppose f is an irreducible polynomial in $k[x]$. Let $\alpha \in F$ be a root of f. In Ω, let β be any other root of f. We show that β is in F. By Corollary 4.1.6 there is a k-algebra isomorphism $\theta : k(\alpha) \to k(\beta)$. By Lemma 4.3.6, θ extends to an isomorphism $\bar{\theta} : \Omega \to \Omega$. By assumption, the restriction of $\bar{\theta}$ to F maps F to F. This proves that $\beta \in F$. □

DEFINITION 4.3.10. Suppose F/k is an algebraic extension of fields. Let B be a basis for F/k, and K the splitting field of $\{\operatorname{Irr.poly}_k(\beta) \mid \beta \in B\}$ over F. The reader should verify that K/k is a normal extension of k containing F. We call K the *normal closure* of F over k.

4. Separable Extensions

DEFINITION 4.4.1. Let k be a field and Ω the algebraic closure of k. Let $f \in k[x]$. We say f is *separable* in case for every irreducible factor p of f, every root of p in Ω is a simple root. If F/k is a extension of fields, then we say F/k is *separable* if every $u \in F$ is the root of a separable polynomial in $k[x]$. If $u \in F$ is the root of a separable polynomial in $k[x]$, then we say u is *separable*. A separable extension is an algebraic extension. If $\operatorname{char} k = 0$, then by Theorem 2.5.13, every polynomial $f \in k[x]$ is separable.

THEOREM 4.4.2. *Let F/k be a finite dimensional extension of fields. The following are equivalent.*

(1) F/k is a Galois extension.
(2) F/k is separable and F is the splitting field over k of a set of polynomials in $k[x]$.
(3) F is the splitting field over k of a set of separable polynomials in $k[x]$.
(4) F/k is normal and separable.

PROOF. (2) is equivalent to (4): follows from Theorem 4.3.9.

(2) implies (3): Suppose F/k is the splitting field of the set $S \subseteq k[x]$. Let T be the set of irreducible factors of all polynomials in S. Given $f \in T$, let $u \in F$ be a root of f. Then $f = \operatorname{Irr.poly}_k(u)$. Since F/k is separable, u is the root of a separable polynomial $g \in k[x]$. In this case f divides g, so f is also separable.

(1) implies (4): If f is a monic irreducible polynomial in $k[x]$ and $\alpha \in F$ is a root of f, then by Theorem 4.1.4, $f = \operatorname{Irr.poly}_k(\alpha)$. Let $u \in F - k$. It is enough to prove that $\operatorname{Irr.poly}_k(u)$ is separable and splits over F. Let $G = \operatorname{Aut}_k(F)$ and $G_u = \{\sigma \in G \mid \sigma(u) = u\}$ the subgroup fixing u. If $U = \{\sigma(u) \mid \sigma \in G\}$ is the orbit of u under the action of G, then U has length $m = [G : G_u]$ and G acts as a group of permutations on U [**8**, Proposition 4.1.2]. Let $\sigma_1, \dots, \sigma_m$ be a full set of left coset representatives for G_u in G. Then the orbit of u is equal to $U = \{\sigma_1(u), \dots, \sigma_m(u)\}$. Consider the polynomial

$$\phi = \prod_{i=1}^{m} (x - \sigma_i(u))$$

in $F[x]$. By Theorem 2.5.2, we can view G as a group of automorphisms of $F[x]$ such that the stabilizer is $F[x]^G = F^G[x] = k[x]$. Since ϕ is fixed by each $\sigma \in G$, it follows that ϕ is in $k[x]$. Since $\phi(u) = 0$, Theorem 4.1.4 says $\operatorname{Irr.poly}_k(u)$ divides ϕ. Since ϕ splits over F, so does $\operatorname{Irr.poly}_k(u)$. By construction, ϕ is a separable polynomial in $k[x]$, hence so is $\operatorname{Irr.poly}_k(u)$.

(3) implies (1): Suppose F is the splitting field for a set S of separable polynomials over k. Proceed by induction on $n = \dim_k(F)$. If $n = 1$, there is nothing to prove. Otherwise, let g be a monic irreducible factor of one of the polynomials in S and assume $\deg g = d > 1$. Since g is separable and splits in F, there are d distinct roots $\alpha_1, \dots, \alpha_d$

in F and $g = (x-\alpha_1)\cdots(x-\alpha_d)$. Now $k(\alpha_1)$ is an intermediate field of F/k and F is a splitting field of a set of separable polynomials over $k(\alpha_1)$. By induction, we can assume $F/k(\alpha_1)$ is a Galois extension with group H and $[H:1] = \dim_{k(\alpha_1)}(F)$. By Corollary 4.1.6, for each i, there is a k-algebra isomorphism $\sigma_i : k(\alpha_1) \to k(\alpha_i)$. By Lemma 4.3.6 each σ_i extends to an automorphism $\bar{\sigma}_i \in \operatorname{Aut}_k(F)$. Since H is a subgroup of $\operatorname{Aut}_k(F)$, consider the cosets $\bar{\sigma}_i H$. By construction, $\bar{\sigma}_i H \cap \bar{\sigma}_j H = \emptyset$ if $i \neq j$. Therefore, the set $\bar{\sigma}_1 H \cup \cdots \cup \bar{\sigma}_d$ has exactly $d[H:1]$ elements. Notice that this is equal to $\dim_k(k(\alpha_1))\dim_{k(\alpha_1)}(F) = \dim_k(F)$. Let G be the subgroup of $\operatorname{Aut}_k(F)$ generated by $\bar{\sigma}_1 H \cup \cdots \cup \bar{\sigma}_d H$. We have shown $[G:1] \geq \dim_k(F)$. By Theorem 4.2.8, $\dim_{F^G}(F) = [G:1]$. This shows $k = F^G$. □

COROLLARY 4.4.3. *(Embedding Theorem for Fields) Let F/k be a finite dimensional extension of fields. If F/k is separable, then there exists a finite dimensional Galois extension K/k which contains F as an intermediate field.*

PROOF. Pick a finite set of separable elements $u_1,\dots,u_n$ that generate F/k. If $f_i = \operatorname{Irr.poly}_k(u_i)$, then f_i is separable over k. Let K be the splitting field for $f_1 \cdots f_n$ over k. So K contains a generating set for F, hence F is an intermediate field of K/k. By Theorem 4.4.2, K/k is a Galois extension. □

PROPOSITION 4.4.4. *Let R be an integral domain. Let $n > 1$ be an integer. The group of nth roots of unity in R, $\mu_n = \{u \in R \mid u^n = 1\}$, is a cyclic group of order at most n.*

PROOF. The set μ_n is clearly a subgroup of R^*. The order of μ_n is at most n, by Corollary 2.5.8. Using the Invariant Factor form of the Basis Theorem for finite abelian groups, Theorem 3.2.11, the finite abelian group μ_n decomposes into cyclic subgroups $\mu_n = \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_\nu$, where $1 < m_1$, $m_1 \mid m_2, \dots, m_{\nu-1} \mid m_\nu$. Let q be a prime divisor of m_1. The subgroup of μ_n annihilated by q is isomorphic to $\mathbb{Z}/q \oplus \cdots \oplus \mathbb{Z}/q$, and has order q^ν. The polynomial $x^q - 1$ has at most q solutions in R, by Corollary 2.5.8. This means $\nu = 1$. □

THEOREM 4.4.5. *(The Primitive Element Theorem) Let F/k be a finite dimensional extension of fields. If*

(1) k is infinite and F/k is separable, or
(2) k is finite,

then there is a separable element $u \in F$ such that $F = k(u)$.

PROOF. (1): By Corollary 4.4.3, let L/k be a finite Galois extension containing F as an intermediate field. By Theorem 4.2.9, there are only finitely many intermediate fields of L/k. That means there are only finitely many intermediate fields of F/k. Choose $u \in F$ such that $\dim_k(k(u))$ is maximal. For contradiction's sake, assume $k(u) \neq F$. Let $v \in F - k(u)$. Consider the set of intermediate fields $S = \{k(u+av) \mid a \in k\}$. Since k is infinite and the set S is finite, there exist $a, b \in k$ such that $a \neq b$ and $k(u+av) = k(u+bv)$. Then $(u+av)-(u+bv) = (a-b)v \in k(u+av)$, and since $(a-b)^{-1} \in k$, $v \in k(u+av)$. In this case, $u \in k(u+av)$ so $k(u,v) \subseteq k(u+av)$. Since $k(u,v)$ is a proper extension of $k(u)$, this shows that the simple extension $k(u+av)$ is a proper extension of $k(u)$. This contradicts the choice of u.

(2): If F has order q, and F^* denotes the group of units of F, then F^* has order $q-1$. Every element u of F^* satisfies $u^{q-1} = 1$. By Proposition 4.4.4 the group F^* is cyclic. There exists $u \in F^*$ such that $F^* = \{1, u, \dots, u^{q-2}\}$. The polynomial $x^{q-1} - 1$ splits in $F[x]$ and has $q-1$ roots in F. □

5. Finite Fields

A finite field has positive characteristic and is finite dimensional over its prime subfield.

LEMMA 4.5.1. *Let F be a field and assume* $\operatorname{char} F = p$ *is positive. For any $r > 0$, the mapping $\varphi : F \to F$ defined by $x \mapsto x^{p^r}$ is a homomorphism of fields. If F is finite, then φ is an automorphism of F. If $r = 1$, then φ is called the* Frobenius homomorphism.

PROOF. The reader should verify that φ is additive and multiplicative. Since F is a field, φ is one-to-one. □

LEMMA 4.5.2. *For each prime number p and for every $n \geq 1$, there exists a field F of order p^n.*

PROOF. Let k denote the field $\mathbb{Z}/p$. Let $f = x^{p^n} - x \in k[x]$. Let F be the splitting field of f over k. Since $f' = -1$, by Theorem 2.5.13, f has no multiple roots in F. Therefore, f is separable and there are p^n distinct roots of f in F. Let $\varphi : F \to F$ be the automorphism of F defined by $x \mapsto x^{p^n}$. If $u \in F$ is a root of f, then $\varphi(u) = u$. By Exercise 4.9.5, the prime field k is fixed by φ. Since F is generated over k by roots of f, F is fixed point-wise by φ. Every u in F is a root of f, and F has order p^n. □

THEOREM 4.5.3. *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) Any two finite fields of order p^n are isomorphic as fields.
(6) F/k is a Galois extension.
(7) 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 $\varphi(x) = x^p$.
(8) 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 $\varphi|_E$.
(9) 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 (8).

PROOF. (1): This was proved in Theorem 4.4.5 (2).

(2): Take u to be a generator for $U(F)$.

(3): As a k-vector space, F is isomorphic to k^n.

(4), (5) and (6): By Theorem 4.4.5, the group of units of F is cyclic of order $p^n - 1$. The polynomial $x^{p^n} - x = x(x^{p^n - 1} - 1)$ has p^n roots in F and they are all simple. Therefore F is the splitting field for the separable polynomial $x^{p^n} - x$ over k. The rest follows from Corollary 4.3.7 and Theorem 4.4.2.

(7): Let $\varphi : F \to F$ be the Frobenius homomorphism, $\varphi(x) = x^p$. For all $i \geq 1$, $\varphi^i(x) = x^{p^i}$. Let G_i denote the subgroup generated by φ^i and let $F_i = F^{G_i}$ be the fixed field of φ^i.

Then $F^{G_i} = \{u \in F \mid x^{p^i} - x = 0\}$ is equal to the set of roots in F of the polynomial $x^{p^i} - x$. For $1 \le i \le n$ the order of the subfield F^{G_i} is less than or equal to p^i. The field F is equal to F^{G_n} and the order of φ is n.

(8) and (9): The proof follows straight from Theorem 4.2.9 and Part (7). □

5.1. Irreducible Polynomials. Throughout this section, p will be a fixed prime number and $\mathbb{F}_p = \mathbb{Z}/p$ is the prime field of order p.

THEOREM 4.5.4. *The factorization of the polynomial $x^{p^n} - x$ in $\mathbb{F}_p[x]$ into irreducible factors is equal to the product of all the monic irreducible polynomials of degree d where d runs through all divisors of n.*

PROOF. Is left to the reader. □

THEOREM 4.5.5. *Let $\psi(n)$ denote the number of distinct monic irreducible polynomials of degree n in $\mathbb{F}_p$.*

(1) If μ is the Möbius function, then $\psi(n) = \dfrac{1}{n}\sum_{d|n}\mu(d)p^{n/d} = \dfrac{1}{n}\sum_{d|n}\mu\left(\dfrac{n}{d}\right)p^d$.

(2) $\psi(n) > \dfrac{p^n}{2n}$.

PROOF. (1): By Theorem 4.5.4, $p^n = \sum_{d|n} d\psi(d)$. Now apply the Möbius Inversion Formula (Theorem 1.2.9).

(2): The reader should verify the identities:

$$\begin{aligned} n\psi(n) &= p^n + \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right)p^d \\ &\ge p^n - \sum_{d|n, d<n} p^d \\ &\ge p^n - \sum_{1 \le d \le n/2} p^d \\ &\ge p^n - p^{\lfloor n/2 \rfloor + 1} \end{aligned}$$

where $\lfloor n/2 \rfloor$ is the greatest integer less than $n/2$. If $n > 2$, then $\lfloor n/2 \rfloor + 1 \le n - 1$, so

$$\psi(n) > \frac{1}{n}\left(p^n - p^{n-1}\right) = \frac{p^n}{n}\left(1 - \frac{1}{p}\right) \ge \frac{p^n}{2n}.$$

If $n = 2$, the formula can be derived from $\psi(2) = (1/2)(p^2 - p)$. □

5.2. Exercises.

EXERCISE 4.5.1. Let K be a finite field of order p^d. As in Theorem 4.5.5, let $\psi(n)$ be the number of irreducible monic polynomials of degree n in $\mathbb{F}_p[x]$. If $d \mid n$, show that there are at least $\psi(n)$ irreducible monic polynomials of degree n/d in $K[x]$.

EXERCISE 4.5.2. Let k be a finite field and K/k a finite dimensional extension of fields, with $\dim_k K = d$. Let n be an arbitrary positive integer and $A = K \oplus \cdots \oplus K$ the direct sum of n copies of K.

1. Show that if there exists a surjective k-algebra homomorphism $f : k[x] \to A$, then there exist at least n distinct irreducible monic polynomials in $k[x]$ of degree d.
2. Find an example of k and A such that the k-algebra A is not the homomorphic image of $k[x]$.

(3) Show that for some integer $m \geq 1$, there exist n distinct irreducible monic polynomials $h_1, \dots, h_n$ in $k[x]$ such that each h_i has degree md.
(4) Show that for some integer $m \geq 1$, if F/k is a finite extension field with $\dim_k F = md$, then the direct sum $F \oplus \cdots \oplus F$ of n copies of F is the homomorphic image of $k[x]$. Show that m can be chosen to be relatively prime to d.
(5) Show that there is a separable polynomial $g \in k[x]$ such that A is isomorphic to a subalgebra of $k[x]/(g)$.

EXERCISE 4.5.3. Let p be a prime number and A a finite ring of order p^2.

(1) Prove that either A is isomorphic to $\mathbb{Z}/(p^2)$, or the characteristic of A is p and A is isomorphic as $\mathbb{Z}/p$-algebras to $(\mathbb{Z}/p)[x]/(\phi)$, for some monic quadratic polynomial ϕ with coefficients in the field $\mathbb{Z}/p$.
(2) Prove that A is commutative.
(3) Prove that A is isomorphic to exactly one of the following four rings:
   (a) $\mathbb{Z}/(p^2)$ (if $\operatorname{char}(A) = p^2$).
   (b) $\mathbb{Z}/p \oplus \mathbb{Z}/p$ (if $\operatorname{char}(A) = p$ and ϕ factors and is separable).
   (c) $(\mathbb{Z}/p)[x]/(x^2)$ (if $\operatorname{char}(A) = p$ and ϕ is a square).
   (d) a finite field of order p^2 (if $\operatorname{char}(A) = p$ and ϕ is irreducible).

6. Separable Closure

Let k be a field of positive characteristic p. Let F/k be an extension of fields and u and element of F which is algebraic over k. We say that u is *purely inseparable* over k in case the irreducible polynomial $\operatorname{Irr.poly}_k(u)$ splits in $F[x]$ and has only one root, namely u. Equivalently, u is purely inseparable over k if and only if there exists $m \geq 1$ such that $\operatorname{Irr.poly}_k(u) = (x-u)^m$ in $F[x]$. If $u \in k$, then $\operatorname{Irr.poly}_k(u) = x - u$, hence u is both purely inseparable over k and separable over k.

LEMMA 4.6.1. *Let F/k be an extension of fields and assume $\operatorname{char} k = p > 0$. Let $u \in F$ and assume u is algebraic over k.*

(1) If u is separable over k and purely inseparable over k, then $u \in k$.
(2) There exists $n \geq 0$ such that u^{p^n} is separable over k.

PROOF. (1): If u is purely inseparable over k, then $\operatorname{Irr.poly}_k(u) = (x-u)^m$. If u is separable over k, then $m = 1$.

(2): If u is separable over k, then take $n = 0$. Let $f = \operatorname{Irr.poly}_k(u)$ and use induction on the degree of f. Assume f is not separable and $d = \deg f > 1$. By Theorem 2.5.13, $f \in k[x^p]$. Therefore, u^p is algebraic over k and the degree of $\operatorname{Irr.poly}_k(u^p)$ is equal to d/p. By induction on d, there is some $n \geq 0$ such that $(u^p)^{p^n}$ is separable over k. □

THEOREM 4.6.2. *Let F/k be an algebraic extension of fields. If*

$$S = \{u \in F \mid k(u) \text{ is separable over } k\},$$

then

(1) S is an intermediate field of F/k,
(2) S/k is separable, and
(3) F/S is purely inseparable.

PROOF. (1) and (2): It is enough to show S is a field. Let α and β be elements of $S - k$. If $f = \operatorname{Irr.poly}_k(\alpha)$, then f is separable and irreducible over k. Likewise, $g = \operatorname{Irr.poly}_k(\beta)$ is separable and irreducible over k. By Theorem 4.4.2, if E is the splitting field over k of

fg, then E/k is a separable extension of fields. Since $k(\alpha, \beta)$ is an intermediate field of E/k, it is itself a separable extension of k. Therefore, S contains $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, α/β.

(3): Let $u \in F - S$. We can assume $\operatorname{char} k = p > 0$. By Lemma 4.6.1, there exists $n > 0$ such that u^{p^n} is separable over k. Then u^{p^n} is in S. Let $\alpha = u^{p^n}$. Consider the polynomial $f = x^{p^n} - \alpha$ in $S[x]$. Then f factors in $F[x]$ as $f = (x-u)^{p^n}$. Since $f(u) = 0$, this proves that u is purely inseparable over S. □

DEFINITION 4.6.3. If F/k is an extension of fields, the *separable closure* of k in F is the field S defined in Theorem 4.6.2. If Ω is an algebraic closure of k, and S is the separable closure of k in Ω, then we call S a *separable closure of k*. We say k is *separably closed*, if k is equal to its separable closure in Ω.

THEOREM 4.6.4. *Let k be a field. The following are equivalent.*

(1) Every irreducible polynomial in $k[x]$ is separable.
(2) The splitting field over k of any polynomial in $k[x]$ is a Galois extension of k.
(3) Every algebraic extension of k is separable over k.
(4) k has characteristic zero or k has positive characteristic p and the Frobenius homomorphism $x \mapsto x^p$ is an automorphism of k.

PROOF. Using Theorem 4.4.2, the reader should verify that (1), (2) and (3) are equivalent.

(3) implies (4): Assume k has positive characteristic p and every algebraic extension of k is separable. Let $\varphi : k \to k$ be the Frobenius homomorphism. Let $\alpha \in k$. We show $\alpha = \varphi(u)$ for some $u \in k$. Consider the polynomial $x^p - \alpha$ in $k[x]$. Let F be an extension of k containing a root u of $x^p - \alpha$. In $F[x]$ we have the factorization $x^p - \alpha = (x-u)^p$. By assumption, F/k is separable, which implies this factorization occurs in $k[x]$. That is, $u \in k$ and $\alpha = \varphi(u)$.

(4) implies (3): Let F/k be an algebraic extension. Let $\alpha \in F - k$. Let $f \in k[x]$ be the irreducible polynomial of α over k. We show that $k(\alpha)$ is a separable extension of k. If $\operatorname{char} k = 0$, it follows from Theorem 2.5.13 that f is separable and we are done. Assume $\operatorname{char} k = p > 0$ and the Frobenius homomorphism $\varphi : k \to k$ is an automorphism of k. By Theorem 2.5.2, $\varphi(f) = g$ is an irreducible polynomial in $k[x]$ such that $\deg g = \deg f$. Since $g(\alpha^p) = (f(\alpha))^p = 0$, we see that $k(\alpha^p)$ is a field extension of k which is an intermediate field of $k(\alpha)/k$ such that $\dim_k(k(\alpha^p)) = \dim_k(k(\alpha))$. It follows that $k(\alpha^p) = k(\alpha)$, hence the Frobenius homomorphism is an automorphism $\varphi : k(\alpha) \to k(\alpha)$. For any $m > 0$, $\varphi^m(x) = x^{p^m}$. Since $k[\alpha] = k(\alpha)$, a typical element in $k(\alpha)$ can be represented in the form $u = \sum_i a_i \alpha^i$ where $a_i \in k$. Therefore $\varphi^m(u) = \sum_i a_i^{p^m}(\alpha^{p^m})^i$ is in $k(\alpha^{p^m})$. This shows $k(\alpha^{p^m}) = k(\alpha)$ for all $m > 0$. Let S be the separable closure of k in $k(\alpha)$. For some $n \geq 0$, $\alpha^{p^n} \in S$. Therefore $k(\alpha) = k(\alpha^{p^n}) \subseteq S$ so $k(\alpha)$ is a separable extension of k. □

EXAMPLE 4.6.5. A field k is called *perfect* if it satisfies one of the statements (1) – (4) in Theorem 4.6.4. The following is a list of fields that are perfect fields.

(1) A field of characteristic zero satisfies Theorem 4.6.4 (4).
(2) An algebraically closed field satisfies Theorem 4.6.4 (1).
(3) By Lemma 4.5.1, a finite field satisfies Theorem 4.6.4 (4).

THEOREM 4.6.6. *(Separable over Separable is Separable) Let $k \subseteq F \subseteq K$ be a tower of algebraic field extensions. If F is separable over k and K is separable over F, then K is separable over k.*

PROOF. If $\operatorname{char} k = 0$, then we are done. Assume $\operatorname{char} k = p > 0$. Let S be the separable closure of k in K. Then $F \subseteq S \subseteq K$. It is enough to show $S = K$. Let $u \in K$. For some $n \geq 0$ we have $\alpha = u^{p^n} \in S$. Then u satisfies the polynomial $x^{p^n} - \alpha \in S[x]$ and in $K[x]$ we have the factorization $x^{p^n} - \alpha = (x-u)^{p^n}$. If $f = \operatorname{Irr.poly}_S(u)$, then f divides $(x-u)^{p^n}$ in $K[x]$. If $g = \operatorname{Irr.poly}_F(u)$, then g is separable and since f divides g in $S[x]$, we know that f has no multiple roots in K. So $f = x - u$ and $u \in S$. □

7. The Trace Map and Norm Map

DEFINITION 4.7.1. Let F/k be a Galois extension with finite group G. For $x \in F$, define

$$T_k^F(x) = \sum_{\sigma \in G} \sigma(x)$$

and

$$N_k^F(x) = \prod_{\sigma \in G} \sigma(x).$$

Note that both T_k^F and N_k^F are mappings from F to k. We call the mapping T_k^F the *trace from F to k*. The trace is k-linear and represents an element of $\operatorname{Hom}_k(F,k)$. The mapping N_k^F is called the *norm from F to k*. The norm induces a homomorphism of multiplicative groups $F^* \to k^*$.

As we have seen already (Example 3.3.3), 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. If F/k is a Galois extension with finite group G, then by Lemma 4.2.5, the trace mapping 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.

EXAMPLE 4.7.2. Suppose F/k is Galois with finite group G. Let $\{a_1, \dots, a_n\}$ be a k-basis for F. For each $j = 1, 2, \dots, n$, let $f_j : F \to k$ be the projection onto coordinate j. That is, $f_j(a_i) = \delta_{ij}$ (Kronecker delta) and $\{(a_j, f_j) \mid j = 1, \dots, n\}$ is a dual basis for F. For each $x \in F$,

$$x = \sum_{j=1}^n f_j(x) a_j.$$

Since T_k^F is a generator for $\operatorname{Hom}_k(F,k)$ over F, there exist unique $y_1, \dots, y_n$ in F such that for each $x \in F$, $f_j(x) = T_k^F(y_j x) = \sum_{\sigma \in G} \sigma(y_j x)$. Combining these facts,

$$\begin{aligned} x &= \sum_{j=1}^n f_j(x) a_j \\ &= \sum_{j=1}^n \sum_{\sigma \in G} \sigma(y_j x) a_j \\ &= \sum_{\sigma \in G} \left(\sigma(x) \sum_{j=1}^n \sigma(y_j) a_j \right). \end{aligned}$$

By Lemma 4.2.6, G is a basis for $\operatorname{Hom}_k(F,F)$ over F. Therefore, $\sum_{j=1}^n \sigma(y_j) a_j = \delta_{\sigma,1}$. We have shown that the elements $a_1, \dots, a_n$ and $y_1, \dots, y_n$ satisfy the conclusion of Lemma 4.2.3.

LEMMA 4.7.3. *Suppose F/k is a Galois extension of fields with finite group G. If H is a normal subgroup of G and $E = F^H$, then $T_k^F = T_k^E \circ T_E^F$ and $N_k^F = N_k^E \circ N_E^F$.*

PROOF. Let $x \in F$. Then

$$\begin{aligned} T_k^E\left(T_E^F(x)\right) &= T_k^E\left(\sum_{\sigma\in H}\sigma(x)\right) \\ &= \sum_{\tau\in G/H}\tau\left(\sum_{\sigma\in H}\sigma(x)\right) \\ &= \sum_{\tau\in G/H}\sum_{\sigma\in H}\tau\sigma(x) \\ &= \sum_{\rho\in G}\rho(x) \\ &= T_k^F(x). \end{aligned}$$

The proof of the second identity is left to the reader. □

For generalizations of Theorem 4.7.4, see [**10**, Theorem 5.1.20].

THEOREM 4.7.4. *(Hilbert's Theorem 90) Let F/k be a Galois extension of fields with finite group G. Assume $G = \langle\sigma\rangle$ is cyclic and $u \in F$. Then*

(1) $T_k^F(u) = 0$ if and only if $u = v - \sigma(v)$ for some $v \in F$.
(2) $N_k^F(u) = 1$ if and only if $u = v/\sigma(v)$ for some $v \in F^*$.

PROOF. Throughout the proof, assume $G = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ and $\sigma^n = 1$.

(1): If $v \in F$, then $T(\sigma(v)) = \sum_{\tau\in G}\tau\sigma(v) = \sum_{\rho\in G}\rho(v) = T(v)$. It follows that $T(v - \sigma(v)) = 0$. Conversely, assume $T(u) = 0$. By Lemma 4.2.5, there exists $w \in F$ with $T(w) = 1$. Starting with

$$\begin{aligned} v = uw + (u+\sigma(u))\sigma(w) + (u+\sigma(u)+\sigma^2(u))\sigma^2(w) + \dots \\ + (u+\sigma(u)+\sigma^2(u)+\dots+\sigma^{n-2}(u))\sigma^{n-2}(w), \end{aligned}$$

apply σ to get

$$\begin{aligned} \sigma(v) = \sigma(u)\sigma(w) + (\sigma(u)+\sigma^2(u))\sigma^2(w) + \dots \\ + (\sigma(u)+\sigma^2(u)+\dots+\sigma^{n-1}(u))\sigma^{n-1}(w). \end{aligned}$$

Subtract $\sigma(v)$ from v. Use the identities $T(u) = u+\sigma(u)+\dots+\sigma^{n-1}(u) = 0$ and $T(w) = 1$ to simplify

$$\begin{aligned} v - \sigma(v) &= uw + u\sigma(w) + u\sigma^2(w) + \dots + u\sigma^{n-2}(w) \\ &\quad - \left(\sigma(u)+\sigma^2(u)+\dots+\sigma^{n-1}(u)\right)\sigma^{n-1}(w) \\ &= u\left((w+\sigma(w)+\sigma^2(w)+\dots+\sigma^{n-2}(w)\right) - (-u)\sigma^{n-1}(w) \\ &= u\left((w+\sigma(w)+\sigma^2(w)+\dots+\sigma^{n-2}(w)+\sigma^{n-1}(w)\right) \\ &= uT(w) = u. \end{aligned}$$

(2): If $v \in F^*$, then $N(\sigma(v)) = \prod_{\tau\in G}\tau\sigma(v) = N(v)$. This shows $N(v/\sigma(v)) = 1$. Conversely, assume $N(u) = 1$. By Lemma 4.2.4, we know that

$$v = ux + u\sigma(u)\sigma(x) + u\sigma(u)\sigma^2(u)\sigma^2(x) + \dots + u\sigma(u)\sigma^2(u)\cdots\sigma^{n-1}(u)\sigma^{n-1}(x)$$

is nonzero for some $x \in F$. In this case, we have

$$u^{-1}v = x + \sigma(u)\sigma(x) + \sigma(u)\sigma^2(u)\sigma^2(x) + \cdots + \sigma(u)\sigma^2(u)\cdots\sigma^{n-1}(u)\sigma^{n-1}(x)$$

and

$$\begin{aligned}\sigma(v) &= \sigma(u)\sigma(x) + \sigma(u)\sigma^2(u)\sigma^2(x) + \cdots + \sigma(u)\sigma^2(u)\cdots\sigma^{n}(u)\sigma^{n}(x)\\ &= \sigma(u)\sigma(x) + \sigma(u)\sigma^2(u)\sigma^2(x) + \cdots + N(u)x\\ &= \sigma(u)\sigma(x) + \sigma(u)\sigma^2(u)\sigma^2(x) + \cdots + x.\end{aligned}$$

This shows $\sigma(v) = u^{-1}v$, hence $u = v/\sigma(v)$. □

7.1. Exercises.

EXERCISE 4.7.1. Let k be a field. Show that for any $n \geq 1$ there exists a polynomial $f \in F[x]$ of degree n such that f has no repeated roots.

EXERCISE 4.7.2. Let F/k be a Galois extension of fields with finite group G. Assume $G = \langle\sigma\rangle$ is cyclic.

(1) Show that the function $D : F^* \to F^*$ defined by $D(u) = u/\sigma(u)$ is a homomorphism of abelian groups.
(2) Show that the kernel of D is k^*, and the image of D is the kernel of $N_k^F : F^* \to F^*$.
(3) If F is a finite field, show that the image of $N_k^F : F^* \to F^*$ is equal to k^*.

8. Cyclic Galois Extensions

We say a finite Galois extension of fields F/k is *cyclic of degree n* if the group $\text{Aut}_k(F)$ is a cyclic group of order n.

EXAMPLE 4.8.1. Let k be a field of positive characteristic p. For any $a \in k$, the polynomial $f = x^p - x - a \in k[x]$ is separable over k. To see this, assume u is a root of f in any extension field F/k. Let $i \in \mathbb{Z}/p$ be any element of the prime field of k. Then $f(u+i) = (u+i)^p - (u+i) - a = u^p + i - u - i - a = f(u) = 0$. Therefore, f has p distinct roots in F, namely $u, u+1, \ldots, u+p-1$.

THEOREM 4.8.2. *(Artin-Schreier) Suppose k is a field of positive characteristic p.*

(1) If F/k is a cyclic Galois extension of degree p, then there exists $a \in k$ such that $f = x^p - x - a$ is an irreducible separable polynomial over k and F is the splitting field for f over k.
(2) If $a \in k$ and $f = x^p - x - a$ is irreducible over k, then
   (a) f is separable,
   (b) $F = k[x]/(f)$ is a splitting field for f,
   (c) F/k is a cyclic Galois extension of k of degree p.

PROOF. (1): Let $G = \text{Aut}_k(F) = \langle\sigma\rangle$. Since G is simple and abelian, there are no proper intermediate fields for F/k. Since $\text{char}(k) = \dim_k(F) = p$, $T_k^F(1) = p = 0$. By Theorem 4.7.4, there is $v \in F$ such that $v - \sigma(v) = 1$. If $u = -v$, then $\sigma(u) = 1 + u$. This shows $u \notin k$, hence $F = k(u)$. Note that $\sigma(u^p) = (\sigma(u))^p = (1+u)^p = 1 + u^p$, and $\sigma(u^p - u) = \sigma(u^p) - \sigma(u) = (1+u^p) - (u+1) = u^p - u$. If $a = u^p - u$, then $a \in k$ and u satisfies the polynomial $f = x^p - x - a$. Since the dimension of $k(u)$ over k is p, this implies f is equal to the irreducible polynomial of u. By Example 4.8.1, f is separable and splits in F.

(2): Suppose $f = x^p - x - a$ is irreducible in $k[x]$. As was shown in Example 4.8.1, f is separable and splits in $F = k[x]/(f)$. By Theorem 4.4.2, F/k is a Galois extension. □

If $\zeta \in k^*$ and ζ generates a subgroup of order n in k^*, then we say ζ is a *primitive nth root of* 1 *in k* and write $\zeta = \sqrt[n]{1}$. There are at most n solutions to $x^n - 1$ in k, so the subgroup $\langle \zeta \rangle$ has $\varphi(n)$ generators. That is, if k contains a primitive nth root of 1, then k contains $\varphi(n)$ primitive nth roots of 1. A cyclic extension F/k of degree n is called a *Kummer extension* if $\sqrt[n]{1} \in k$.

THEOREM 4.8.3. *Let $n > 0$ and assume k is a field containing a primitive nth root of* 1. *The following are equivalent.*

(1) F/k is a cyclic Galois extension of degree d, for some positive divisor d of n.
(2) F is a splitting field over k of $x^n - a$ for some $a \in k^*$.
(3) F is a splitting field over k of $x^d - a$ for some $a \in k^*$ and some positive divisor d of n.

PROOF. Throughout the proof, let $\zeta = \sqrt[n]{1}$ be a primitive nth root of 1 in k.

(2) implies (1): Let α be a root of $x^n - a$ in F. For each $i \geq 0$ we have $\left(\zeta^i \alpha\right)^n = (\zeta^n)^i \alpha^n = a$, so the roots of $x^n - a$ in F are $\{\zeta^i \alpha \mid 0 \leq i < n\}$. This shows $x^n - a$ is separable. Also, since $\zeta \in k$, this implies $F = k(\alpha)$ is a simple extension. If $\sigma \in G = \operatorname{Aut}_k(F)$, then $\sigma(\alpha) = \zeta^i \alpha$ for some i such that $0 \leq i < n$. As σ runs through the nonidentity elements of G, consider the positive numbers i such that $\sigma(\alpha) = \zeta^i \alpha$ and pick the smallest. Fix $\sigma \in G$, such that $\sigma(\alpha) = \zeta^i \alpha$ and i is minimal. We prove that G is generated by σ. Let τ be any element of G. Then $\tau(\alpha) = \zeta^j \alpha$ and we can assume $0 < i \leq j < n$. Dividing, $j = iq + r$, where $0 \leq r < i$. Now $\sigma^q(\alpha) = \zeta^{qi}\alpha$. Therefore, $\sigma^{-q}\tau(\alpha) = \sigma^{-q}(\zeta^j \alpha) = \zeta^j \sigma^{-q}(\alpha) = \zeta^j \zeta^{-qi} \alpha = \zeta^r \alpha$. By the choice of i we conclude that $r = 0$, so $\tau = \sigma^q$. The order of G is equal to the order of ζ^i, which is a divisor of n.

(3) implies (2): Assume F is the splitting field of $x^d - a$ where d is a divisor of n, and $a \in k$. Let $\rho = \zeta^{n/d}$. Then $\rho = \sqrt[d]{1}$. Let $\alpha \in F$ satisfy $\alpha^d = a$. Then $x^d - a$ factors in $F[x]$ as $(x - \alpha)(x - \rho\alpha) \cdots (x - \rho^{d-1}\alpha)$. This implies $F = k(\alpha)$, because $\rho \in k$. Consider the polynomial $x^n - a^{n/d}$. For any i such that $0 \leq i < n$ we see that $\left(\zeta^i \alpha\right)^n = \alpha^n = \left(\alpha^d\right)^{n/d} = a^{n/d}$. So $x^n - a^{n/d}$ splits in F.

(1) implies (3): Assume F/k is cyclic of degree d and that σ is a generator for $G = \operatorname{Aut}_k(F)$. Since $\rho = \zeta^{n/d} = \sqrt[d]{1}$ is in k, the norm of ρ is $N(\rho) = \rho^d = 1$. By Theorem 4.7.4, there is $u \in F^*$ such that $\rho = u/\sigma(u)$. Setting $v = u^{-1}$, we have $\rho = v^{-1}\sigma(v)$, or $\sigma(v) = \rho v$. Then $\sigma(v^d) = (\rho v)^d = v^d$. This says $v^d \in k$ and v satisfies the polynomial $x^d - v^d$. The roots of $x^d - v^d$ are $\{v, \rho v, \ldots, \rho^{d-1} v\}$. Note that $\sigma^i(v) = \rho^i v$, for all i such that $0 \leq i < d$. If f is the irreducible polynomial for v, then f has d roots in F. Therefore $\deg(f) = d$ and $f = x^d - v^d$. We have shown that F is the splitting field of f and $F = k(v)$. □

Let k be a field. We say F is a *cyclotomic extension* of k of order n if F is the splitting field over k of $x^n - 1$. If $\operatorname{char} k = p > 0$, then we can factor $n = p^e m$ where $(m, p) = 1$. Then $x^n - 1 = (x^m)^{p^e} - 1^{p^e} = (x^m - 1)^{p^e}$, so the splitting field of $x^n - 1$ is equal to the splitting field of $x^m - 1$. For this reason, we assume n is relatively prime to $\operatorname{char} k$ and $x^n - 1$ is separable. In Theorem 4.8.4, $\varphi(n)$ denotes the Euler φ function.

THEOREM 4.8.4. *Let F be a cyclotomic extension of k of order n. If* $\operatorname{char} k = p > 1$, *assume* $(n, p) = 1$. *Then*

(1) $F = k(\zeta)$ where ζ is a primitive nth root of 1 *over k.*
(2) F is a Galois extension of k and $\operatorname{Aut}_k(F)$ *is a subgroup of the group of units in* $\mathbb{Z}/n$. *The dimension* $\dim_k(F)$ *is a divisor of* $\varphi(n)$.

PROOF. (1): By assumption, $x^n - 1$ is separable, and the group μ_n of nth roots of unity in F is a cyclic group of order n, by Proposition 4.4.4. Let ζ be a primitive nth root of unity in F. Therefore $F = k(\zeta)$ is a simple extension.

(2): Since F is the splitting field of a separable polynomial, F/k is Galois. The Galois group $G = \operatorname{Aut}_k(F)$ acts on the cyclic group of order n generated by ζ. This defines a homomorphism $G \to \operatorname{Aut}(\langle\zeta\rangle)$. Since $F = k(\zeta)$, this mapping is one-to-one. The order of $\operatorname{Aut}(\langle\zeta\rangle)$ is $\varphi(n)$. □

DEFINITION 4.8.5. Let k be a field and Ω the algebraic closure of k. If F is an intermediate field of Ω/k, we say F is a *radical extension* of k in case there exist elements $u_1, \dots, u_n$ in Ω and positive integers $e_1, \dots, e_n$ such that

(1) $F = k(u_1, \dots, u_n)$,
(2) $u_1^{e_1} \in k$, and
(3) for $1 < i \le n$, $u_i^{e_i} \in k(u_1, \dots, u_{i-1})$.

If $f \in k[x]$, we say f is *solvable by radicals* in case the splitting field of f is contained in a radical extension of k.

LEMMA 4.8.6. *Let F/k be a radical extension of fields. As in Definition 4.3.10, let K be the normal closure of F/k. Then K/k is a radical extension.*

PROOF. First we show that $K = F_1 F_2 \cdots F_m$ where each F_i is an intermediate field of K/k and $F_i \cong F$. We are given $F = k(u_1, \dots, u_n)$ as in Definition 4.8.5. For each i, and for each root α of $\operatorname{Irr.poly}_k(u_i)$, there is a k-algebra isomorphism $\theta : k(u_i) \to k(\alpha)$ which extends by Lemma 4.3.6 to a k-algebra isomorphism $\bar{\theta} : K \to K$. Then $\bar{\theta}(F)$ is an intermediate field of K/k which is k-isomorphic to F and contains α. Since K/k is generated by the roots α of the irreducible polynomials of the elements u_i, there is a finite number of fields of the form $\bar{\theta}(F)$ that generate K.

Let $F_1 = k(u_1, \dots, u_n)$ as in Definition 4.8.5. By the first step, there are isomorphic copies F_i of F_1 such that $K = F_1 F_2 \cdots F_m$. Then $F_2 = k(v_1, \dots, v_n)$ where the v_i are as in Definition 4.8.5. Clearly $F_1 F_2 = k(u_1, \dots, u_n, v_1, \dots, v_n)$ is a radical extension of k. An iterative argument shows that $K = F_1 F_2 \dots F_m$ is a radical extension of k. □

THEOREM 4.8.7. *If F/k is a radical extension of fields, and E is an intermediate field, then* $\operatorname{Aut}_k(E)$ *is solvable.*

PROOF. Step 1: Reduce to the case where $F = E$ and F/k is a Galois extension. Let L be the fixed field $E^{\operatorname{Aut}_k(E)}$. Then E/L is a Galois extension with group $\operatorname{Aut}_k(E) = \operatorname{Aut}_L(E)$. By Theorem 4.4.2, E/L is normal and separable. Let K be the normal closure of F/L. Then K/L and F/L are radical extensions. By Theorem 4.3.9, any $\sigma \in \operatorname{Aut}_L(K)$ maps E to E. There is a homomorphism of groups $\operatorname{Aut}_L(K) \to \operatorname{Aut}_L(E)$ defined by $\sigma \mapsto \sigma|_E$ which is onto since K is a splitting field over L of a set of polynomials. Since the homomorphic image of a solvable group is solvable, it suffices to show that $\operatorname{Aut}_L(K)$ is solvable. Let L_1 be the fixed field $K^{\operatorname{Aut}_K(K)}$. Then K/L_1 is a Galois extension with group $\operatorname{Aut}_{L_1}(K) = \operatorname{Aut}_L(K)$. Since K/k is a radical extension, so is K/L_1. It is enough to prove the result for the radical Galois extension K/L_1.

Step 2: Assume $F = k(u_1, \dots, u_n)$ is a radical extension of k and that F/k is Galois with group G. We prove that G is solvable. For each i, there is n_i such that $u_i^{n_i} \in k(u_1, \dots, u_{i-1})$. If $p = \operatorname{char} k$ is positive, then we factor $n_i = p^t m_i$ such that $(p, m_i) = 1$. In this case, $\left(u_i^{m_i}\right)^{p^t} \in k(u_1, \dots, u_{i-1})$ and since F is separable over $k(u_1, \dots, u_{i-1})$, we see that $u_i^{m_i} \in k(u_1, \dots, u_{i-1})$. From now on we assume $(p, n_i) = 1$. Set $m = n_1 n_2 \cdots n_n$. Since

$(m,p)=1$, the polynomial x^m-1 is separable over k and if ζ is a primitive mth root of unity over k, then $F(\zeta)/k$ is a Galois extension with intermediate field F. Since F/k is Galois, by Theorem 4.2.9, G is the homomorphic image of $\operatorname{Aut}_k(F(\zeta))$. It suffices to show $\operatorname{Aut}_k(F(\zeta))$ is solvable. By Theorem 4.8.4, $k(\zeta)/k$ is a Galois extension with an abelian Galois group. Therefore $\operatorname{Aut}_{k(\zeta)}(F(\zeta))$ is a normal subgroup of $\operatorname{Aut}_k(F(\zeta))$ and since

$$\operatorname{Aut}_k(F(\zeta))/\operatorname{Aut}_{k(\zeta)}(F(\zeta)) \cong \operatorname{Aut}_k(k(\zeta))$$

it suffices to show $\operatorname{Aut}_{k(\zeta)}(F(\zeta))$ is a solvable group. Set $E_0=k(\zeta)$ and for each $i=1,2,\dots,n$ set $E_i=k(\zeta,u_1,\dots,u_i)$. Therefore $E_n=F(\zeta)$ is a Galois extension of each E_i. Let $H_i=\operatorname{Aut}_{E_i}(E_n)$ be the corresponding subgroup of $\operatorname{Aut}_{E_0}(E_n)$. By construction, E_i/E_{i-1} is a Kummer extension, hence is a cyclic Galois extension, by Theorem 4.8.3. Therefore, $H_{i-1}=\operatorname{Aut}_{E_{i-1}}(E_n)$ is a normal subgroup of $H_i=\operatorname{Aut}_{E_i}(E_n)$ and the factor group $H_i/H_{i-1}\cong\operatorname{Aut}_{E_{i-1}}(E_i)$ is a cyclic group. This shows $1=H_n\subseteq H_{n-1}\subseteq\cdots\subseteq H_1\subseteq H_0=\operatorname{Aut}_{k(\zeta)}(F(\zeta))$ is a solvable series. □

9. Exercises

EXERCISE 4.9.1. Let F/k be a purely inseparable finite dimensional extension of fields. Show that $\dim_k(F)=p^n$ for some $n\ge 0$.

EXERCISE 4.9.2. Let $f\in k[x]$ be an irreducible separable polynomial of degree n over the field k. Let F/k be the splitting field for f over k and let $G=\operatorname{Aut}_k(F)$ be the Galois group. We call G the *Galois group* of f. Prove the following.

(1) G acts transitively on the roots of f. That is, given two roots α,β of f, there is $\sigma\in G$ such that $\sigma(\alpha)=\beta$. (Hint: apply Theorem 4.1.5 and Lemma 4.3.6.)
(2) n divides $[G:1]$.

EXERCISE 4.9.3. Let F/k be a Galois extension of fields with finite group G. Let $\{a_1,\dots,a_n\}$ be a k-basis for F. For each j, let f_j be the map in $\operatorname{Hom}_k(F,k)$ which projects onto coordinate j.

(1) If $\alpha\in F$, use the dual basis $\{(a_i,f_i)\mid i=1,\dots,n\}$ to show that the matrix of ℓ_α with respect to the basis $\{a_1,\dots,a_n\}$ is $(f_j(\alpha a_i))$.
(2) Use the results derived in Example 4.7.2 to show that the trace map T_k^F defined in Exercise 3.4.6 is equal to the trace map defined in Definition 4.7.1.

EXERCISE 4.9.4. Let F/k be a Galois extension of fields with finite group G. Let α be an arbitrary element of F, and set

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

(1) Show that $g=\operatorname{char.poly}_k(\alpha)$. (Hint: Show that $g\in k[x]$. The only irreducible factor of g is $\operatorname{Irr.poly}_k(\alpha)$. Use Exercise 3.4.9.)
(2) Show that the trace map T_k^F defined in Exercise 3.4.6 is equal to the trace map defined in Definition 4.7.1.
(3) Show that the norm map N_k^F defined in Exercise 3.4.6 is equal to the norm map defined in Definition 4.7.1.

EXERCISE 4.9.5. If R is a commutative ring, let $\operatorname{Aut}(R)$ denote the group of all ring automorphisms of R. Prove the following.

(1) $\operatorname{Aut}(\mathbb{Z})=(1)$.
(2) $\operatorname{Aut}(\mathbb{Z}/(n))=(1)$ for any n.
(3) $\operatorname{Aut}(\mathbb{Q})=(1)$.

(4) $\operatorname{Aut}(\mathbb{R}) = (1)$.

EXERCISE 4.9.6. Let k be a field and A a matrix in $M_n(k)$. Prove that A is similar to the transpose of A.

EXERCISE 4.9.7. Prove the following for $f = x^3 + x - 1$.

(1) f is irreducible in $\mathbb{Q}[x]$.
(2) If $F = \mathbb{Q}[x]/(f)$ and σ is an automorphism of F, then σ is the identity function.
(3) In $\mathbb{R}[x]$, f factors into a product of a linear polynomial and an irreducible quadratic.
(4) If F is the splitting field of f over $\mathbb{Q}$, then the Galois group $\operatorname{Aut}_{\mathbb{Q}}(F)$ is a nonabelian group of order six.

EXERCISE 4.9.8. Let F be the splitting field of $f = x^3 - 5$ over $\mathbb{Q}$.

(1) Show that the Galois group $\operatorname{Aut}_{\mathbb{Q}}(F)$ is a nonabelian group of order six.
(2) Find all intermediate fields K between $\mathbb{Q}$ and F.
(3) Prove or give a counterexample: Each intermediate field K is a Galois extension of $\mathbb{Q}$.

EXERCISE 4.9.9. Let F be the splitting field of $f = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

(1) Show that the Galois group $\operatorname{Aut}_{\mathbb{Q}}(F)$ is a noncyclic abelian group of order four.
(2) Find all intermediate fields K between $\mathbb{Q}$ and F.
(3) Prove or give a counterexample: Each intermediate field K is a Galois extension of $\mathbb{Q}$.

EXERCISE 4.9.10. Let k be a field, $n \geq 1$ and $a \in k$. Let $f = x^n - a$ and F/k a splitting field for f. Show that the following are equivalent

(1) Every root of f in F is a simple root.
(2) $F[x]/(f)$ is a direct sum of fields.
(3) $n = 1$ or $na \neq 0$.

EXERCISE 4.9.11. Consider the polynomial $f = x^4 + p^2$ in $\mathbb{Q}[x]$, where p is a prime number. Determine the following.

(1) The splitting field of f over $\mathbb{Q}$. Call this field K.
(2) The Galois group of f over $\mathbb{Q}$.
(3) The lattice of intermediate fields of $K/\mathbb{Q}$. Determine which intermediate fields are normal over $\mathbb{Q}$.

EXERCISE 4.9.12. This exercise is a continuation of Exercise 3.1.28. 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

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

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 $N^L_K : L \to K$ restricts to a norm map $N^S_R : S \to R$.

EXERCISE 4.9.13. Suppose K/k is a separable extension of fields. For $i = 1,2$ let F_i be an intermediate field, $k \subseteq F_i \subseteq K$, such that $[F_i : k] = 2$. Prove that F_1 and F_2 are isomorphic as k-algebras if and only if they are equal as sets.

EXERCISE 4.9.14. Let p be a prime number, and F/k an extension of fields which is cyclic of degree p^n. If E is an intermediate field such that $F = E(a)$, and E/k is cyclic of degree p^{n-1}, then $F = k(a)$.

EXERCISE 4.9.15. Let k be a field of positive characteristic p.

(1) The map $a \mapsto a^p - a$ defines a homomorphism of additive groups $\varphi : k \to k$. Prove that a cyclic extension field E/k exists if and only if the map φ is not onto.
(2) In this exercise, we outline a proof that a cyclic extension field E/k can be embedded in a larger cyclic extension field F/k. For the complete classification of cyclic extensions F/k of degree p^n, the interested reader is referred to [**1**]. Assume $n > 1$, E/k is cyclic of degree p^{n-1}, and $\operatorname{Aut}_k(E) = \langle \sigma \rangle$.
   (a) Show that there exists $a, b \in E$ satisfying: $T^E_k(a) = 1$ and $\sigma(b) - b = a^p - a$.
   (b) Show that $x^p - x - a$ is irreducible in $E[x]$.
   (c) Let $F = E[x]/(x^p - x - a)$. Show that F/E is cyclic of degree p and F/k is cyclic of degree p^n.

10. Transcendental Field Extensions

DEFINITION 4.10.1. 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 $\Xi = Z$.

LEMMA 4.10.2. *Let F/k be an extension of fields and Ξ a subset of F which is algebraically independent over k. For $u \in F - k(\Xi)$, the following are equivalent*

(1) $\Xi \cup \{u\}$ is algebraically independent over k.
(2) u is transcendental over $k(\Xi)$.

PROOF. (2) implies (1): Suppose there exist a polynomial f in $k[x_1, \dots, x_n]$ and elements $\xi_1, \dots, \xi_{n-1}$ in Ξ such that $f(\xi_1, \dots, \xi_{n-1}, u) = 0$. Expand f as a polynomial in x_n with coefficients in $k[x_1, \dots, x_{n-1}]$, say $f = \sum_j h_j x_n^j$. Then $0 = f(\xi_1, \dots, \xi_{n-1}, u) = \sum_j h_j(\xi_1, \dots, \xi_{n-1}) u^j$. But u is transcendental over $k(\Xi)$, so $h_j(\xi_1, \dots, \xi_{n-1}) = 0$ for each j. But Ξ is algebraically independent, so each polynomial $h_j = 0$. Thus $f = 0$.

(1) implies (2): Prove the contrapositive. Assume u is algebraic over $k(\Xi)$ and $f = \operatorname{min.poly}_{k(\Xi)}(u) = x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + h_0$. Each h_j is in $k(\Xi)$, so there is a finite subset $\xi_1, \dots, \xi_n$ of Ξ and polynomials $\alpha_0, \dots, \alpha_m$, $\beta_0, \dots, \beta_m$ in $k[x_1, \dots, x_n]$ such that $h_j = \alpha_j(\xi_1, \dots, \xi_n)/\beta_j(\xi_1, \dots, \xi_n)$. Multiply across by the least common multiple, β, of the denominators to get

$$f(x)\beta(\xi_1, \dots, \xi_n) = \sum_j \gamma_j(\xi_1, \dots, \xi_n) x^j$$

where $\beta(\xi_1, \dots, \xi_n) \neq 0$ and each γ_j is in $k[x_1, \dots, x_n]$. Since $(f\beta)(\xi_1, \dots, \xi_n, u) = 0$, we are done. □

LEMMA 4.10.3. *Let F/k be an extension of fields and Ξ a subset of F which is algebraically independent over k. The following are equivalent.*

(1) F is algebraic over $k(\Xi)$.
(2) Ξ is a transcendence base for F over k.

PROOF. (1) implies (2): Suppose Z is linearly independent, $Z \supseteq \Xi$, and $z \in Z$. Then z is algebraic over $k(\Xi)$, so by Lemma 4.10.2, $\Xi \cup \{z\}$ is linearly dependent. Therefore, $z \in \Xi$, which implies $Z = \Xi$.

(2) implies (1): We prove the contrapositive. Suppose $u \in F - k(\Xi)$ and u is transcendental over $k(\Xi)$. Then $\Xi \cup \{u\}$ is algebraically independent, so Ξ is not a transcendence base. □

LEMMA 4.10.4. *Let F/k be an extension of fields.*

(1) If Ξ is a subset of F such that F is algebraic over $k(\Xi)$, then Ξ contains a subset which is a transcendence base for F over k.
(2) If F is a finitely generated field extension of k, then there is a finite transcendence base for F/k.

PROOF. (1): The reader should verify that by Zorn's Lemma, Proposition 1.3.3, the set

$$\{Z \subseteq \Xi \mid Z \text{ is algebraically independent over } k\}$$

contains a maximal member, call it X. Given $u \in \Xi$, by Lemma 4.10.2, u is algebraic over $k(X)$. Then $k(\Xi)$ is algebraic over $k(X)$. By Proposition 4.1.9 (4), F is algebraic over $k(X)$. By Lemma 4.10.3, X is a transcendence base.

(2): Is left to the reader. □

THEOREM 4.10.5. *Let F/k be an extension of fields and assume $\Xi = \{\xi_1, \dots, \xi_n\}$ is a transcendence base for F over k. If Z is another transcendence base for F over k, then Z also has cardinality n.*

PROOF. Step 0: If $n = 0$, then by Exercise 4.10.1, F/k is an algebraic extension. Since Z is algebraically independent over k, we conclude that $Z = \emptyset$. Assume from now on that $n > 0$.

Step 1: There exists $\zeta_1 \in Z$ such that $\zeta_1, \xi_2, \dots, \xi_n$ is a transcendence base for F/k. First we show that there exists $\zeta \in Z$ such that ζ is transcendental over $K = k(\xi_2, \dots, \xi_n)$. Assume the contrary. Then F is algebraic over $K(Z)$ and $K(Z)$ is algebraic over K, hence F is algebraic over K. Then ξ_1 is algebraic over K, which contradicts Lemma 4.10.2. Suppose $\zeta_1 \in Z$ and ζ_1 is transcendental over K. By Lemma 4.10.2, $\{\zeta_1, \xi_2, \dots, \xi_n\}$ is algebraically independent over k. The set $\{\zeta_1, \xi_2, \dots, \xi_n\} \cup \{\xi_1\}$ is algebraically dependent, so Lemma 4.10.2 says ξ_1 is algebraic over $k(\zeta_1, \xi_2, \dots, \xi_n)$. In this case, the field $k(\Xi)(\zeta_1) = k(\zeta_1, \xi_2, \dots, \xi_n)(\xi_1)$ is algebraic over $k(\zeta_1, \xi_2, \dots, \xi_n)$ and F is algebraic over $k(\Xi)(\zeta_1) = k(\zeta_1, \xi_2, \dots, \xi_n)(\xi_1)$, hence F is algebraic over $k(\zeta_1, \xi_2, \dots, \xi_n)$. By Lemma 4.10.3, the set $\zeta_1, \xi_2, \dots, \xi_n$ is a transcendence base for F/k.

Step 2: Iterate Step 1 $n-1$ more times to get a subset $\{\zeta_1, \dots, \zeta_n\}$ of Z which is a transcendence base for F/k. By Definition 4.10.1, this implies $Z = \{\zeta_1, \dots, \zeta_n\}$. □

DEFINITION 4.10.6. Let F/k be an extension of fields such that a finite transcendence base exists. 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.

THEOREM 4.10.7. *Suppose $k \subseteq F \subseteq K$ is a tower of field extensions. Assume $\Xi = \{\xi_1, \dots, \xi_n\}$ is a transcendence base for F/k and $Z = \{\zeta_1, \dots, \zeta_m\}$ is a transcendence base for K/F. Then*

(1) $\Xi \cup Z$ is a transcendence base for K/k, and

(2) $\operatorname{tr.deg}_k(K) = \operatorname{tr.deg}_k(F) + \operatorname{tr.deg}_F(K)$.

PROOF. (2): Follows straight from (1).

(1): The reader should verify that K is algebraic over $k(Z \cup \Xi)(F)$ and $k(Z \cup \Xi)(F)$ is algebraic over $k(Z \cup \Xi)$. Therefore, K is algebraic over $k(Z \cup \Xi)$. Let f be a polynomial in $k[x_1, \dots, x_n][z_1, \dots, z_m]$ such that $f(\xi_1, \dots, \xi_n, \zeta_1, \dots, \zeta_m) = 0$. Since Z is algebraically independent over F, this implies $f(\xi_1, \dots, \xi_n, z_1, \dots, z_m)$ is the zero polynomial in the ring $k(\xi_1, \dots, \xi_n)[z_1, \dots, z_m]$. Therefore, each coefficient of $f(\xi_1, \dots, \xi_n, z_1, \dots, z_m)$ is an algebraic relation over k involving $\xi_1, \dots, \xi_n$. Because $\xi_1, \dots, \xi_n$ are algebraically independent over k, we conclude that $f = 0$. This proves $Z \cup \Xi$ is algebraically independent over k. By Lemma 4.10.3 we are done. □

10.1. Exercises.

EXERCISE 4.10.1. If F/k is an extension of fields, show that $\emptyset$ is a transcendence base if and only if F/k is an algebraic extension.

EXERCISE 4.10.2. If F/k is an extension of fields, and $\Xi \subseteq F$ is algebraically independent over k, show that there exists a transcendence base Z such that $Z \supseteq \Xi$.

EXERCISE 4.10.3. If k is a field, show that $\operatorname{tr.deg}_k k(x_1, \dots, x_n) = n$ and $\{x_1, \dots, x_n\}$ is a transcendence base for $k(x_1, \dots, x_n)$ over k.

EXERCISE 4.10.4. If F is a finitely generated extension field of the field k, show that $\operatorname{tr.deg}_k(F)$ is equal to the least integer n such that there exist $\xi_1, \dots, \xi_n$ in F and F is algebraic over $k(\xi_1, \dots, \xi_n)$.

CHAPTER 5

Modules

1. 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 5.1.1. As in Definition 2.1.9, 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

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{5.1}$$

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 (5.1) 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 (5.1) 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 (5.1) 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 5.1.2. 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

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

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

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

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

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

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 5.5.10).

DEFINITION 5.1.3. 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 $\operatorname{Hom}_{\mathfrak{D}}\big(\mathfrak{F}(M),\mathfrak{F}'(M)\big)$ such that, for every pair of modules M and N in $\mathfrak{C}$ and any $f \in \operatorname{Hom}_{\mathfrak{C}}(M,N)$, 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 5.1.4. 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 5.1.5. Let $\mathfrak{C}$ and $\mathfrak{D}$ be categories of modules and $\mathfrak{F} : \mathfrak{A} \to \mathfrak{C}$ a covariant functor. We say that $\mathfrak{F}$ is *fully faithful* if

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

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

PROPOSITION 5.1.6. *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

$$\operatorname{Hom}_{\mathfrak{D}}\big(\mathfrak{F}(A),\mathfrak{F}(B)\big) \to \operatorname{Hom}_{\mathfrak{C}}\Big(\mathfrak{G}\big(\mathfrak{F}(A)\big),\mathfrak{G}\big(\mathfrak{F}(B)\big)\Big) \tag{5.2}$$

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

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

from which we deduce that $\mathfrak{G}(g)=\mathfrak{G}\big(\mathfrak{F}(f)\big)$. Since (5.2) 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 [**5**, Proposition (1.1), p. 4]. □

2. Progenerator Modules

DEFINITION 5.2.1. Let R be a ring and M an R-module. We say M is a *projective* R-module if M is isomorphic as an R-module to a direct summand of a free R-module.

EXAMPLE 5.2.2. A free module trivially satisfies Definition 5.2.1, hence a free module is a projective module.

PROPOSITION 5.2.3. *Let R be a ring and M an R-module. The following are equivalent.*

(1) M is projective.

(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

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

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

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

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 3.1.11.

(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

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

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 1.3.5). 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 $\gamma\iota$. □

EXAMPLE 5.2.4. Let D be a division ring and $R = M_2(D)$ the ring of two-by-two matrices over D. By Lemma 3.3.7, $\dim_D(R) = 4$. 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 Proposition 3.1.33 that Re_1 and Re_2 are not free R-modules.

EXAMPLE 5.2.5. If $R = M_n(D)$ is the ring of n-by-n matrices over a division ring D, then we will see in Example 7.3.2 that R is a simple artinian ring. By Theorem 7.2.3, every R-module is projective. If $n \geq 2$, then using the method of Example 5.2.4 one can show that R contains left ideals that are not free.

EXAMPLE 5.2.6. Here is a list of rings with the property that every finitely generated projective module is free.

(1) If R is a division ring (in particular, a field) and M is an R-module, then M is a vector space. It follows from Theorem 3.1.28 that M is free.

(2) Let R be a principal ideal domain and M a finitely generated projective R-module. For some $n \geq 1$ there is an exact sequence $R^n \to M \to 0$. By Proposition 5.2.3 this sequence splits, so M is isomorphic to a submodule of R^n. By Theorem 3.2.2, 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 6.4.2.

(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 [**25**, Theorem 4.62]. The same conclusion is true if k is a principal ideal domain [**25**, Theorem 4.63] or [**17**, Theorem V.2.9].

EXAMPLE 5.2.7. 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 5.2.3 (1). But I is not free, since it has only 3 elements. Likewise J is not free.

COROLLARY 5.2.8. *Let R be a ring and M a finitely generated projective R-module. Then M is of finite presentation over R. 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. □

LEMMA 5.2.9. *(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 3.1.32. Moreover, 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 3.1.24, define an onto homomorphism $\pi : R^I \to M$ by $\pi(e_i) = m_i$. By Proposition 5.2.3 (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 3.1.32, 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 5.2.10. *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. As in Definition 3.3.16, we make $\operatorname{Hom}_R(M,R)$ into a right R-module by the action $(fr)(m) = f(m)r$. The rest is left to the reader. □

DEFINITION 5.2.11. 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 5.2.12. *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.

PROOF. Part (1) is Exercise 3.1.2. Part (4) follows from Parts (1), (2) and (3).

(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

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

□

EXAMPLE 5.2.13. 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 5.2.14. 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 5.3.1, S is an integral domain. By Exercise 5.3.2, 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 5.2.9, notice that the splitting of

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

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

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

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

EXAMPLE 5.2.15. 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 $M = (x,y)$ be the maximal ideal of S generated by the images of x and y. By Exercise 5.3.3, S is an integral domain. By Exercise 5.3.4, 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 $m = ax + by$, 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 $\phi_i : M \to R$ 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 5.2.9, 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 $\iota(y-1) = (\frac{-x}{2}, \frac{-y-1}{2})$.

3. Nakayama's Lemma

Let R be a ring, $A \subseteq R$ a left ideal of R, and M an R-module. As in Definition 3.1.4, 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 5.3.1. *(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 5.3.2. *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 5.3.1, $\mathfrak{m}M \neq M$. □

PROPOSITION 5.3.3. *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 $\{(m_i, f_i) \mid 1 \leq i \leq n\}$ 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 5.3.1, $\mathfrak{T}_R(M) + \operatorname{annih}_R(M) = R$. 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 2.1.14, $\mathfrak{T}_R(M) \cap \operatorname{annih}_R(M) = 0$. □

COROLLARY 5.3.4. *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 5.3.3, $\mathfrak{T}_R(M) = R$ 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 5.3.5. *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 5.3.2, $M/A = 0$. □

3.1. Exercises.

EXERCISE 5.3.1. 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 4.9.12 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 $N^S_R : S \to R$ 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^S_R. 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 5.3.2. In what follows, let S be the ring defined in Exercise 5.3.1. 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: 2.3.4 (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: if M were free, it would have rank one.)

EXERCISE 5.3.3. 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 4.9.12 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 $N^S_R : S \to R$ 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 5.3.4. In what follows, let S be the ring defined in Exercise 5.3.3. Any ideal in S is an S-module. Let $M = (x, y-1)$ denote the ideal in S generated by x and y. 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: 2.3.4 (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: if M were free, it would have rank one.)

EXERCISE 5.3.5. Let R be any ring and M an R-module. Suppose there is an infinite exact sequence

$$\cdots \to A_{n+1} \to A_n \to \cdots \to A_2 \to A_1 \to A_0 \to M \to 0 \tag{5.3}$$

of R-modules. If each A_i is a free R-module, then we say (5.3) is a *free resolution* of M. Use Lemma 3.1.24 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 5.3.6. 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

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

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

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

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

EXERCISE 5.3.7. 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

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

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

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

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

EXERCISE 5.3.8. 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 5.3.9. 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 5.3.10. This is a slight generalization of Exercise 5.3.9. 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 5.3.11. 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 5.3.12. 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 5.3.13. Let R be a commutative ring and J an ideal in R. Prove:

(1) If J is a direct summand of R (see Definition 2.2.3), 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 5.3.14. State and prove a version of Exercise 5.3.7 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.

4. Tensor Product

4.1. Tensor Product of Modules and Homomorphisms.

DEFINITION 5.4.1. 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 5.4.2. 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

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

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

THEOREM 5.4.3. *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 5.4.2. 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 $f : M \times N \to C$. Define $h : F \to C$ by $h(x,y) = f(x,y)$. This diagram

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

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 $\phi\left((x,y) + K\right) = f(x,y)$, 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 5.4.2 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

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

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

EXAMPLE 5.4.4. 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 5.4.5. 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 5.4.6. *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. □

LEMMA 5.4.7. *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. □

DEFINITION 5.4.8. 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 5.4.9. 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 as in Example 3.1.2, 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.

LEMMA 5.4.10. *Let R and S be rings. If M and M' are in ${}_S\mathfrak{M}_R$, and N and N' are in ${}_R\mathfrak{M}$, then the following are true.*

(1) If $s \in S$, $m \in M$ and $n \in N$, the multiplication rule $s(m \otimes n) = sm \otimes n$ turns $M \otimes_R N$ into a left S-module.
(2) If $f : M \to M'$ is a homomorphism of left S right R bimodules and $g : N \to N'$ is a homomorphism of left R-modules, then $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ is a homomorphism of left S-modules.

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 is left to the reader.

(2): The reader should verify that $f \otimes g$ is S-linear. □

COROLLARY 5.4.11. *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 5.4.10. □

COROLLARY 5.4.12. *Let R be a commutative ring. If M and M' are R-modules and B is an R-algebra, then the following are true.*

(1) $B \otimes_R M$ is a left B-module under the action $b_1(b_2 \otimes m) = b_1 b_2 \otimes m$.
(2) If $f : M \to M'$ is an R-module homomorphism, then $1 \otimes f : B \otimes_R M \to B \otimes_R M'$ is a B-module homomorphism.

PROOF. This follows from Lemma 5.4.10 since B is a left B right R bimodule. □

LEMMA 5.4.13. *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. □

LEMMA 5.4.14. *(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

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

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

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

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. □

LEMMA 5.4.15. *(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*

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

and

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

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 5.3.6. 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. □

LEMMA 5.4.16. *Let R be a ring and 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. □

4.2. Tensor Functor.

LEMMA 5.4.17. *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 R is a commutative ring and B is an R-algebra, then $B \otimes_R (\cdot)$ defines a covariant functor from ${}_R\mathfrak{M}$ to ${}_B\mathfrak{M}$.*

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 5.4.7, the composition of functions is preserved by tensoring with M.

For Part (2), use Part (1) and Lemma 5.4.10. For Part (3), use Part (1) and Corollary 5.4.11. For Part (4), use Part (1) and Corollary 5.4.12. □

LEMMA 5.4.18. *(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 5.4.7, $(1 \otimes \beta) \circ (1 \otimes \alpha) = 1 \otimes \beta\alpha = 1 \otimes 0 = 0$.

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

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

The reader should verify that f is R-balanced. So there exists a homomorphism γ making the diagram

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

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

DEFINITION 5.4.19. By Lemma 5.4.18 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 5.4.20. 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.

4.2.1. *Tensor Product of Algebras.*

LEMMA 5.4.21. *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 5.4.11 (1), the tensor product of R-modules is an R-module. Using Corollary 5.4.11 (2), 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

$$\begin{aligned} (A \otimes_R B) \otimes_R (A \otimes_R B) &\xrightarrow{\cong} A \otimes_R (B \otimes_R A) \otimes_R B \\ &\xrightarrow{1\otimes\tau\otimes 1} A \otimes_R (A \otimes_R B) \otimes_R B \\ &\xrightarrow{\cong} (A \otimes_R A) \otimes_R (B \otimes_R B) \\ &\xrightarrow{\mu\otimes\nu} A \otimes_R B. \end{aligned} \tag{5.4}$$

Since it is defined by the composition of the homomorphisms in (5.4), 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 $1 \otimes 1$. □

4.2.2. *Modules Under Change of Base Ring.*

THEOREM 5.4.22. *Let $\phi : A \to B$ be a homomorphism of rings. As in Example 5.4.9, 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.

PROOF. (1): Apply Lemmas 5.4.13, 5.4.15, 5.4.17, and 5.4.18.

(2): By Proposition 5.2.3, 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 5.3.11 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 3.1.24 we are done.

(5): Is left to the reader. □

PROPOSITION 5.4.23. *Let R be a commutative ring and let M and N be two R-modules.*

(1) If M and N are finitely generated over R, then so is $M \otimes_R N$.

(2) *If M and N are projective over R, then so is $M \otimes_R N$.*
(3) *If M and N are generators over R, then so is $M \otimes_R N$.*
(4) *If M and N are progenerators over R, then so is $M \otimes_R N$.*

PROOF. (1): We are given exact sequences

$$R^{(m)} \xrightarrow{\alpha} M \to 0 \tag{5.5}$$

and

$$R^{(n)} \xrightarrow{\beta} N \to 0. \tag{5.6}$$

Tensor (5.5) with $(\cdot) \otimes_R N$ to get the exact sequence

$$R^{(m)} \otimes_R N \xrightarrow{\alpha \otimes 1} M \otimes_R N \to 0. \tag{5.7}$$

Tensor (5.6) with $R^{(m)} \otimes_R (\cdot)$ to get the exact sequence

$$R^{(m)} \otimes_R R^{(n)} \xrightarrow{1 \otimes \beta} R^{(m)} \otimes_R N \to 0. \tag{5.8}$$

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 5.5.1 (1) there are exact sequences

$$M^{(m)} \xrightarrow{\alpha} R \to 0 \tag{5.9}$$

and

$$N^{(n)} \xrightarrow{\beta} R \to 0. \tag{5.10}$$

Tensor (5.9) with $(\cdot) \otimes_R N^{(n)}$ to get the exact sequence

$$M^{(m)} \otimes_R N^{(n)} \xrightarrow{\alpha \otimes 1} R \otimes_R N^{(n)} \to 0. \tag{5.11}$$

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). □

PROPOSITION 5.4.24. *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 5.3.11 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 3.1.24 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 5.4.18,

$$F_2 \otimes_R N \xrightarrow{f_2 \otimes 1} M \otimes_R N \to 0$$

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 5.4.14 and Lemma 5.4.15 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 5.3.11 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 5.3.11 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 5.4.6,

$$M \otimes_R N \otimes_R F \xrightarrow{f \otimes 1} M \to 0$$

is split exact. If $M \otimes_R N$ is projective, then by Lemma 5.4.15 and Exercise 5.3.8, M is projective. If $M \otimes_R N$ is finitely generated, then so is M. The other cases are left to the reader. □

4.3. Exercises.

EXERCISE 5.4.1. Assume A is a $\mathbb{Z}$-module and $m > 0$. Prove that $A \otimes_{\mathbb{Z}} \mathbb{Z}/m \cong A/mA$.

EXERCISE 5.4.2. 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 5.4.3. 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 $y' \in N'$. See Lemma 6.9.7 for a generalization of this result.

EXERCISE 5.4.4. 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 5.4.5. 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 5.4.6. Let

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{5.12}$$

be a short exact sequence of left R-modules. Given a right R-module M, consider the sequence

$$0 \to M \otimes_R A \xrightarrow{1\otimes\alpha} M \otimes_R B \xrightarrow{1\otimes\beta} M \otimes_R C \to 0. \tag{5.13}$$

Prove:

(1) If (5.12) is split exact, then (5.13) is split exact.
(2) If M is a free right R-module, then (5.13) is exact, hence M is flat.
(3) If M is a projective right R-module, then (5.13) is exact, hence M is flat.

EXERCISE 5.4.7. If R is any ring and M is an R-module, use Exercise 5.4.6 and Exercise 5.3.5 to show that M has a *flat resolution*.

EXERCISE 5.4.8. 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 submodule generated by $\{rx \mid r \in I, x \in B\}$ as defined in Definition 3.1.4.

EXERCISE 5.4.9. 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 5.4.10. 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

$$\begin{tikzcd} & A \otimes_R B & \\ A \arrow[ur, "\rho_1"] & & B \arrow[ul, "\rho_2"'] \\ & R \arrow[ul, "\theta_1"] \arrow[ur, "\theta_2"'] & \end{tikzcd} \tag{5.14}$$

commutes. Show that $\operatorname{im}(\rho_1)$ commutes with $\operatorname{im}(\rho_2)$. 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 $\operatorname{im}(\alpha)$ commutes with $\operatorname{im}(\beta)$. Show that there exists a unique R-algebra homomorphism $\gamma : A \otimes_R B \to C$ such that the diagram

$$\begin{tikzcd} & C & \\ A \arrow[ur, "\alpha"] \arrow[r, "\rho_1"'] & A \otimes_R B \arrow[u, dotted, "\exists\gamma"'] & B \arrow[ul, "\beta"'] \arrow[l, "\rho_2"] \end{tikzcd} \tag{5.15}$$

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 (5.15) commutes.

EXERCISE 5.4.11. 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 5.4.12. 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 5.4.13. Let A be an R-algebra. Show that $A \otimes_R R[x] \cong A[x]$ as R-algebras.

EXERCISE 5.4.14. 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 5.4.15. 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 5.4.16. 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 5.5.11.)

EXERCISE 5.4.17. 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 5.4.6 and Exercise 5.4.16, 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 5.4.18. Let R be a commutative ring and S a commutative R-algebra. Let A be an S-algebra. Using Exercise 5.4.16, show that there is a well defined epimorphism of rings $A \otimes_R A \to A \otimes_S A$.

EXERCISE 5.4.19. Prove that if A is an R-algebra, then $A \otimes_R M_n(R) \cong M_n(A)$ as R-algebras.

EXERCISE 5.4.20. 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 3.2.4).

EXERCISE 5.4.21. 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 12.4.4.

5. 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 5.5.1 lists four such possibilities.

LEMMA 5.5.1. *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:

$$(fg)(x) = f(g(x)).$$

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 5.3.1 (Nakayama's Lemma).

COROLLARY 5.5.2. *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 5.3.1, $I + \operatorname{annih}_{R[x]} M = R[x]$. 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 5.5.3. *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 5.3.2 (Corollary to Nakayama's Lemma) implies $C = 0$. □

5.1. Hom Functor.

LEMMA 5.5.4. *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 5.5.5. *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

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{5.16}$$

in ${}_R\mathfrak{M}$, we prove that the corresponding sequence

$$0 \to \operatorname{Hom}_R(M,A) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_R(M,B) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_R(M,C) \tag{5.17}$$

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 (5.16) 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. □

A partial converse to Proposition 5.5.5 (3) is

LEMMA 5.5.6. *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 5.5.5 (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. □

5.2. Various Identities Involving the Hom Functor.

LEMMA 5.5.7. *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 5.5.1 (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. □

PROPOSITION 5.5.8. *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 5.3.6 there exists a unique f such that the diagram

$$\begin{tikzcd}
M_j \arrow[r, "\iota_j"] \arrow[dr, "g(j)"'] & \bigoplus_{i\in I} M_i \arrow[d, dotted, "\exists! f"] \\
& N
\end{tikzcd}$$

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 5.3.7.) □

COROLLARY 5.5.9. *(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.

5.3. 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 5.5.10. *(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 $\mathrm{Hom}_S(B,C)$ into a left R-module by $(rf)(b) = f(br)$. Let $f \in \mathrm{Hom}_S(B \otimes_R A, C)$. 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 $A \to \mathrm{Hom}_S(B,C)$. This map is additive in f so ψ is well defined. Conversely, say $g \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C))$. 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 $\phi(g) \in \mathrm{Hom}_S(B \otimes_R A, C)$ 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 5.5.11. *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*

$$\mathrm{Hom}_S(B,C) \otimes_R A \xrightarrow{\alpha} \mathrm{Hom}_S(\mathrm{Hom}_R(A,B),C)$$

of abelian groups. On generators, the map is defined by $\alpha(f \otimes a)(g) = f(g(a))$.

PROOF. Note that $\mathrm{Hom}_S(B,C)$ is a right R-module by the action $(fr)(b) = f(rb)$ and $\mathrm{Hom}_R(A,B)$ is a right S-module by the action $(gs)(a) = g(a)s$. Given any (f,a) in $\mathrm{Hom}_S(B,C) \times A$, define $\phi(f,a) \in \mathrm{Hom}_S(\mathrm{Hom}_R(A,B),C)$ 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

$$\begin{tikzcd}
\mathrm{Hom}_S(B,C) \otimes_R A \arrow[r, "\alpha"] \arrow[d, "1\otimes\psi"] & \mathrm{Hom}_S(\mathrm{Hom}_R(A,B),C) \arrow[d, "\mathrm{H}(\mathrm{H}(\psi))"] \\
\mathrm{Hom}_S(B,C) \otimes_R A' \arrow[r, "\alpha"] & \mathrm{Hom}_S(\mathrm{Hom}_R(A',B),C)
\end{tikzcd}$$

commutes. If $A = R$, then by Lemma 5.5.7 we see that α is an isomorphism. If $A = R^n$ is finitely generated and free, then use Lemma 5.5.9 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 5.5.12. *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*

$$\mathrm{Hom}_A(M,M') \otimes_R \mathrm{Hom}_B(N,N') \xrightarrow{\psi} \mathrm{Hom}_{A\otimes_R B}(M \otimes_R N, M' \otimes_R N')$$

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. Define $\rho : \mathrm{Hom}_A(M,M') \times \mathrm{Hom}_B(N,N') \to \mathrm{Hom}_{A\otimes_R B}(M \otimes_R N, M' \otimes_R N')$ 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 5.5.7, 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 5.5.9, Lemma 5.4.15 and Case 1, both sides are naturally isomorphic to $(M' \otimes_R N')^{(mn)}$.

Case 3: The general case. By Proposition 5.2.3 (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 5.5.9 and Lemma 5.4.15

$$\operatorname{Hom}_A(F,M') \otimes_R \operatorname{Hom}_B(G,N') = \big(\operatorname{Hom}_A(M,M') \otimes_R \operatorname{Hom}_B(N,N')\big) \oplus H \tag{5.18}$$

is an internal direct sum of the left hand side for some submodule H. Likewise,

$$\operatorname{Hom}_{A\otimes_R B}(F \otimes_R G, M' \otimes_R N') = \operatorname{Hom}_{A\otimes_R B}(M \otimes_R N, M' \otimes_R N') \oplus H' \tag{5.19}$$

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 (5.18) and (5.19). The restriction of Ψ gives the desired isomorphism ψ. □

COROLLARY 5.5.13. *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 5.5.14. *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 $N = N'$. □

THEOREM 5.5.15. *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 5.5.1, $\operatorname{Hom}_A(L,M)$ 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 5.5.7, 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 5.5.9, Lemma 5.4.15 and Case 1, both sides are naturally isomorphic to $(M \otimes_R N)^{(n)}$.

Case 3: The general case. By Proposition 5.2.3 (1), we can write $L \oplus K \cong F$ where F is a free A module of rank n. Using Lemma 5.5.9 and Lemma 5.4.15

$$\operatorname{Hom}_A(F,M) \otimes_B N = \operatorname{Hom}_A(L,M) \otimes_R N \oplus H \tag{5.20}$$

is an internal direct sum of the left hand side for some submodule H. Likewise,

$$\operatorname{Hom}_A(F,M \otimes_B N) = \operatorname{Hom}_A(L,M \otimes_R N) \oplus H' \tag{5.21}$$

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 (5.20) and (5.21). The restriction of Ψ gives the desired isomorphism ψ. □

5.4. Exercises.

EXERCISE 5.5.1. 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 [**5**, 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 5.3.11.

EXERCISE 5.5.2. 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.

EXERCISE 5.5.3. 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, $\mathrm{H}_\phi : \mathrm{Hom}_R(B,M) \to \mathrm{Hom}_R(A,M)$ is an isomorphism.

EXERCISE 5.5.4. Let R be a commutative ring and M a finitely generated R-module. Let $\phi \in \mathrm{Hom}_R(M,M)$. Show that there exists a monic polynomial $p(x) \in R[x]$ such that $p(\phi) = 0$. (Hint: lift ϕ to a homomorphism in $\mathrm{Hom}_R(R^n,R^n)$ and use Cayley-Hamilton (Theorem 3.4.12).)

EXERCISE 5.5.5. Let R be a ring. Show that there exists an isomorphism of rings $\mathrm{Hom}_R(R,R) \cong R^o$, where R is viewed as a left R-module and R^o denotes the opposite ring.

EXERCISE 5.5.6. 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 5.5.7. Let R be a ring, M a left R-module, and N a right R-module. Prove the following:

(1) $M^* = \mathrm{Hom}_R(M,R)$ is a right R-module by the formula given in Lemma 5.5.1 (2).
(2) $N^* = \mathrm{Hom}_R(N,R)$ is a left R-module by the rule $(rf)(x) = rf(x)$.
(3) Let $M^{**} = \mathrm{Hom}_R(M^*,R)$ be the double dual of M (see Definition 3.3.21). 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 5.5.8. Let R be a ring. We say a left R-module M is *reflexive* in case the homomorphism $M \to M^{**}$ of Exercise 5.5.7 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) If P is a finitely generated projective R-module and M is a reflexive R-module, then $P \otimes_R M$ is reflexive.

EXERCISE 5.5.9. Let A be a finite abelian group. Prove that $\mathrm{Hom}_{\mathbb{Z}}(A,\mathbb{Z}) = (0)$. Conclude that A is not a reflexive $\mathbb{Z}$-module.

EXERCISE 5.5.10. Let R be a PID and A a finitely generated torsion R-module. Prove that $\mathrm{Hom}_R(A,R) = (0)$. Conclude that A is not a reflexive R-module.

EXERCISE 5.5.11. Exercise 5.4.16 shows how the tensor group behaves when the ring in the middle is changed. The dual result for Hom groups is the object of this exercise. 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. Show that θ induces a well defined $\mathbb{Z}$-module monomorphism $\mathrm{Hom}_S(M,N) \to \mathrm{Hom}_R(M,N)$.

6. Injective Modules

Throughout this section, R will be an arbitrary ring. Unless otherwise specified, an R-module is a left R-module.

DEFINITION 5.6.1. Let R be a ring and E an R-module. Then E is *injective* if for any diagram of R-modules

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & A \arrow[u, "\phi"] \arrow[r, "\alpha"] & B \arrow[ul, dotted, "\exists\psi"'] \end{tikzcd}$$

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

THEOREM 5.6.2. *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. □

PROPOSITION 5.6.3. *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.

$$\begin{tikzcd} & \prod_i E_i \arrow[r, "\pi_i"] & E_i \\ 0 \arrow[r] & A \arrow[u, "\phi"] \arrow[r, "\alpha"] & B \arrow[u, dotted, "\exists\psi_i"'] \end{tikzcd}$$

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. □

LEMMA 5.6.4. *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 1.3.3, $\mathscr{S}$ 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. □

DEFINITION 5.6.5. 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 5.6.6. 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.

LEMMA 5.6.7. *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 5.6.4, 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 5.6.4, 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 $\tau(1) = x$. □

LEMMA 5.6.8. *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 5.6.6, $\mathbb{Q}$ is divisible and by Exercises 5.6.1 and 5.6.2, $\mathbb{Q}^I/K$ is divisible. □

LEMMA 5.6.9. *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 5.5.10) 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 5.6.2. 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 5.6.7 and Theorem 5.6.2, 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. □

PROPOSITION 5.6.10. *Every left R-module M is isomorphic to a submodule of an injective R-module.*

PROOF. By Lemma 5.5.7 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 5.6.8, there is a one-to-one homomorphism of abelian groups $\sigma : M \to D$ for some divisible abelian group D. By Proposition 5.5.5, 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 5.6.9, we are done. □

PROPOSITION 5.6.11. *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 5.6.1 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 5.6.10, 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 5.6.3, E is injective. □

6.1. Exercises.

EXERCISE 5.6.1. Prove that if A is a divisible abelian group and $B \subseteq A$ is a subgroup, then A/B is divisible.

EXERCISE 5.6.2. 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 5.6.3. 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 5.6.4. Let R be any ring and M an R-module. Suppose there is an infinite exact sequence

$$0 \to M \to E^0 \to E^1 \to E^2 \to \cdots \to E^n \to E^{n+1} \to \cdots \tag{5.22}$$

of R-modules. If each E^i is an injective R-module, then we say (5.22) is an *injective resolution* of M. Use Proposition 5.6.10 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 5.6.5. Prove that if D is a division ring, then any nonzero vector space over D is an injective D-module.

EXERCISE 5.6.6. 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 5.6.12. *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 5.5.10, this functor is naturally isomorphic to $\operatorname{Hom}_R(\cdot, \operatorname{Hom}_S(M,I))$, which is also exact. By Theorem 5.6.2, $\operatorname{Hom}_S(M,I)$ is injective. □

DEFINITION 5.6.13. 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 5.6.14. *The $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is a cogenerator for ${}_\mathbb{Z}\mathfrak{M}$.*

PROOF. By Example 5.6.6 and Exercise 5.6.1, $\mathbb{Q}/\mathbb{Z}$ is a divisible abelian group. By Lemma 5.6.7, $\mathbb{Q}/\mathbb{Z}$ 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 $\operatorname{Hom}_\mathbb{Z}(M, \mathbb{Q}/\mathbb{Z})$. □

DEFINITION 5.6.15. 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 5.6.16. *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 5.6.2, the second sequence is exact. Conversely, it is enough to assume

$$\operatorname{Hom}_\mathbb{Z}(C, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\beta} \operatorname{Hom}_\mathbb{Z}(B, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_\mathbb{Z}(A, \mathbb{Q}/\mathbb{Z}) \tag{5.23}$$

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 5.6.14, 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 5.6.14, 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 (5.23) 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. □

THEOREM 5.6.17. *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 5.6.12 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 5.6.2, the functor $\operatorname{Hom}_R(\cdot, \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}))$ is exact. By Theorem 5.5.10, 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 5.6.16, $0 \to M \otimes_R A \to M \otimes_R B$ is an exact sequence of $\mathbb{Z}$-modules. This proves M is flat. □

THEOREM 5.6.18. *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 5.4.6 and of finite presentation by Corollary 5.2.8.

Assume M is flat and of finite presentation over R. Then M is finitely generated, so by Proposition 5.5.5 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 5.6.16, it is enough to show that

$$0 \to \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M, B), \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M, A), \mathbb{Q}/\mathbb{Z}) \tag{5.24}$$

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

$$F_1 \to F_0 \to M \to 0. \tag{5.25}$$

Suppose $B \in {}_R\mathfrak{M}_{\mathbb{Z}}$. Suppose $E \in \mathfrak{M}_{\mathbb{Z}}$ is injective. Consider the diagram

$$\begin{tikzcd}
\operatorname{Hom}_{\mathbb{Z}}(B,E) \otimes_R F_1 \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_{\mathbb{Z}}(B,E) \otimes_R F_0 \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_{\mathbb{Z}}(B,E) \otimes_R M \arrow[r] \arrow[d, "\alpha"] & 0 \\
\operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(F_1,B),E) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(F_0,B),E) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,B),E) \arrow[r] & 0
\end{tikzcd}$$

The top row is obtained by tensoring (5.25) with $\operatorname{Hom}_{\mathbb{Z}}(B,E)$, hence it is exact. The bottom row is exact because it comes from (5.25) 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 5.5.11, so the diagram commutes. The two left-most vertical maps are isomorphisms, by Lemma 5.5.11. The Five Lemma (Theorem 5.7.1) 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

$$\begin{tikzcd}
0 \to \operatorname{Hom}_{\mathbb{Z}}(B,\mathbb{Q}/\mathbb{Z}) \otimes_R M \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_{\mathbb{Z}}(A,\mathbb{Q}/\mathbb{Z}) \otimes_R M \arrow[d, "\alpha"] \\
0 \to \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,B),\mathbb{Q}/\mathbb{Z}) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Hom}_R(M,A),\mathbb{Q}/\mathbb{Z})
\end{tikzcd}$$

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 (5.24), so we are done. □

7. Some Homological Algebra

7.1. The Five Lemma.

THEOREM 5.7.1. *(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. □

7.2. The Snake Lemma. We now prove what is perhaps the most fundamental tool in homological algebra, the so-called Snake Lemma.

THEOREM 5.7.2. *(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 that g_1^* is well-defined. 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 $\partial(f_2(y)) \equiv x \pmod{\operatorname{im}\alpha}$. □

8. Direct Limits and Inverse Limits

8.1. The Direct Limit.

DEFINITION 5.8.1. 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 5.8.2. 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

$$\begin{tikzcd}
\varinjlim A_i \arrow[rr, dotted, "\beta"] & & X \\
& A_i \arrow[ul, "\alpha_i"'] \arrow[ur, "f_i"] \arrow[d, "\phi^i_j"] & \\
& A_j \arrow[uul, "\alpha_j"] \arrow[uur, "f_j"'] &
\end{tikzcd}$$

commute for all $i \leq j$ in I.

PROPOSITION 5.8.3. *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 $i \le k$ and $j \le k$ 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 $i \le m$, $j \le m$, $j \le n$, $k \le n$, 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 $m \le p$ and $n \le p$. 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 $i \le k$ and $j \le k$, 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 $i \le j$ 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 $i \le j$, $f_i = f_j \phi^i_j$. Suppose $x \in A_i$ and $y \in A_j$ are related. Then there exists $k \in I$ such that $i \le k$, $j \le k$ 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 5.8.2, so $L = \varinjlim A_i$.

Mimic the uniqueness part of the proof of Theorem 5.4.3 to prove that the direct limit is unique. □

COROLLARY 5.8.4. *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. □

LEMMA 5.8.5. *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 $k \ge i$ such that $\phi^i_k(x) = 0$ in A_k.*

PROOF. This follows straight from the construction in Proposition 5.8.3. Namely, $x \sim 0$ if and only if there exists $k \ge i$ such that $\phi^i_k(x) = 0$ in A_k. □

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 $i \le j$. 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 5.8.6. *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 5.8.3.

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 5.8.5 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 5.8.5 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 5.8.7. *In the context of Theorem 5.8.6,*

$$\varinjlim (A_i \oplus B_i) \cong \left(\varinjlim A_i\right) \oplus \left(\varinjlim B_i\right)$$

8.1.1. *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 5.8.4. 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 5.4.17 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 5.8.8. *In the above context, $\varinjlim M_i \otimes_{R_i} N_i = M \otimes_R N$.*

PROOF. By Exercise 5.4.17 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 5.8.2. 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 5.4.3, β is unique and satisfies $\beta\alpha_i = f_i$. □

8.1.2. *Direct Limits and Adjoint Pairs.*

THEOREM 5.8.9. *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 5.8.2. 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

$$\begin{tikzcd}
\varinjlim A_i \arrow[rr, dotted, "\theta"] & & GX \\
& A_i \arrow[ul, "\alpha_i"'] \arrow[ur, "\psi f_i"] \arrow[d, "\phi^i_j"] & \\
& A_j \arrow[uul, "\alpha_j"] \arrow[uur, "\psi f_j"'] &
\end{tikzcd}$$

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. □

COROLLARY 5.8.10. *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 5.8.8. We give a second proof based on Theorem 5.8.9. View M as a left $\mathbb{Z}$ right R bimodule. By Theorem 5.5.10, Tensor-Hom, $(M\otimes_R(\cdot), \operatorname{Hom}_{\mathbb{Z}}(M,\cdot))$, is an adjoint pair. □

8.2. The Inverse Limit.

DEFINITION 5.8.11. 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 5.8.12. 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

$$\begin{tikzcd}
\varprojlim A_i \arrow[dr, "\alpha_i"] \arrow[ddr, "\alpha_j"'] & & X \arrow[ll, dotted, "\beta"'] \arrow[dl, "f_i"'] \arrow[ddl, "f_j"] \\
& A_i & \\
& A_j \arrow[u, "\phi_i^j"'] &
\end{tikzcd}$$

commute for all $i \leq j$ in I.

PROPOSITION 5.8.13. *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 5.8.12, so $L = \varprojlim A_i$.

Mimic the uniqueness part of the proof of Theorem 5.4.3 to prove that the inverse limit is unique. □

COROLLARY 5.8.14. *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 5.8.15. *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 5.8.9. 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 5.8.16. *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*

$$\operatorname{Hom}_R(M, \varprojlim A_i) \cong \varprojlim \operatorname{Hom}_R(M, A_i).$$

PROOF. We view M as a left R right $\mathbb{Z}$ bimodule. By Theorem 5.5.10, Tensor-Hom, $(M \otimes_{\mathbb{Z}} (\cdot), \operatorname{Hom}_R(M, \cdot))$, is an adjoint pair. □

EXAMPLE 5.8.17. 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

$$\begin{tikzcd} M \arrow[r, "h_2"] \arrow[d, "h_1"'] & M_2 \arrow[d, "f_2"] \\ M_1 \arrow[r, "f_1"] & M_3 \end{tikzcd} \tag{5.26}$$

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 (5.26). 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 (5.26) 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 $A = \{(x_1,x_2) \in A_1 \oplus A_2 \mid f_1(x_1) = f_2(x_2)\}$.

8.3. 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 5.8.13, 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 5.8.18. *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, $x_{n+1} = (\phi_{n+1})^{-1}(x_n - y_n)$. □

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 5.8.19. *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 5.8.18, the leftmost vertical map is onto. The rest of the proof follows from Theorem 5.7.2 and Lemma 5.8.18. □

8.3.1. *The I-adic completion of a module.*

DEFINITION 5.8.20. 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 $x_1 x_2 \cdots x_n$ 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 5.8.12, 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 5.8.21. *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 $\cap I^nM = 0$.*

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 $\cap I^n M = 0$. □

PROPOSITION 5.8.22. *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 5.8.14, $\hat{R}$ is a commutative ring. For each i, let $\alpha_i : \hat{R} \to R/I^i$ and $\beta_i : \hat{M} \to M/I^i M$ be the natural maps. Then

$$\alpha_i \otimes \beta_i : \hat{R} \otimes_{\mathbb{Z}} \hat{M} \to R/I^i \otimes_{\mathbb{Z}} M/I^i M$$

is a well defined R-module homomorphism. Since $M/I^i M$ is a module over R/I^i, let

$$\mu_i : R/I^i \otimes_{\mathbb{Z}} M/I^i M \to M/I^i M$$

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. □

8.4. Exercises.

EXERCISE 5.8.1. 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 rings. State a version of Theorem 2.5.2 for $R[X]$.

EXERCISE 5.8.2. 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 5.8.3. 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 5.8.4. 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 5.8.5. 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 5.8.6. 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 5.8.7. 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 5.8.12.)

EXERCISE 5.8.8. 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 5.8.9. 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 5.8.8, 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 5.8.10. 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 5.8.11. 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 5.3.6, 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 5.8.2, 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 5.8.12. 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 5.3.7, there exists $d : \prod_{k\in I} M_k \to \prod_{(i,j)\in\Xi} M_i$. Use Proposition 5.8.13 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 5.8.13. 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 5.8.11 (3). Apply the functor $\operatorname{Hom}_R(\cdot, M)$. Use Proposition 5.5.8 and Exercise 5.8.12.)

EXERCISE 5.8.14. 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 5.8.15. 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 5.8.16. 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 5.8.17. (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 5.8.18. Let R be a ring and $\{A_i, \phi_j^i\}$ 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 5.5.12, 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 5.8.19. Let R be a commutative ring and $\{A_i, \phi_j^i\}$ 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 5.8.20. 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 9.3.5 for an application of this result.

EXERCISE 5.8.21. In the context of the pullback diagram (5.26), 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 5.8.22. 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 5.8.23. 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.

9. The Morita Theorems

9.1. 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 5.5.1 (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 $sm = s(m)$ and under this operation M is a left R left S bimodule. By Lemma 5.5.1 (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 $M^* \otimes_S M$. Moreover $M^* \otimes_R M$ 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 5.9.1. *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 5.2.9, 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 5.2.11).

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. □

9.2. 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 5.9.1, M is a left R left S bimodule. A slight variation of Lemma 5.4.17 (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 5.9.2. *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 5.9.1 (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 5.9.1 (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 ${}_S\mathfrak{M}$. □

COROLLARY 5.9.3. *In the setting of Theorem 5.9.2, 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 5.1.6 applied to the functor $(\,)\otimes_R M$ says that for any two right R-modules A and B, the assignment

$$\operatorname{Hom}_R(A,B)\to \operatorname{Hom}_S(A\otimes_R M, B\otimes_R M) \tag{5.27}$$

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 (5.27) with $A=B=R$. For (2), use (5.27) 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 5.1.6 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

$$\operatorname{Hom}_S(C,D)\to \operatorname{Hom}_R(M^*\otimes_S C, M^*\otimes_S D) \tag{5.28}$$

is a one-to-one correspondence. By Lemma 5.5.7, M is isomorphic to $\operatorname{Hom}_S(S,M)$. By (5.28) 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 (5.28) 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 5.5.5, $S^o\cong \operatorname{Hom}_S(S,S)$ 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 5.9.1 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

$$\begin{aligned} R &\cong M^*\otimes_S M\\ &\cong M^*\otimes_S \operatorname{Hom}_R(M^*,R)\\ &\cong \operatorname{Hom}_R(M^*,R)\otimes_{S^o} M^*\\ &\cong \operatorname{Hom}_R(M^*,R)\otimes_{\operatorname{Hom}_R(M^*,M^*)} M^* \end{aligned} \tag{5.29}$$

and

$$
\begin{aligned}
\operatorname{Hom}_{R^o}(M^*,R^o)\otimes_{R^o} M^* &\cong M^*\otimes_R \operatorname{Hom}_R(M^*,R)\\
&\cong M^*\otimes_R M\\
&\cong S\\
&\cong \operatorname{Hom}_R(M^*,M^*)\\
&\cong \operatorname{Hom}_{R^o}(M^*,M^*)
\end{aligned}
\tag{5.30}
$$

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 5.9.1 with M^* in place of M, we see that M^* is an R-generator by (5.29) and a finitely generated and projective left R^o-module by (5.30). 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 5.9.4. *Let R, M and S be as in Theorem 5.9.2. 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

$$\sum_i \theta_S\bigl(f_i\otimes\beta_i(n_i)\bigr)=\sum_i f_i\bigl(\beta_i(n_i)\bigr)\ ,f_i\in M^*\ ,\beta_i\in\mathfrak{b}\ ,n_i\in M.$$

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 $\sum_i f_i\bigl(\beta_i(n_i)\bigr)$. The reader should verify that the correspondences are inverses of each other. □

COROLLARY 5.9.5. *In the setting of Theorem 5.9.2, 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 3.1.24 to write L as the homomorphic image of a free R-module

$$R^I\to L\to 0 \tag{5.31}$$

where I is an index set. Tensor (5.31) with $(\cdot) \otimes_R M$ to get the exact sequence

$$M^I \to L \otimes_R M \to 0 \tag{5.32}$$

of S-modules. By Corollary 5.9.3 (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 (5.32), $M^I = \bigoplus_{i \in I} M$ 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 5.2.3, (5.31) splits. It follows that (5.32) also splits. Use Exercise 5.3.8 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 5.5.1 (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 5.1.6, $1 \otimes \delta : M^* \otimes_S C \to M^* \otimes_S D$ is a nonzero homomorphism of right R-modules. Since L is an R-generator, by Exercise 5.5.1 (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 5.1.6, $\delta \circ (\alpha \otimes 1)$ is nonzero. □

9.3. Exercises.

EXERCISE 5.9.1. Let R be any ring and let M be a left R-progenerator. Set $S = \operatorname{Hom}_R(M,M)$. Show that

$$(\,) \otimes_R M : \mathfrak{M}_R \to {}_S\mathfrak{M}$$

and

$$\operatorname{Hom}_S(M, \,) : {}_S\mathfrak{M} \to \mathfrak{M}_R$$

are inverse equivalences, establishing $\mathfrak{M}_R \sim {}_S\mathfrak{M}$. (Hint: Use Corollary 5.9.3 (2) and Theorem 5.5.15.)

EXERCISE 5.9.2. 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 6

Modules over Commutative Rings

1. Localization of Modules and Rings

Let R be a commutative ring and W a multiplicative subset of R. Recall that in Section 2.4 we defined the quotient ring $W^{-1}R$. We extend this notion to modules and algebras. Let M be an R-module and W a multiplicative set in 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 $w(w_2 m_1 - w_1 m_2) = 0$. The same argument used in Section 2.4 shows that $\sim$ is an equivalence relation on $R \times W$. 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 6.1.1. *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

$$\frac{m_1}{w_1} + \frac{m_2}{w_2} = \frac{w_2 m_1 + w_1 m_2}{w_1 w_2}.$$

(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

$$\frac{m_1}{w_1}\frac{m_2}{w_2} = \frac{m_1 m_2}{w_1 w_2}$$

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 $a \otimes b \mapsto ab$. □

EXAMPLE 6.1.2. Given a prime ideal P in R, let $W = R - P = \{x \in R \mid x \notin P\}$. As remarked in Example 2.4.1 (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 2.1.22, 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 6.1.6, R_P/PR_P is isomorphic to the quotient field of R/P.

REMARK 6.1.3. Lemma 6.1.4 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 5.3.10).

LEMMA 6.1.4. *$W^{-1}R$ 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 6.1.1, 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 6.1.5. 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 2.2.8 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.

PROPOSITION 6.1.6. *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 6.1.7. *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 6.1.8. *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

$$0 \to \ker(\varphi) \to M \xrightarrow{\varphi} N \to \operatorname{coker}(\varphi) \to 0. \tag{6.1}$$

Tensoring (6.1) with $(\cdot) \otimes_R R[W^{-1}]$ we get

$$0 \to W^{-1}\ker(\varphi) \to W^{-1}M \xrightarrow{\varphi_W} W^{-1}N \to W^{-1}\operatorname{coker}(\varphi) \to 0 \tag{6.2}$$

which is exact, by Lemma 6.1.4.

(1): If φ_W is one-to-one, then by Lemma 6.1.7 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 6.1.7 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 6.1.9. *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 6.1.7 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 6.1.7 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 6.1.10. *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_P is free of finite rank. Pick a basis $\{m_1/\alpha_1,\dots,m_n/\alpha_n\}$ for M_P over R_P. Since $\{1/\alpha_1,\dots,1/\alpha_n\}$ are units in R_P, it follows that $\{m_1/1,\dots,m_n/1\}$ is a basis for M_P over R_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

$$0 \to \ker\varphi \to R^n \xrightarrow{\varphi} M \to \operatorname{coker}\varphi \to 0. \tag{6.3}$$

Tensoring (6.3) with $(\cdot) \otimes_R R_\mathfrak{p}$, we get

$$0 \to (\ker\varphi)_\mathfrak{p} \to R^n_\mathfrak{p} \xrightarrow{\varphi_\mathfrak{p}} M_\mathfrak{p} \to (\operatorname{coker}\varphi)_\mathfrak{p} \to 0 \tag{6.4}$$

which is exact, by Lemma 6.1.4. 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 6.1.7 there exists $\beta \in R - \mathfrak{p}$ such that $\beta \cdot \operatorname{coker}\varphi = 0$. Then $(\operatorname{coker}\varphi)_\beta = 0$. Tensoring (6.3) with $(\;)\otimes_R R_\beta$ we get the sequence

$$0 \to (\ker\varphi)_\beta \to R^n_\beta \xrightarrow{\varphi_\beta} M_\beta \to 0 \tag{6.5}$$

which is exact. Since M is a finitely presented R-module, M_β is a finitely presented R_β-module. By Lemma 6.1.11, $(\ker\varphi)_\beta$ is a finitely generated R_β-module. Since $\beta \in R - P$, by Theorem 2.4.3 there exists a homomorphism of rings $R_\beta \to R_P$ so we can tensor (6.5) with $(\cdot)\otimes_{R_\beta} R_{\mathfrak{p}}$ to get (6.4) again. That is, $(\ker\varphi)_\beta \otimes_{R_\beta} R_{\mathfrak{p}} \cong (\ker\phi)_{\mathfrak{p}} = 0$. Lemma 6.1.7 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 $0 = \big((\ker\phi)_\beta\big)_\mu = (\ker\phi)_{\beta\mu}$. We also have $(\operatorname{coker}\phi)_{\beta\mu} = 0$. Tensor (6.3) with $R_{\mu\beta}$ to get $R^{(n)}_{\mu\beta} \cong M_{\mu\beta}$. □

LEMMA 6.1.11. *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): These are Exercise 3.1.9.

(3): Consider the commutative diagram

(6.6)
$$\begin{tikzcd}
 & R^{(n)} \arrow[r, "\phi"] \arrow[d, dotted, "\exists\rho"] & R^{(n)} \arrow[r, "\psi"] \arrow[d, dotted, "\exists\eta"] & C \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & C \arrow[r] & 0
\end{tikzcd}$$

where the top row exists because C is of finite presentation. The homomorphism η exists by Proposition 5.2.3 (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 5.7.2 applied to (6.6) 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. □

1.2. Exercises.

EXERCISE 6.1.1. 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 6.1.2. 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 6.1.3. 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 6.1.4. 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 6.1.5. 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 6.1.6. 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 6.1.7. 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 6.1.8. 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 6.1.9. 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 6.1.10. 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 6.1.11. 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.

2. Module Direct Summands of Rings

DEFINITION 6.2.1. 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 6.2.2. 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 6.2.3. 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 6.2.4. *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 2.2.6 (3). □

THEOREM 6.2.5. *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 6.2.4, 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 6.2.1. 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 6.2.2. 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

DEFINITION 6.3.1. 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 6.3.2. *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 6.3.3. *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) $V(L_1) \cup V(L_2) = V\big(\{x_1 x_2 \mid x_1 \in L_1, x_2 \in L_2\}\big)$.

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 $P \supseteq L_1 L_2$ and $L_1 \not\subseteq P$. Pick $x_1 \in L_1$ such that $x_1 \notin P$. Since $x_1 L_2 \subseteq P$ 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 $L_1 L_2 \subseteq P$. □

DEFINITION 6.3.4. By Lemma 6.3.3, 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 6.3.5. *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 1.3.3. 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 $xy \notin P$. □

LEMMA 6.3.6. *Let R be a commutative ring. As in Exercise 2.1.17, let* $\operatorname{Rad}_R(0) = \{x \in R \mid x^n = 0 \text{ for some } n > 0\}$ *be the nil radical of R. Then*

$$\operatorname{Rad}_R(0) = \bigcap_{P \in \operatorname{Spec} R} P.$$

In particular, $\operatorname{Rad}_R(0)$ *is an ideal.*

PROOF. 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 6.3.5 says there exists $P \in \operatorname{Spec} R$ such that $x \notin P$. □

LEMMA 6.3.7. *Let A be an ideal in R. The set*

$$\operatorname{Rad}(A) = \{x \in R \mid x^n \in A \text{ for some } n > 0\}$$

is called the nil radical of A. *Then,* $\operatorname{Rad}(A)$ *is an ideal in R which contains A, and*

$$\operatorname{Rad}(A) = I(V(A)) = \bigcap_{P \in V(A)} P.$$

A radical ideal *is an ideal such that* $A = \operatorname{Rad} A$.

PROOF. 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 (Proposition 2.1.20). Under this correspondence, prime ideals correspond to prime ideals. To finish, apply Lemma 6.3.6. □

LEMMA 6.3.8. *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 6.3.7, $P \supseteq \operatorname{Rad}(A)$. 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, $V(I(Y)) \subseteq V(A) = \bar{Y}$. □

COROLLARY 6.3.9. *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 6.3.2, 6.3.7, and 6.3.8. The last part is proved in Lemma 6.3.10. □

LEMMA 6.3.10. *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 1.4.4 the closure of $\{P\}$ is irreducible. By Lemma 6.3.8, the closure of $\{P\}$ is equal to $V(P)$, which is equal to $\bar{Y}$. By Lemma 1.4.4, Y is irreducible. The rest is left to the reader. □

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 6.3.11. *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 6.3.7, $\operatorname{Rad}(R\alpha) = I(V(\alpha))$. By Lemma 6.3.8, $V(\operatorname{Rad}(R\alpha)) = V(\alpha)$. 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. □

LEMMA 6.3.12. *Let* R *be a commutative ring and* $\operatorname{idemp}(R) = \{e \in R \mid e = e^2\}$ *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 6.3.11, 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 6.3.13. *Let R be a commutative ring and define*

$\mathscr{C} = \{Y \subseteq \operatorname{Spec} R \mid Y \textit{ is open and closed}\}$

$\mathscr{D} = \{A \subseteq R \mid A \textit{ is an ideal in } R \textit{ which is an } R\textit{-module direct summand of } R\}$.

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 6.3.12, Parts (1) and (2) show that γ is well defined and one-to-one. By Lemma 6.2.4 (1), δ is well defined and onto. By Lemma 6.3.12 (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 $A_1 A_2 = A_1 \cap A_2$, by Exercise 2.2.6. Since $\operatorname{Spec} R = X_1 \cup X_2 = V(A_1 A_2) = V(A_1 \cap A_2)$, Lemma 6.3.7 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 2.2.7) and $R\alpha_1^m \cap R\alpha_2^m = (0)$. By Proposition 2.2.7, R is isomorphic to the internal direct sum $R \cong R\alpha_1^m \oplus R\alpha_2^m$. By Theorem 2.2.6 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. □

COROLLARY 6.3.14. *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 6.3.13 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 6.3.5, 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 2.2.8, the direct sum map

$$R \xrightarrow{\phi} Re_1 \oplus \cdots \oplus Re_r$$

is onto. By Exercise 2.2.6, 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. □

COROLLARY 6.3.15. *The topological space* $\operatorname{Spec} R$ *is connected if and only if* 0 *and* 1 *are the only idempotents of R.*

COROLLARY 6.3.16. *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 6.2.4 (2).

(2) is equivalent to (3): Since $R = Re \oplus R(1-e)$, it follows from Exercise 6.3.5 that $V(1-e)$ is homeomorphic to $\operatorname{Spec} Re$. This follows from Corollary 6.3.15. □

3.1. Exercises.

EXERCISE 6.3.1. 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 6.3.2. Prove that if R is a local ring, then 0 and 1 are the only idempotents in R.

EXERCISE 6.3.3. 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 6.3.4. 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 6.3.5. 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 6.3.3. 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 6.3.6. Let R be a commutative ring which is a direct sum of ideals $R = A_1 \oplus \cdots \oplus A_n$. As in Theorem 2.2.6, 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 6.3.3. 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 6.3.7. 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 2.1.23.)

EXERCISE 6.3.8. 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 6.3.9. 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 6.3.10. 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 $W = \{\alpha^i \mid 0 \leq i\}$ 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 6.3.11. 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 6.3.12. Show that if R is a commutative ring, then $\operatorname{Spec} R$ is quasi-compact. That is, every open cover of $\operatorname{Spec} R$ has a finite subcover.

4. Locally Free Modules

4.1. Finitely Generated Projective over a Local Ring is Free. The reader is referred to Exercise 2.1.22 for the definition of local ring.

LEMMA 6.4.1. *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 5.3.5, this implies $M = T$. □

Another proof of Proposition 6.4.2 is presented in Corollary 6.8.5.

PROPOSITION 6.4.2. *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 6.4.1 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 5.4.6,

$$0 \to \ker\phi \otimes_R R/\mathfrak{m} \to (R/\mathfrak{m})^{(n)} \xrightarrow{\phi} P/\mathfrak{m}P \to 0$$

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 5.3.2), $\ker\phi = (0)$. □

COROLLARY 6.4.3. *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 6.4.2 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 6.4.6, 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. □

4.2. A Finitely Generated Projective Module is Locally Free.

DEFINITION 6.4.4. 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 5.4.22). Therefore, M_P is a finitely generated free R_P-module (Proposition 6.4.2) 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 6.4.5. *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 5.4.22, $M \otimes_R S$ 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 6.1.11, θ extends to a local homomorphism of local rings $\theta : R_P \to S_Q$. The proof follows from

$$\begin{aligned}(M \otimes_R S) \otimes_S S_Q &\cong M \otimes_R (S \otimes_S S_Q)\\ &\cong M \otimes_R S_Q\\ &\cong M \otimes_R (R_P \otimes_{R_P} S_Q)\\ &\cong (M \otimes_R R_P) \otimes_{R_P} S_Q\\ &\cong (R_P)^{(n)} \otimes_{R_P} S_Q\\ &\cong (S_Q)^{(n)}.\end{aligned}$$

□

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 6.4.6. *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

$$\operatorname{Spec} R \xrightarrow{\phi} \{0, 1, 2, \dots\}$$
$$P \mapsto \operatorname{Rank}_P M$$

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 6.4.2 we know that M_P is a free module over R_P. By Corollary 5.2.8, M is an R-module of finite presentation. An application of Lemma 6.1.10 completes the proof.

(2): If $Q \in U(\alpha)$, then $\alpha \in R - Q$. By Exercise 2.1.3, $R_Q = (R_\alpha)_{QR_\alpha}$. Since M_α is R_α-free of rank n, it follows from Proposition 2.3.6 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 $\operatorname{Rank}_P(M) = n$. 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 $\operatorname{Rank}_Q(M) = n$ for all $Q \in U(\alpha)$. This shows that (3) follows from Part (2). □

COROLLARY 6.4.7. *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 [**21**, 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 $\phi(P) = \operatorname{Rank}_P(M)$ is continuous and locally constant (Theorem 6.4.6). 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 quasi-compact (Exercise 6.3.12) 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 6.3.14). The rest is left to the reader. □

COROLLARY 6.4.8. *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 $P \in \operatorname{Spec} R$, $\operatorname{Rank}_P M = n$.*

PROOF. By Proposition 6.3.15 we know $\operatorname{Spec} R$ is connected. The continuous image of a connected space is connected. The rest follows from Corollary 6.4.7. □

4.3. Exercises. For the following, R always denotes a commutative ring.

EXERCISE 6.4.1. 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 6.4.2. 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 6.4.3. Let $f : R \to S$ be a homomorphism of commutative rings and let $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 6.3.3.

(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 6.4.4. Let $f : R \to S$ be a homomorphism of commutative rings and let $f^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ the continuous map of Exercise 6.3.3. 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 6.4.5. 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 6.4.6. 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 6.4.7. 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 6.4.8. 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 5.4.19 we defined a left R-module N to be flat if the functor $(\,) \otimes_R N$ is both left and right exact. In Exercise 5.9.2 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 6.5.1 below adds more necessary and sufficient conditions for N to be faithfully flat.

LEMMA 6.5.1. *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

$$0 \to A/\ker f \xrightarrow{\bar{f}} B \xrightarrow{\bar{g}} \operatorname{im} g \to 0 \tag{6.7}$$

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 (6.7) with N to get the sequence

$$0 \to A/\ker f \otimes_R N \xrightarrow{\bar{f}\otimes 1} B \otimes_R N \xrightarrow{\bar{g}\otimes 1} \operatorname{im} g \otimes_R N \to 0. \tag{6.8}$$

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 (6.8) 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 5.4.7, $\operatorname{im}(g\circ f)\otimes_R N = \operatorname{im}((g\otimes 1)\circ(f\otimes 1)) = 0$. 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 6.5.2. If N is projective, then N is flat (Exercise 5.4.6) 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 6.5.3. *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 6.1.4, so E is flat by Exercise 6.5.4. 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 6.5.1. □

5.2. Faithfully Flat Algebras.

LEMMA 6.5.4. *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 6.3.3 is onto.

PROOF. (1): Let $x \neq 0$, $x \in M$. Then Rx is a nonzero submodule of M. If follows from Lemma 6.5.1 (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 6.5.3, $S_P = S \otimes_R R_P$ 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 $Q \cap R = (\mathfrak{m} \cap S) \cap R = \mathfrak{m} \cap R = (\mathfrak{m} \cap R_P) \cap R = PR_P \cap R = P$. □

LEMMA 6.5.5. *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 6.5.4 (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 6.5.1 (3), S is faithfully flat. □

PROPOSITION 6.5.6. *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 5.3.4, A is R-faithful. The sequence

$$0 \to R \xrightarrow{\varepsilon} A$$

is exact, where $\varepsilon(r) = r \cdot 1$. By Exercise 5.5.2, there is a splitting map for ε if and only if

$$\operatorname{Hom}_R(A,R) \xrightarrow{\mathrm{H}_\varepsilon} \operatorname{Hom}_R(R,R) \to 0 \tag{6.9}$$

is exact. Let $\mathfrak{m}$ be a maximal ideal in R. By Theorem 5.4.22, $A \otimes_R R/\mathfrak{m} = A/\mathfrak{m}A$ 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 5.5.13. Therefore the top row is exact. Corollary 5.5.3 says that (6.9) 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 5.9.2. □

5.3. Another Hom Tensor Relation.

PROPOSITION 6.5.7. *Let S be a flat commutative R-algebra. Let M be a finitely presented R-module and N any R-module. 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 an isomorphism of S-modules.

PROOF. If M is free, then this follows from Corollary 5.5.13. There is some n and an exact sequence of R-modules

$$R^{(n)} \to R^{(n)} \to M \to 0. \tag{6.10}$$

Tensoring with $S \otimes_R (\cdot)$ is right exact, so

$$S^{(n)} \to S^{(n)} \to S \otimes_R M \to 0 \tag{6.11}$$

is an exact sequence of S-modules. By Proposition 5.5.5, the contravariant functor $\operatorname{Hom}_R(\cdot,N)$ is left exact. Applying it to (6.10), we get the exact sequence

$$0 \to \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(R^{(n)},N) \to \operatorname{Hom}_R(R^{(n)},N). \tag{6.12}$$

By Lemma 5.5.7 and Lemma 5.5.9, (6.12) can be written as

$$0 \to \operatorname{Hom}_R(M,N) \to N^{(n)} \to N^{(n)}. \tag{6.13}$$

Tensoring (6.13) with the flat module S gives the exact sequence

$$0 \to S \otimes_R \operatorname{Hom}_R(M,N) \to (S \otimes_R N)^{(n)} \to (S \otimes_R N)^{(n)}. \tag{6.14}$$

Apply the left exact functor $\operatorname{Hom}_S(\cdot, S \otimes_R N)$ to (6.11). Use Lemma 5.5.7 and Lemma 5.5.9 to simplify. This gives the exact sequence

$$0 \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \to (S \otimes_R N)^{(n)} \to (S \otimes_R N)^{(n)}. \tag{6.15}$$

Combining (6.14) and (6.15) with the natural maps yields a commutative diagram

$$\begin{tikzcd}
S \otimes_R \operatorname{Hom}_R(M,N) \arrow[r, "f_1", "\text{1-to-1}"'] \arrow[d, "\alpha"'] & (S \otimes_R N)^{(n)} \arrow[r, "f_2"] \arrow[d, "\beta"', "="] & (S \otimes_R N)^{(n)} \arrow[d, "\gamma"', "="] \\
\operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \arrow[r, "g_1", "\text{1-to-1}"'] & (S \otimes_R N)^{(n)} \arrow[r, "g_2"] & (S \otimes_R N)^{(n)}.
\end{tikzcd}$$

Since f_1 and β are one-to-one, α is one-to-one. To see that α is onto, let x be an element of the lower left corner. 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 5.7.2. □

PROPOSITION 6.5.8. *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. □

5.4. Faithfully Flat Descent of Central Algebras.

DEFINITION 6.5.9. 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 6.5.10. *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. □

PROPOSITION 6.5.11. *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 6.5.1, $R \to Z(A)$ is an isomorphism. □

5.5. Exercises.

EXERCISE 6.5.1. 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". Prove:

(1) f is one-to-one if and only if f_P is one-to-one for all $P \in \operatorname{Max} R$.
(2) f is onto if and only if f_P is onto for all $P \in \operatorname{Max} R$.

EXERCISE 6.5.2. 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 6.5.3. (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 6.5.4. 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 6.5.5. 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 6.5.6. State and prove a version of Lemma 6.5.1 for a ring R which is not necessarily commutative.

EXERCISE 6.5.7. Let R be a ring. Show that R is a faithfully flat R-module. Show that a free R-module is faithfully flat.

EXERCISE 6.5.8. 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 6.5.9. (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 6.5.10. (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 6.5.11. 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 6.5.12. Let $\theta : R \to S$ be a local homomorphism of local rings (see Exercise 2.1.22). If S is a flat R-algebra, show that S is faithfully flat.

EXERCISE 6.5.13. 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 5.3.7 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-module.
(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 6.5.14. 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 5.3.9.)
(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 6.5.15. 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 6.5.16. 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 $W \subseteq \text{Units}(R)$.

5.6. 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 6.5.12 is from [**22**, Proposition 1, p. 87].

PROPOSITION 6.5.12. *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 $k_i \ge 0$. For some $\ell_i \ge 0$, $f_i^{\ell_i}(\beta_i - f_i^{k_i}\alpha) = 0$ in S. For some large integer L, $f_i^L \alpha = f_i^L \beta_i$ 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 6.5.13. *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 6.4.4), then S is a finitely generated R-algebra.*

PROOF. Is left to the reader. □

6. Chain Conditions

DEFINITION 6.6.1. 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 1.1 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 6.6.2. 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 6.6.3. *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 Exercise 1.5.10, □

COROLLARY 6.6.4. *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 6.6.5. 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 6.6.11. This and Corollary 3.3.11 says the ring of n-by-n matrices over a division ring is artinian.

(3) By Exercise 6.6.12, any finite dimensional algebra over a field is artinian.

LEMMA 6.6.6. *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 Exercise 1.5.10.

(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. □

COROLLARY 6.6.7. *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 6.6.8. 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 6.6.7 (3) is satisfied. In particular, a PID is noetherian.

(2) It follows from the Hilbert Basis Theorem, Theorem 9.2.1, that a polynomial ring $k[x_1,\dots,x_n]$ in n variables over a field k is noetherian.

(3) It follows from Theorem 7.4.1 that an artinian ring is noetherian.

LEMMA 6.6.9. *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 5.7.1), the center vertical arrow is onto so $B_d = B_i$. □

COROLLARY 6.6.10. *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 6.6.9 to the exact sequence $0 \to A \to M \to M/A \to 0$. □

COROLLARY 6.6.11. *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 6.6.9 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 6.6.9 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 6.6.12. *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 3.1.24, 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 6.6.6 implies (2), (3) and (4). By Definition 6.6.2, R as an R-module satisfies the ACC on submodules. By Corollary 6.6.11, $R^{(m)}$ satisfies the ACC on submodules. By Lemma 6.6.9, M and K both satisfy the ACC on submodules. □

COROLLARY 6.6.13. *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 6.6.9 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 6.6.14. *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 6.3.9 and Proposition 1.4.7. □

COROLLARY 6.6.15. *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 6.6.14 and 1.4.7. For each i, let $P_i = I(Z_i)$. By Lemma 6.3.10, each of the ideals $P_1, \ldots, P_r$ 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 6.3.10, $V(Q)$ is irreducible. By the uniqueness part of Proposition 1.4.7, $V(Q) = Z_i$. 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 $P_1, \ldots, P_r$. By Lemma 6.3.10, $V(P)$ 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 6.6.16. *Let R be a commutative noetherian ring. Then there exist primitive idempotents $e_1, \ldots, e_n$ 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, $e_1 = f_1, \ldots, e_n = f_n$.*

PROOF. Let $\operatorname{Spec} R = X_1 \cup \cdots \cup X_n$ be the decomposition into connected components, which exists by Propositions 6.6.14 and 1.4.7. By Corollary 6.3.14 there are idempotents $e_1, \ldots, e_n$ 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 6.3.16 implies each e_i is a primitive idempotent. The uniqueness claim comes from Theorem 6.2.5. □

6.1. Exercises.

EXERCISE 6.6.1. 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 6.6.2. Let R be an artinian ring and M a finitely generated R-module. Show that M satisfies the DCC on submodules.

EXERCISE 6.6.3. Prove that if R is an artinian ring and I is a two-sided ideal in R, then R/I is artinian.

EXERCISE 6.6.4. Let R be a commutative artinian ring and W is a multiplicative set in R. Show that $W^{-1}R$ is artinian.

EXERCISE 6.6.5. 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 6.6.6. Prove that if R is an artinian domain, then R is a division ring.

EXERCISE 6.6.7. 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 6.6.8. 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.

6.2. Composition Series.

DEFINITION 6.6.17. 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 6.6.18. 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.

PROPOSITION 6.6.19. *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 $i = 0, \dots, n-1$. 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. □

PROPOSITION 6.6.20. *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 6.6.19 all chains in M are of bounded length.

(2) implies (1): By Lemma 6.6.6, 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. □

DEFINITION 6.6.21. If R is any ring, and M has a composition series, then we say M is a *module of finite length*. The *length* of M is the number $\ell(M)$, which is the length of any composition series of M, by Proposition 6.6.19.

PROPOSITION 6.6.22. *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. □

6.3. Faithfully Flat Base Change.

LEMMA 6.6.23. *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) *M is a generator module over R if and only if $S \otimes_R M$ is a generator over S.*
(7) *M is faithful over R if and only if $S \otimes_R M$ is faithful over S.*

PROOF. (1): If M is finitely generated, then Theorem 5.4.22 (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

$$R^{(n)} \to M \to 0 \tag{6.16}$$

which is defined by $(r_1, \dots, r_n) \mapsto \sum r_i x_i$. Tensoring (6.16) with S gives the sequence

$$S^{(n)} \to S \otimes_R M \to 0$$

which is exact. Since S is faithfully flat, (6.16) 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 6.1.11 (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 5.4.22 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 5.2.8, $S \otimes_R M$ 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 5.5.5 (2) it is enough to show $\operatorname{Hom}_R(M, \cdot)$ is a right exact functor. Start with an exact sequence

$$A \xrightarrow{\alpha} B \to 0 \tag{6.17}$$

of R-modules. It is enough to show

$$\operatorname{Hom}_R(M,A) \xrightarrow{\mathrm{H}_\alpha} \operatorname{Hom}_R(M,B) \to 0 \tag{6.18}$$

is exact. Since S is faithfully flat over R, it is enough to show

$$S \otimes_R \operatorname{Hom}_R(M,A) \xrightarrow{1 \otimes \mathrm{H}_\alpha} S \otimes_R \operatorname{Hom}_R(M,B) \to 0 \tag{6.19}$$

is exact. Tensoring is right exact, so tensoring (6.17) with $S \otimes_R (\cdot)$ gives the exact sequence

$$S \otimes_R A \xrightarrow{1 \otimes \alpha} S \otimes_R B \to 0. \tag{6.20}$$

Since we are assuming $S \otimes_R M$ is S-projective, by Proposition 5.5.5 (2) we can apply the functor $\operatorname{Hom}_S(S \otimes_R M, \cdot)$ to (6.20) yielding

$$\operatorname{Hom}_S(S \otimes_R M, S \otimes_R A) \xrightarrow{\mathrm{H}_{1\otimes\alpha}} \operatorname{Hom}_S(S \otimes_R M, S \otimes_R B) \to 0 \tag{6.21}$$

which is exact. Combine (6.19) and (6.21) 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 6.5.7. 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 6.5.9, $M \otimes_R S$ 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.

(5), (6), (7): Are left to the reader. □

6.4. Exercises.

EXERCISE 6.6.9. 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 6.6.10. 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 6.6.11. 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 $\operatorname{Hom}_D(M,M)$ is both artinian and noetherian.

EXERCISE 6.6.12. 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.

7. Locally Free Modules

7.1. Locally Free of Finite Rank Equals Finitely Generated Projective.

DEFINITION 6.7.1. Let R be a commutative ring and M an R-module. Then M is *locally free of finite rank* if there exist elements $f_1, \dots, f_n$ 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 6.7.2. *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 follows straight from Corollary 5.2.8 and Proposition 6.4.2. It is trivial that (3) implies (4).

(4) implies (2): Using Lemma 6.1.10, 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 6.3.1). By Exercise 6.3.12, 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 6.7.3). 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 6.7.1). Now apply Lemma 6.6.23 (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 6.7.2 utilize this rank function to give us a powerful test for locally free modules and for flatness over an integral domain.

COROLLARY 6.7.3. *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 6.4.1, $M_{\mathfrak{m}}$ 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 6.1.8, 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 6.1.4 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 6.7.2 can now be applied to finish the proof. □

COROLLARY 6.7.4. *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 5.6.18 and Corollary 5.3.4, (1) and (2) are equivalent. Proposition 6.7.2, Corollary 6.7.3, and Corollary 5.3.4 imply that (2) and (3) are equivalent. □

7.2. Invertible Modules and the Picard Group.

LEMMA 6.7.5. *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) $M^* \otimes_R M \cong R$.
(5) For some R-module N, there is an isomorphism $M \otimes_R N \cong R$.

PROOF. The hypotheses on M imply that M is an R-progenerator module.

(1) is equivalent to (2): By Corollary 5.5.13, for each prime ideal $P \in \operatorname{Spec} R$, $M^* \otimes_R R_P = \operatorname{Hom}_R(M,R) \otimes_R R_P \cong \operatorname{Hom}_{R_P}(M_P,R_P)$. Since M is finitely generated projective, M_P is free of finite rank by Proposition 6.4.2. Suppose $M_P \cong R_P^{(n)}$. Then $(M_P)^* = \operatorname{Hom}_{R_P}(M_P,R_P) \cong \operatorname{Hom}_{R_P}(R_P^{(n)},R_P) \cong \operatorname{Hom}_{R_P}(R_P,R_P)^{(n)} \cong R_P^{(n)}$. Therefore $\operatorname{Rank}_R(M) = 1$ if and only if $\operatorname{Rank}_R(M^*) = 1$.

(1) implies (3): Let $\phi : R \to \operatorname{Hom}_R(M,M)$ be the left regular representation of R in $\operatorname{Hom}_R(M,M)$ defined in Example 3.3.2. For each prime ideal $P \in \operatorname{Spec} R$, $M_P \cong R_P$. Therefore localizing ϕ at P yields

$$R_P \xrightarrow{\phi_P} \operatorname{Hom}_{R_P}(M_P,M_P) \cong \operatorname{Hom}_{R_P}(R_P,R_P) \cong R_P$$

which is an isomorphism. By Exercise 6.5.1, ϕ is an isomorphism.

(3) and (4) are equivalent because $M^* \otimes_R M \cong \operatorname{Hom}_R(M,M)$ by Lemma 5.9.1 (1).

(4) implies (5): Take N to be M^*.

(5) implies (1): Fix a prime $P \in \operatorname{Spec} R$. Then $M_P \cong R_P^{(n)}$ for some n. Now $R_P \cong R_P \otimes_R (M \otimes_R N) \cong M_P \otimes_R N \cong R_P^{(n)} \otimes_R N \cong N_P^{(n)}$. So N_P is finitely generated projective over the local ring R_P, hence is free of finite rank over R_P. Then $n = 1$. Since P was arbitrary, we are done. □

DEFINITION 6.7.6. If M is an R-module that satisfies any of the equivalent properties of Lemma 6.7.5, 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 6.7.7, $\operatorname{Pic}(R)$ is an abelian group, which is called the *Picard group* of R.

PROPOSITION 6.7.7. *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. □

EXAMPLE 6.7.8. See Exercise 5.3.2. 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 6.7.2 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 6.7.9. 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 3.1.28).
(2) R is a local ring (Proposition 6.4.2).
(3) R is a principal ideal domain (Proposition 3.2.5).

7.3. Exercises.

EXERCISE 6.7.1. 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 6.7.2. 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 6.7.3. Let R be a commutative ring. Assume $f_1, \dots, f_n$ are elements of R that generate the unit ideal. That is, $R = Rf_1 + \cdots + Rf_n$. Let $S = R_{f_1} \oplus \cdots \oplus R_{f_n}$ be the direct sum. Let $\theta : R \to S$ be defined by $\theta(x) = (x/1, \dots, x/1)$. Show that S is a faithfully flat R-module.

EXERCISE 6.7.4. 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 6.7.5. 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 6.7.6. 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 6.7.7. 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. 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.
(4) Use Corollary 6.7.4 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 $U(x^2)$.

EXERCISE 6.7.8. This exercise is a continuation of Exercise 6.7.7. Let k be a field, $A = k[x]$ and $R = k[x^2, x^3]$. Show:

(1) For each $\alpha \in k$, set $P_\alpha = R(1 - \alpha x) + \mathfrak{m}$. Then P_α is an R-submodule of A, and P_α is isomorphic to R if and only if $\alpha = 0$.
(2) The R-module homomorphisms $P_\alpha \otimes_R P_\beta \to P_\alpha P_\beta \to P_{\alpha+\beta}$ are isomorphisms. (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) $\operatorname{Pic} R \cong k$. (This is a challenge and may involve tools not yet covered in this text. See [**10**, Exercise 14.2.19] for a method involving the Mayer-Vietoris sequence.)
(5) A is equal to the integral closure of R in K. (As in (4), this is a challenge. You can attempt to do it now, or come back to it later. See Section 9.1)

EXERCISE 6.7.9. 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 6.7.4 and Exercise 5.4.21, show that T is not flat over S. See [**10**, Exercise 4.4.19] for more properties of the extension T/S.

8. Flat Modules and Algebras

8.1. Flat if and only if Locally Flat.

PROPOSITION 6.8.1. *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 5.4.22.
(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 3.1.14 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 6.5.3,

$$E = \bigoplus_{\mathfrak{m} \in \operatorname{Max} R} R_{\mathfrak{m}}$$

is a faithfully flat R-module, so $(S) \otimes_R A$ is exact. □

PROPOSITION 6.8.2. *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 6.8.2. 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.) □

8.2. A Finiteness Criterion for Flat.

PROPOSITION 6.8.3. *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 5.8.3, $B = \varinjlim B_\alpha$ where $\{B_\alpha\}$ is the directed system of finitely generated submodules of B. By Corollary 5.8.10, $M \otimes_R B = \varinjlim (M \otimes_R B_\alpha)$. 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 5.8.5, 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 $v = 0$. □

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 6.8.4. *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 $a_1, \ldots, a_r$ in R and $x_1, \ldots, x_r$ in M such that $\sum_i a_i x_i = 0$, then there exist an integer s, elements $\{b_{ij} \in R \mid 1 \leq i \leq r, 1 \leq j \leq s\}$ in R, and $y_1, \ldots, y_s$ 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 5.8.3, $I = \varinjlim I_\alpha$, where each I_α is a finitely generated right ideal in R and $I_\alpha \subseteq I$. By Corollary 5.8.10, $\varinjlim (I_\alpha \otimes_R M) = I \otimes_R M$. By hypothesis the sequence

$$0 \to I_\alpha \otimes_R M \xrightarrow{\mu_\alpha} M$$

is exact for each α. By Theorem 5.8.6, 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 5.5.10, 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 5.6.4, $\operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is an injective right R-module. By Theorem 5.6.17, 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. □

COROLLARY 6.8.5. *Let R be a local ring and M a finitely generated R-module. The following are equivalent.*

1. *(1) M is a free R-module.*
2. *(2) M is a projective R-module.*
3. *(3) M is a flat R-module.*

PROOF. (1) implies (2): Follows straight from the definition of projective.

(2) implies (3): This is Exercise 5.4.6.

(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 6.4.1.

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 6.8.4 (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 6.8.4 (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. □

8.3. Finitely Presented and Flat is Projective.

LEMMA 6.8.6. *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. *(1) For any right ideal I of R, $A \cap IB = IA$.*
2. *(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. *(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 6.8.4 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 5.7.2) 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

$$\begin{aligned} f(x_j) &= f_1(x_j) + f_2(x_j) - f_2(f_1(x_j)) \\ &= f_1(x_j) + f_2(x_j - f_1(x_j)) \\ &= f_1(x_j) + x_j - f_1(x_j) \\ &= x_j. \end{aligned}$$

□

We give another proof of Theorem 5.6.18.

COROLLARY 6.8.7. *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 5.4.6 and of finite presentation by Corollary 5.2.8.

(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 6.8.6 (3), this sequence is split exact. □

COROLLARY 6.8.8. *Let R be a commutative ring and M an R-module of finite presentation. Then M is R-projective if and only if $M_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$-projective for every $\mathfrak{p}$ in* $\operatorname{Spec} R$.

PROOF. Is left to the reader. □

8.4. Flat Algebras.

LEMMA 6.8.9. *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 2.2.8. Tensoring with S,

$$0 \to (I \cap J) \otimes_R S \to S \to S/IS \oplus S/JS$$

is exact. By Corollary 6.8.4, 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 6.8.4 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 2.1.21, $(I : J) = \bigcap_i (I : Ra_i)$. By Part (1) and Step 1,

$$(I : J)S = \bigcap_i (I : Ra_i)S = \bigcap_i (IS : Ra_i S) = (IS : \sum_i Ra_i S) = (IS : JS).$$

□

PROPOSITION 6.8.10. *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 6.8.4, $\mathfrak{a} \otimes_R S = \mathfrak{a}S$. 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

$$\begin{aligned}
\operatorname{annih}_R(I+J)S &= (\operatorname{annih}_R(I) \cap \operatorname{annih}_R(J))\, S \quad \text{(Exercise 3.1.5)} \\
&= \operatorname{annih}_R(I)S \cap \operatorname{annih}_R(J)S \quad \text{(Lemma 6.8.9)} \\
&= \operatorname{annih}_S(I \otimes_R S) \cap \operatorname{annih}_S(J \otimes_R S) \quad \text{(Induction Hypothesis)} \\
&= \operatorname{annih}_S(I \otimes_R S + J \otimes_R S) \quad \text{(Exercise 3.1.5)} \\
&= \operatorname{annih}_S\left((I+J) \otimes_R S\right).
\end{aligned}$$

Hence the proposition holds for $I+J$. □

COROLLARY 6.8.11. *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 6.8.10.

(2): By Exercise 3.1.6, $(I:J) = \operatorname{annih}_R((I+J)/I)$. To complete the proof, apply Part (1). □

8.5. Exercises.

EXERCISE 6.8.1. 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 6.8.2. 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 6.8.3. 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 6.8.4. 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 6.8.1 to assume R is a local PID. Use Corollary 6.8.4.)

EXERCISE 6.8.5. Let R be a commutative ring, M an R-module, and $a \in R$. Prove that the following are equivalent:

(1) The multiplication map $\mu : aR \otimes_R M \to M$ of Corollary 6.8.4 is one-to-one.

(2) The "left multiplication by a" homomorphism $\ell_a : M \to M$ is one-to-one.

9. Multilinear Algebra

9.1. Graded Algebras. The reader is referred to Section 9.4 for the definitions and conventions of graded rings and modules. Let R be a commutative ring. A *graded R-algebra* is an R-algebra A which as an R-module is the internal direct sum $A = \bigoplus_{n=0}^{\infty} A_n$ of a set of R-submodules $\{A_n\}_{n\geq 0}$ satisfying the property that $A_iA_j \subseteq A_{i+j}$ for all $i, j \geq 0$. It follows that A_0 is a subalgebra of A and $R \cdot 1 \subseteq A_0$. An element x in A_n is said to be *homogeneous of degree n* and we write $\deg(x) = n$. Let B be another graded R-algebra, and $\theta : A \to B$ an R-algebra homomorphism. Then θ is a *graded R-algebra homomorphism* in case $\theta(A_i) \subseteq B_i$ for all $i \geq 0$. A *graded R-subalgebra* of A is a subalgebra B of A such that B is a graded R-submodule of A. A *graded left ideal* of A is an ideal I of A which is a graded R-submodule of A. The definitions for *graded right ideal* and *graded two-sided ideal* of A are similar. If I is a graded two-sided ideal of A, the reader should verify that A/I is a graded R-algebra. If $\theta : A \to B$ is a graded homomorphism of graded R-algebras, the reader should verify that the kernel of θ is a graded two-sided ideal of A and the image of θ is a graded subalgebra of B.

PROPOSITION 6.9.1. *Let R be a commutative ring and A a graded R-algebra. Let S be a set of homogeneous elements of A. The R-subalgebra of A generated by S is a graded subalgebra. The left ideal of A generated by S is a graded left ideal. The right ideal of A generated by S is a graded right ideal. The two-sided ideal of A generated by S is a graded two-sided ideal.*

PROOF. Let B denote the R-subalgebra of A generated by S. Let P be the set of all products of finitely many elements of S. Then B is equal to the R-submodule of A generated by $P \cup \{1\}$, which is graded since P consists of homogeneous elements. The rest is left to the reader. □

DEFINITION 6.9.2. Let R be a commutative ring. A graded R-algebra A is said to be *anticommutative* if for all homogeneous elements x, y in A

$$xy = (-1)^{\deg(x)\deg(y)} yx.$$

A graded R-algebra A is said to be *alternating* if A is anticommutative and $x^2 = 0$ for all homogeneous elements x of odd degree.

DEFINITION 6.9.3. Let R be a commutative ring. Let A and B be graded R-algebras. The *graded tensor product* of A and B, denoted $A \otimes_R B$, is defined by the following rules.

(1) As an R-module, $A \otimes_R B$ is the usual tensor product.

(2) As a graded R-module, the homogeneous component of degree n is

$$(A \otimes_R B)_n = \bigoplus_{i+j=n} (A_i \otimes_R B_j).$$

(3) The multiplication rule on $A \otimes_R B$ is defined to be

$$(u \otimes x)(v \otimes y) = (-1)^{\deg(x)\deg(v)} uv \otimes xy$$

for homogeneous elements $u, v \in A$, $x, y \in B$.

The reader should verify that the multiplication rule can be extended to $A \otimes_R B$ and that $A \otimes_R B$ is a graded R-algebra. If A and B are two commutative graded R-algebras, we define the *commutative graded tensor product* of A and B, denoted $A \otimes_R B$, in the same way, except the multiplication rule is induced by $(u \otimes x)(v \otimes y) = uv \otimes xy$.

PROPOSITION 6.9.4. *Let R be a commutative ring. Let A and B be graded R-algebras. The graded tensor product $A \otimes_R B$ satisfies the following.*

(1) The assignments $a \mapsto a \otimes 1$, $b \mapsto 1 \otimes b$ are graded R-algebra homomorphisms $\rho_1 : A \to A \otimes_R B$, $\rho_2 : B \to A \otimes_R B$. For any homogeneous elements $x \in A$, $y \in B$, $\rho_1(x)\rho_2(y) = (-1)^{\deg(x)\deg(y)} \rho_2(y)\rho_1(x)$.

(2) Suppose C is a graded R-algebra and $\alpha : A \to C$, $\beta : B \to C$ are graded R-algebra homomorphisms such that $\alpha(x)\beta(y) = (-1)^{\deg(x)\deg(y)} \beta(y)\alpha(x)$ for any homogeneous $x \in A$, $y \in B$. Then there exists a unique graded R-algebra homomorphism $\gamma : A \otimes_R B \to C$ such that the diagram

$$\begin{tikzcd}
 & C & \\
A \arrow[ur, "\alpha"] \arrow[r, "\rho_1"'] & A \otimes_R B \arrow[u, dotted, "\exists\gamma"'] & B \arrow[ul, "\beta"'] \arrow[l, "\rho_2"]
\end{tikzcd}$$

commutes.

PROOF. Is left to the reader. □

9.2. The Tensor Algebra of a Module. Let R be a commutative ring and A an R-algebra, and M a left A-module. Then M is a left R-module by the action $rx = (r \cdot 1)x$ for all $r \in R$ and $x \in M$. 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 $a, b \in A$, $r \in R$, $x \in M$:

(1) $(ax)b = a(xb)$ and
(2) $rx = (r \cdot 1)x = x(r \cdot 1) = xr$.

The *enveloping algebra* of A is $A^e = A \otimes_R A^o$. If M is a left A^e-module, then we can make M into a two-sided A/R-module by

$$\begin{aligned} ax &= a \otimes 1 \cdot x, \\ xa &= 1 \otimes a \cdot x. \end{aligned}$$

Conversely, any two-sided A/R-module can be turned into a left A^e-module in the same way.

Definition 6.9.5. Let A be an R-algebra and M a two-sided A/R-module. For $n \geq 0$ we define two-sided A/R-modules $T^n(M)$ as follows. Define $T^0(M)$ to be A, the free two-sided A/R-module of rank one. If $n > 0$, define $T^n(M)$ to be $M^{\otimes n}$ by which we mean $M \otimes_A \cdots \otimes_A M$, the tensor product of n copies of M. By Lemma 5.4.10, $T^n(M)$ is a two-sided A/R-module. The *tensor algebra* of M, denoted $T(M)$, is the graded R-algebra defined by the following rules.

(1) As a graded R-module, $T(M)$ is equal to $\bigoplus_{n \geq 0} T^n(M)$.
(2) The product rule on $T(M)$ is induced on homogeneous components by

$$T^i(M) \otimes_A T^j(M) \xrightarrow{\eta_{i,j}} T^{i+j}(M)$$

which is a two-sided A/R-module isomorphism.

The reader should verify that $T(M)$ is a graded R-algebra, the identity mapping of A onto $T^0(M)$ is a natural R-algebra homomorphism $\tau^0 : A \to T(M)$, and the identity mapping of M onto $T^1(M)$ is a two-sided A/R-module homomorphism $\tau^1 : M \to T(M)$. In case the rings A and R are ambiguous, we write $T^n_{A/R}(M)$ instead of $T^n(M)$ and $T_{A/R}(M)$ instead of $T(M)$. If $A = R$, we sometimes write $T^n_R(M)$ instead of $T^n_{A/R}(M)$ and $T_R(M)$ instead of $T_{A/R}(M)$.

Proposition 6.9.6. *Let A be an R-algebra and M a two-sided A/R-module. The tensor algebra satisfies the following.*

(1) The R-algebra $T(M)$ is generated by the set $T^0(M) + T^1(M)$.
(2) (Universal Mapping Property) For any R-algebra homomorphism $\theta : A \to B$ and two-sided A/R-module homomorphism $f : M \to B$, there exists a unique homomorphism ϕ of both R-algebras and two-sided A/R-modules such that the diagram of R-algebras

$$\begin{tikzcd} A \arrow[rr, "\tau^0"] \arrow[dr, "\theta"'] & & T(M) \arrow[dl, dotted, "\exists\phi"] \\ & B & \end{tikzcd}$$

commutes and the diagram of two-sided A/R-modules

$$\begin{tikzcd}
M \arrow[r, "\tau^1"] \arrow[dr, "f"'] & T(M) \arrow[d, dotted, "\exists\phi"] \\
& B
\end{tikzcd}$$

commutes. Up to an isomorphism of both R-algebras and two-sided A/R-modules, $T(M)$ is uniquely determined by this mapping property.

(3) *If $\theta : M \to N$ is a homomorphism of two-sided A/R-modules, then there exists a unique homomorphism $T(\theta)$ of both graded R-algebras and two-sided A/R-modules such that the diagram*

$$\begin{tikzcd}
M \arrow[r, "\tau_M"] \arrow[d, "\theta"'] & T(M) \arrow[d, "T(\theta)"] \\
N \arrow[r, "\tau_N"] & T(N)
\end{tikzcd}$$

commutes.

(4) *The assignment $M \mapsto T(M)$ defines a covariant functor from the category of two-sided A/R-modules to the category of graded R-algebras which are also two-sided A/R-modules. The assignment $M \mapsto T^n(M)$ defines a covariant functor from the category of two-sided A/R-modules to the category of two-sided A/R-modules.*

(5) *Given an exact sequence of two-sided A/R-modules*

$$0 \to K \to M \xrightarrow{\theta} N \to 0$$

the graded R-algebra homomorphism $T(\theta) : T(M) \to T(N)$ is onto, and the kernel of $T(\theta)$ is the ideal in $T(M)$ generated by the image of K in $T^1(M)$.

(6) *If $R \to S$ is a homomorphism of commutative rings, then for all $n \geq 0$ there is an isomorphism of two-sided $(S \otimes_R A)/S$-modules*

$$S \otimes_R T^n_{A/R}(M) \cong T^n_{S\otimes_R A/S}(S \otimes_R M)$$

and an isomorphism

$$S \otimes_R T_{A/R}(M) \cong T_{S\otimes_R A/S}(S \otimes_R M)$$

of both graded S-algebras and two-sided $(S \otimes_R A)/S$-modules.

PROOF. (1), (4) and (6): Are left to the reader.

(2): Notice that

$$\phi(x) = \begin{cases} \theta(x) & \text{for all } x \in T^0(M), \\ f(x) & \text{for all } x \in T^1(M) \end{cases}$$

and $T^0(M) + T^1(M)$ contains a generating set for the R-algebra $T(M)$. The rest is left to the reader.

(3): Apply Part (2) to the composite map $M \to N \to T(N)$.

(5): Use Lemma 6.9.7 and induction on n to show that $T^n(\theta) : T^n(M) \to T^n(N)$ is onto. Since $T(\theta)(K) = 0$, it is clear that the ideal generated by K is in the kernel of $T(\theta)$. Use Lemma 6.9.7 and induction on n to show that the kernel of $T^n(\theta) : T^n(M) \to T^n(N)$

is generated by elements of the form $x_1 \otimes x_2 \otimes \cdots \otimes x_n$ where at least one of the x_i is in K. Elements of this form are in the two-sided ideal of $T(M)$ generated by K. □

LEMMA 6.9.7. *Let R be any ring. Let*

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

be an exact sequence in $\mathfrak{M}_R$ and

$$0 \to D \xrightarrow{\delta} E \xrightarrow{\varepsilon} F \to 0$$

an exact sequence in ${}_R\mathfrak{M}$. Then

$$(A \otimes_R E) \oplus (B \otimes_R D) \xrightarrow{\alpha\otimes 1 + 1\otimes\delta} B \otimes_R E \xrightarrow{\beta\otimes\varepsilon} C \otimes_R F \to 0$$

is an exact sequence of abelian groups.

PROOF. By Lemma 5.4.18, tensoring is right exact. The diagram

$$\begin{tikzcd}
A \otimes_R D \arrow[r, "\alpha\otimes 1"] \arrow[d, "1\otimes\delta"] & B \otimes_R D \arrow[r, "\beta\otimes 1"] \arrow[d, "1\otimes\delta"] & C \otimes_R D \arrow[r] \arrow[d, "1\otimes\delta"] & 0 \\
A \otimes_R E \arrow[r, "\alpha\otimes 1"] \arrow[d, "1\otimes\varepsilon"] & B \otimes_R E \arrow[r, "\beta\otimes 1"] \arrow[d, "1\otimes\varepsilon"] & C \otimes_R E \arrow[r] \arrow[d, "1\otimes\varepsilon"] & 0 \\
A \otimes_R F \arrow[r, "\alpha\otimes 1"] \arrow[d] & B \otimes_R F \arrow[r, "\beta\otimes 1"] \arrow[d] & C \otimes_R F \arrow[r] \arrow[d] & 0 \\
0 & 0 & 0 &
\end{tikzcd}$$

commutes and the rows and columns are exact. It is clear that $\beta \otimes \varepsilon$ is onto and the image of $\alpha \otimes 1 + 1 \otimes \delta$ is contained in the kernel of $\beta \otimes \varepsilon$. Given $z \in \ker(\beta \otimes \varepsilon)$, show that $z \in \operatorname{im}(\alpha \otimes 1 + 1 \otimes \delta)$. The reader should verify that there exists $w \in B \otimes_R D$ such that $(1 \otimes \delta)(\beta \otimes 1)(w) = (\beta \otimes 1)(z)$. The proof follows from the fact that $(1 \otimes \delta)(w) - z \in \ker(\beta \otimes 1) = \operatorname{im}(\alpha \otimes 1)$. □

9.3. The Symmetric Algebra of a Module.

DEFINITION 6.9.8. Let R be a commutative ring, M an R-module, and $T(M)$ the tensor algebra of M. Let I be the ideal of $T(M)$ generated by the set $\{x \otimes y - y \otimes x \mid x, y \in T^1(M)\}$. By Proposition 6.9.1, I is a graded ideal of $T(M)$. The *symmetric algebra* of M, denoted $S(M)$, is the graded R-algebra $T(M)/I$. The homogeneous component of degree n in $S(M)$ is denoted $S^n(M)$. In case the ring of scalars is ambiguous, we write $S^n_R(M)$ instead of $S^n(M)$ and $S_R(M)$ instead of $S(M)$.

The reader should verify that the sequence $0 \to I \cap T^n(M) \to T^n(M) \to S^n(M) \to 0$ is exact. In particular, $R = S^0(M)$ and $M = S^1(M)$.

PROPOSITION 6.9.9. *Let R be a commutative ring and M an R-module. The symmetric algebra of M, $S(M)$, satisfies the following.*

(1) The R-algebra $S(M)$ is generated by the set $M = S^1(M)$.
(2) $S(M)$ is a commutative graded R-algebra.

(3) *(Universal Mapping Property) Let $\tau : M \to S(M)$ be the identity mapping of M onto $S^1(M)$. For any R-algebra A and R-module homomorphism $f : M \to A$ such that $f(x)f(y) = f(y)f(x)$ for all $x,y \in M$, there exists a unique R-algebra homomorphism ϕ such that the diagram*

$$\begin{tikzcd} M \arrow[rr, "\tau"] \arrow[dr, "f"'] & & S(M) \arrow[dl, dotted, "\exists\phi"] \\ & A & \end{tikzcd}$$

commutes. Up to an R-algebra isomorphism, $S(M)$ is uniquely determined by this mapping property.

(4) *If $\theta : M \to N$ is an R-module homomorphism, then there exists a unique graded R-algebra homomorphism $S(\theta)$ such that the diagram*

$$\begin{tikzcd} M \arrow[r, "\tau_M"] \arrow[d, "\theta"'] & S(M) \arrow[d, "S(\theta)"] \\ N \arrow[r, "\tau_N"] & S(N) \end{tikzcd}$$

commutes.

(5) *$S(M)$ is a covariant functor from the category of R-modules to the category of commutative graded R-algebras. $S^n(M)$ is a covariant functor from the category of R-modules to the category of R-modules.*

(6) *Given an exact sequence of R-modules*

$$0 \to K \to M \xrightarrow{\theta} N \to 0$$

the graded R-algebra homomorphism $S(\theta) : S(M) \to S(N)$ is onto, and the kernel of $S(\theta)$ is the ideal in $S(M)$ generated by the image of K in $S^1(M)$.

(7) *If $R \to T$ is a homomorphism of commutative rings, then for all $n \geq 0$ there is an isomorphism of T-modules $T \otimes_R S^n_R(M) \cong S^n_T(T \otimes_R M)$ and an isomorphism of graded T-algebras $T \otimes_R S_R(M) \cong S_T(T \otimes_R M)$.*

(8) *Let M_1, M_2 be two R-modules. There is a natural isomorphism of graded R-algebras $S(M_1) \otimes_R S(M_2) \cong S(M_1 \oplus M_2)$, where $S(M_1) \otimes_R S(M_2)$ denotes the commutative graded tensor product.*

PROOF. (1): Since $T^1(M)$ contains a generating set for the R-algebra $T(M)$, it follows that $S^1(M)$ contains a generating set for the R-algebra $S(M)$.

(2): For all $x,y \in M = T^1(M)$, $x \otimes y + I = y \otimes x + I$. Use Part (1).

(3): Apply Proposition 6.9.6 (2) to get $\phi : T(M) \to A$. Check that $I \subseteq \ker(\phi)$, so ϕ factors through $S(M)$.

(4) , (5) and (7): Are left to the reader.

(6): Write $I(M)$ for the ideal in $T(M)$ which defines $S(M)$. Similarly, let $I(N)$ denote the ideal in $T(N)$ which defines $S(N)$. By Proposition 6.9.6 (5), $T(\theta)$ is onto. Since θ is onto, for any $x,y \in N$, we can write $x = \theta(u)$ and $y = \theta(v)$ for some $u,v \in M$. Therefore, $T(\theta)$ maps $u \otimes v - v \otimes u$ onto $x \otimes y - y \otimes x$. Therefore, the restriction of $T(\theta)$ defines a homomorphism $I(M) \to I(N)$. The diagram of R-modules

$$\begin{tikzcd}
0 \arrow[r] & I(M) \arrow[r] \arrow[d] & T(M) \arrow[r] \arrow[d, "T(\theta)"] & S(M) \arrow[r] \arrow[d, "S(\theta)"] & 0 \\
0 \arrow[r] & I(N) \arrow[r] & T(N) \arrow[r] & S(N) \arrow[r] & 0
\end{tikzcd}$$

commutes and the rows are exact. The three vertical maps are onto. By the Snake Lemma, Theorem 5.7.2, $\ker(T(\theta)) \to \ker(S(\theta))$ is onto. By Proposition 6.9.6 (5), the kernel of $T(\theta)$ is the ideal generated by K. This proves Part (6).

(8): For each j, let $\iota_j : M_j \to M_1 \oplus M_2$ be the natural injection homomorphism. By Part (4), there exists a natural homomorphism of graded rings $S(\iota_j) : S(M_j) \to S(M_1 \oplus M_2)$. By Exercise 5.4.10 there exists a unique R-algebra homomorphism

$$S(M_1) \otimes_R S(M_2) \xrightarrow{\gamma} S(M_1 \oplus M_2).$$

The reader should verify that γ is a graded homomorphism of graded R-algebras. To complete the proof, we construct the inverse mapping to γ. By Exercise 5.3.6, there exists a unique R-module homomorphism f such that the diagram

$$\begin{tikzcd}
M_j \arrow[rr, "\tau_j"] \arrow[dr, "\iota_j"'] & & S(M_j) \arrow[r, "\rho_j"] & S(M_1) \otimes_R S(M_2) \\
& M_1 \oplus M_2 \arrow[urr, dotted, "\exists f"'] & &
\end{tikzcd}$$

commutes. The maps ρ_j are as in Exercise 5.4.10. By Part (3) there exists a unique R-algebra homomorphism ϕ such that the diagram

$$\begin{tikzcd}
M_1 \oplus M_2 \arrow[rr, "f"] \arrow[dr, "\tau"'] & & S(M_1) \otimes_R S(M_2) \\
& S(M_1 \oplus M_2) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

commutes. The reader should verify that ϕ is a graded R-algebra homomorphism and that γ and ϕ are inverses of each other. □

9.4. The Exterior Algebra of a Module.

DEFINITION 6.9.10. Let R be a commutative ring, M an R-module, and $T(M)$ the tensor algebra of M. Let I be the ideal of $T(M)$ generated by the set $\{x \otimes x \mid x \in T^1(M)\}$. By Proposition 6.9.1, I is a graded ideal of $T(M)$. The *exterior algebra* of M, denoted $\bigwedge(M)$ (and pronounced "wedge"), is the graded R-algebra $T(M)/I$. The homogeneous component of degree n in $\bigwedge(M)$ is denoted $\bigwedge^n(M)$. In case the ring of scalars is ambiguous, we write $\bigwedge_R^n(M)$ instead of $\bigwedge^n(M)$ and $\bigwedge_R(M)$ instead of $\bigwedge(M)$. The coset of $x_1 \otimes x_2 \otimes \cdots \otimes x_n$ in $\bigwedge^n(M)$ is denoted $x_1 \wedge x_2 \wedge \cdots \wedge x_n$.

The reader should verify that the sequence $0 \to I \cap T^n(M) \to T^n(M) \to \bigwedge^n(M) \to 0$ is exact. In particular, $R = \bigwedge^0(M)$ and $M = \bigwedge^1(M)$.

PROPOSITION 6.9.11. *Let R be a commutative ring and M an R-module. The exterior algebra of M, $\bigwedge(M)$, satisfies the following.*

(1) *The R-algebra $\bigwedge(M)$ is generated by the set $M = \bigwedge^1(M)$.*

(2) *(Universal Mapping Property) Let $\tau : M \to \bigwedge(M)$ be the identity mapping of M onto $\bigwedge^1(M)$. For any R-algebra A and R-module homomorphism $f : M \to A$ such that $f(x)f(x) = 0$ for all $x \in M$, there exists a unique R-algebra homomorphism ϕ such that the diagram*

$$\begin{tikzcd} M \arrow[rr, "\tau"] \arrow[dr, "f"'] & & \bigwedge(M) \arrow[dl, dotted, "\exists\phi"] \\ & A & \end{tikzcd}$$

commutes. Up to an R-algebra isomorphism, $\bigwedge(M)$ is uniquely determined by this mapping property.

(3) *If $\theta : M \to N$ is an R-module homomorphism, then there exists a unique graded R-algebra homomorphism $\bigwedge(\theta)$ such that the diagram*

$$\begin{tikzcd} M \arrow[r, "\tau_M"] \arrow[d, "\theta"'] & \bigwedge(M) \arrow[d, "\bigwedge(\theta)"] \\ N \arrow[r, "\tau_N"] & \bigwedge(N) \end{tikzcd}$$

commutes.

(4) *Given an exact sequence of R-modules*

$$0 \to K \to M \xrightarrow{\theta} N \to 0$$

the graded R-algebra homomorphism $\bigwedge(\theta) : \bigwedge(M) \to \bigwedge(N)$ is onto, and the kernel of $\bigwedge(\theta)$ is the ideal in $\bigwedge(M)$ generated by the image of K in $\bigwedge^1(M)$.

(5) *$\bigwedge(M)$ is an alternating R-algebra.*

(6) *If M is a finitely generated R-module which has a generating set consisting of n elements, then $\bigwedge(M)$ is a finitely generated R-module and for all $p > n$, $\bigwedge^p(M) = 0$.*

(7) *$\bigwedge(M)$ is a covariant functor from the category of R-modules to the category of alternating R-algebras. $\bigwedge^n(M)$ is a covariant functor from the category of R-modules to the category of R-modules.*

(8) *If $R \to T$ is a homomorphism of commutative rings, then for all $n \geq 0$ there is a natural isomorphism of T-modules $\bigwedge_T^n(T \otimes_R M) \cong T \otimes_R \bigwedge_R^n(M)$ and a natural isomorphism of graded T-algebras $\bigwedge_T(T \otimes_R M) \cong T \otimes_R \bigwedge_R(M)$.*

(9) *Let M_1, M_2 be two R-modules. There is a natural isomorphism of graded R-algebras $\bigwedge(M_1) \otimes_R \bigwedge(M_2) \cong \bigwedge(M_1 \oplus M_2)$, where $\bigwedge(M_1) \otimes_R \bigwedge(M_2)$ denotes the graded tensor product.*

PROOF. (1): Is left to the reader.

(2): Similar to the proof of Proposition 6.9.9 (3).

(3): Is left to the reader.

(4): Similar to the proof of Proposition 6.9.9 (6).

(5): Assume $m > 0$ and $n > 0$. Let $u \in \bigwedge^m(M)$ and $v \in \bigwedge^n(M)$. Write $u = \sum u_i$ where each u_i is of the form $x_1 \wedge \cdots \wedge x_m$. Likewise, write $v = \sum v_i$ where each v_i is of the form $y_1 \wedge \cdots \wedge y_n$. By Exercise 6.9.9, $u_i \wedge v_j = (-1)^{mn} v_j \wedge u_i$ for each pair i, j. It follows that

$u \wedge v = (-1)^{mn} v \wedge u$, so $\bigwedge(M)$ is anticommutative. If m is odd, the reader should verify that $u \wedge u = 0$, hence $\bigwedge(M)$ is alternating.

(6): Suppose M is generated by $x_1, \dots, x_n$. Let $J = \{1, \dots, n\}$. For all $p \geq 1$, $\bigwedge^p(M)$ is generated by the finite set $\{x_{\sigma_1} \wedge \cdots \wedge x_{\sigma_p} \mid \sigma \in J^p\}$. Suppose $\sigma \in J^p$ and $p > n$. The pigeon hole principle says that $\sigma_i = \sigma_j$ for some $i \neq j$, and Exercise 6.9.7 says $x_{\sigma_1} \wedge \cdots \wedge x_{\sigma_p} = 0$. That is, $\bigwedge^p(M) = 0$ for all $p > n$.

(7) and (8): Are left to the reader.

(9): For each j, let $\iota_j : M_j \to M_1 \oplus M_2$ be the natural injection homomorphism. By Part (3), there exists a natural homomorphism of graded rings $\bigwedge(\iota_j) : \bigwedge(M_j) \to \bigwedge(M_1 \oplus M_2)$. By Proposition 6.9.4, there exists a unique graded R-algebra homomorphism

$$\bigwedge(M_1) \otimes_R \bigwedge(M_2) \xrightarrow{\gamma} \bigwedge(M_1 \oplus M_2).$$

To complete the proof, we construct the inverse mapping to γ. By Exercise 5.3.6, there exists a unique R-module homomorphism f such that the diagram

$$\begin{tikzcd}
M_j \arrow[r, "\tau_j"] \arrow[dr, "\iota_j"'] & \bigwedge(M_j) \arrow[r, "\rho_j"] & \bigwedge(M_1) \otimes_R \bigwedge(M_2) \\
& M_1 \oplus M_2 \arrow[ur, dotted, "\exists f"'] &
\end{tikzcd}$$

commutes. The maps ρ_j are as in Proposition 6.9.4. The reader should verify that the graded tensor product $\bigwedge(M_1) \otimes_R \bigwedge(M_2)$ is alternating. By Part (2) there exists a unique R-algebra homomorphism ϕ such that the diagram

$$\begin{tikzcd}
M_1 \oplus M_2 \arrow[rr, "f"] \arrow[dr, "\tau"'] & & \bigwedge(M_1) \otimes_R \bigwedge(M_2) \\
& \bigwedge(M_1 \oplus M_2) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

commutes. The reader should verify that ϕ is a graded R-algebra homomorphism and that γ and ϕ are inverses of each other. □

DEFINITION 6.9.12. Let R be a commutative ring and M and N two R-modules. For $n \geq 1$, let $M^n = M \oplus \cdots \oplus M$ denote the direct sum of n copies of M. As in Definition 3.4.1, 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 $i \neq j$.

EXAMPLE 6.9.13. Let $\tau : M^n \to \bigwedge^n(M)$ be the composite map

$$M^n \to T^n(M) \to \bigwedge^n(M)$$

defined by $(x_1, \dots, x_n) \mapsto x_1 \otimes \cdots \otimes x_n \mapsto x_1 \wedge \cdots \wedge x_n$. By Definition 5.4.2, Definition 6.9.10, and Exercise 6.9.7 it follows that τ is an alternating multilinear form.

PROPOSITION 6.9.14. *(Universal Mapping Property) Let R be a commutative ring and M and N two R-modules. For any alternating multilinear form $f : M^n \to N$ there exists a unique R-module homomorphism $\bar{f} : \bigwedge^n(M) \to N$ such that $\bar{f}\tau = f$.*

$$\begin{tikzcd}
M^n \arrow[rr, "\tau"] \arrow[dr, "f"'] & & \overset{n}{\bigwedge}(M) \arrow[dl, dotted, "\exists \bar{f}"] \\
& N &
\end{tikzcd}$$

commutes. Up to an R-module isomorphism, $\bigwedge^n(M)$ is uniquely determined by this mapping property.

PROOF. Since f is multilinear, it factors through the tensor product $T^n(M)$. That is, there exists a unique $f' : T^n(M) \to N$ such that the left side of the diagram

$$\begin{tikzcd}
M^n \arrow[r] \arrow[dr, "f"'] & T^n(M) \arrow[r] \arrow[d, "f'"] & \overset{n}{\bigwedge}(M) \arrow[dl, dotted, "\exists \bar{f}"] \\
& N &
\end{tikzcd}$$

commutes. The reader should verify that $f'(I \cap T^n(M)) = 0$. Therefore, f' factors through $\bigwedge^n(M)$, giving $\bar{f}$. The map $\bar{f}$ is unique because $\bigwedge^n(M)$ is generated by the image of τ. The last claim is proved as in the proof of Theorem 5.4.3. □

PROPOSITION 6.9.15. *Let R be a commutative ring, L an invertible R-module, and M a finitely generated projective R-module of constant rank n. Then*

$$\overset{n}{\bigwedge}(L \otimes_R M) = L^{\otimes n} \otimes_R \overset{n}{\bigwedge}(M).$$

PROOF. Let $\sigma : T^n(L \otimes_R M) \to T^n(L) \otimes_R T^n(M)$ be the R-module isomorphism induced by $(l_1 \otimes x_1, \dots, l_n \otimes x_n) \mapsto (l_1 \otimes \cdots \otimes l_n) \otimes (x_1 \otimes \cdots \otimes x_n)$. The reader should verify that the composite map

$$(L \otimes_R M)^n \to T^n(L \otimes_R M) \xrightarrow{\sigma} T^n(L) \otimes_R T^n(M) \to T^n(L) \otimes_R \overset{n}{\bigwedge}(M)$$

is alternating multilinear. By Proposition 6.9.14 this map factors through an R-module homomorphism $\bar{f} : \bigwedge^n(L \otimes M) \to T^n(L) \otimes_R \bigwedge^n(M)$. In the special case that M is a free R-module, it follows from Exercise 6.9.10 and Exercise 6.9.12 that $\bar{f}$ is an isomorphism. By Proposition 6.9.11 (8), the exterior power commutes with change of base. Localizing at a prime ideal P of R, the modules M and L are free. Therefore, $\bar{f}$ is locally an isomorphism. □

9.5. Exercises.

EXERCISE 6.9.1. Let R be a commutative ring and M a finitely generated projective R module with $\mathrm{Rank}_R(M) = n$. Show that $T^r(M)$ is a finitely generated projective R-module and $\mathrm{Rank}_R(T^r(M)) = n^r$.

EXERCISE 6.9.2. Let R be a commutative ring. Let $M = Ra$ be a free R-module of rank 1 with generator a. Show that there is an isomorphism of R-algebras $T(M) \to R[x]$ defined by the assignment $a \mapsto x$.

EXERCISE 6.9.3. Let R be a commutative ring. Let M be a rank one R-progenerator. Use Proposition 6.7.2, Exercise 6.7.3, and Exercise 6.9.2 to prove that the tensor algebra $T(M)$ is commutative.

EXERCISE 6.9.4. Let R be an integral domain with field of fractions K. Let M be a finitely generated torsion-free R-module. If $K \otimes_R M$ has dimension one over K, prove that the tensor algebra $T(M)$ is commutative.

EXERCISE 6.9.5. Let R be a commutative ring. Let M be a finitely generated free R-module of rank n with basis $m_1, \dots, m_n$. Show that there is an isomorphism of R-algebras $S(M) \to k[x_1, \dots, x_n]$ defined by the assignments $m_i \mapsto x_i$.

EXERCISE 6.9.6. Let R be a commutative ring and M a finitely generated projective R module with $\operatorname{Rank}_R(M) = n$. Show that $S^r(M)$ is a finitely generated projective R-module and $\operatorname{Rank}_R(S^r(M)) = \binom{n+r-1}{n-1}$.

EXERCISE 6.9.7. Prove that $x_1 \wedge x_2 \wedge \cdots \wedge x_n = 0$, if there exist distinct subscripts i and j such that $x_i = x_j$.

EXERCISE 6.9.8. For any permutation σ of the set $\{1, 2, \dots, n\}$, show that

$$x_{s_1} \wedge x_{s_2} \wedge \cdots \wedge x_{s_n} = \operatorname{sign}(\sigma) x_1 \wedge x_2 \wedge \cdots \wedge x_n.$$

EXERCISE 6.9.9. For any elements $x_1, \dots, x_m, y_1, \dots, y_n \in M$, show that

$$x_1 \wedge x_2 \wedge \cdots \wedge x_m \wedge y_1 \wedge y_2 \wedge \cdots \wedge y_n = (-1)^{mn} y_1 \wedge y_2 \wedge \cdots \wedge y_n \wedge x_1 \wedge x_2 \wedge \cdots \wedge x_m.$$

EXERCISE 6.9.10. Let R be a commutative ring and M a free R-module with basis $\{x_1, \dots, x_n\}$. Use Proposition 6.9.11 to prove that if $0 \le m \le n$, then $\bigwedge^m(M)$ is a free R-module of rank $\binom{n}{m}$ with basis $\{x_{i_1} \wedge \cdots \wedge x_{i_m} \mid 1 \le i_1 < \cdots < i_m \le n\}$.

EXERCISE 6.9.11. Let R be a commutative ring and M a finitely generated projective R-module. Prove:

(1) $\bigwedge^m(M)$ is a finitely generated projective R-module.
(2) $\bigwedge(M)$ is a finitely generated projective R-module.
(3) If M has constant rank n, then $\bigwedge^m(M)$ has constant rank $\binom{n}{m}$ and $\bigwedge(M)$ has constant rank 2^n.

EXERCISE 6.9.12. Let R be a commutative ring and $M = P_1 \oplus \cdots \oplus P_m$, where each P_i is an invertible R-module (see Definition 6.7.6). Prove:

(1) $\bigwedge^m(M) \cong P_1 \otimes_R P_2 \otimes_R \cdots \otimes_R P_m$.
(2) Suppose $N = Q_1 \oplus \cdots \oplus Q_n$, where each Q_i is an invertible R-module. If $M \cong N$, then $m = n$ and $P_1 \otimes_R P_2 \otimes_R \cdots \otimes_R P_m \cong Q_1 \otimes_R Q_2 \otimes_R \cdots \otimes_R Q_n$.

EXERCISE 6.9.13. Let R be a commutative ring, S a commutative R-algebra, and M an S-module. Show that $T^n_R(M)$ is a left $T^n_R(S)$-module where the multiplication rule is $(s_1 \otimes \cdots \otimes s_n)(x_1 \otimes \cdots \otimes x_n) = (s_1x_1 \otimes \cdots \otimes s_nx_n)$. Prove the following.

(1) If M is a finitely generated S-module, then $T^n_R(M)$ is a finitely generated $T^n_R(S)$-module.
(2) If M is a projective S-module, then $T^n_R(M)$ is a projective $T^n_R(S)$-module.
(3) If M is an S-module generator, then $T^n_R(M)$ is a $T^n_R(S)$-module generator.
(4) If A is an S-algebra, then $T^n_R(A)$ is a $T^n_R(S)$-algebra.

EXERCISE 6.9.14. Let R be a commutative ring and $M = R^n$ the free R-module of rank n. Let $\theta : M \to M$ be an R-module homomorphism, and $\bigwedge^n(\theta) : \bigwedge^n(M) \to \bigwedge^n(M)$ the R-module homomorphism guaranteed by Proposition 6.9.11 (3). By Exercise 6.9.10, $\bigwedge^n(M) \cong R$. Show that $\bigwedge^n(\theta) : R \to R$ is left multiplication by $\det(\theta)$, the determinant of θ (Section 3.4.1).

10. A Theorem of Bass

In this short section we prove a theorem of Bass (Theorem 6.10.2) which was stated without proof in [**10**, Theorem 14.2.1]. The proof given in [**5**, Proposition (4.6), p. 476] is K-theoretic, whereas the proof given below is based on the method suggested in the paragraph immediately preceding [**21**, Theorem III.17] and utilizes only theorems proven in this book or [**10**]. The main idea for the proof is the following lemma.

LEMMA 6.10.1. *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 $\varphi \in \operatorname{Hom}_R(M,M)$ to the diagonal homomorphism $\oplus_{i=1}^n \varphi \in \operatorname{Hom}_R(M^{(n)},M^{(n)})$ defines a monomorphism of rings. If R is commutative, Δ is an R-algebra homomorphism.

PROOF. The proof is left to the reader. □

THEOREM 6.10.2. *(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 5.4.24, 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 6.4.7, 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 6.7.5 and 6.7.3, 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 6.10.1 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 5.9.1 (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 5.9.3 (6), M^* is an R-progenerator. By Proposition 5.4.23, $\operatorname{Hom}_R(M,M)$ is an R-progenerator module. By Proposition 6.5.6, $\operatorname{Hom}_R(M,M)$ 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 6.5.7, $\operatorname{Hom}_R(M,M) \otimes_R S$ 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

$$\begin{tikzcd}
\operatorname{Hom}_S(M \otimes_R S, M \otimes_R S) \arrow[r, "\Delta"] & \operatorname{Hom}_S((M \oplus N) \otimes_R S, (M \oplus N) \otimes_R S) \\
\operatorname{Hom}_R(M,M) \otimes_R S \arrow[u, "\cong"] & \operatorname{Hom}_R(M \oplus N, M \oplus N) \otimes_R S \arrow[u, "\cong"'] \\
\operatorname{Hom}_R(M,M) \arrow[u, "\subseteq"] \arrow[r, dashed, "\exists \delta"] & \operatorname{Hom}_R(M \oplus N, M \oplus N) \arrow[u, "\subseteq"']
\end{tikzcd} \tag{6.22}$$

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 (see [**10**, § 5.3]). 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 faithfully flat descent ([**10**, Proposition 5.3.4]), there exists an R-algebra homomorphism δ such that diagram (6.22) 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 5.9.2, 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. □

CHAPTER 7

Artinian Rings

1. The Jacobson Radical and Nakayama's Lemma

DEFINITION 7.1.1. Let R be any ring and M a left R-module. If N is a submodule of M, then N is called *maximal* in case $N \neq M$ and whenever there is a submodule P such that $N \subseteq P \subseteq M$, then $N = P$ or $P = M$. If $N \subseteq M$ is a maximal submodule of M, then 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 7.1.2. *$\mathrm{J}(R)$ 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 5.5.7). Then $\rho_r(\mathrm{J}(R)) = \mathrm{J}(R) \cdot r \subseteq \mathrm{J}(R)$. □

THEOREM 7.1.3. *(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 1.3.3, $R(1+x)$ 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 $\{x_1, \dots, x_n\}$ 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 7.1.2, $b_i = a_i r_i \in \mathrm{J}(R)$, 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. □

COROLLARY 7.1.4. *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 7.1.2 both $\mathrm{J}_r(R)$ and $\mathrm{J}(R)$ are two-sided ideals of R. It follows from Theorem 7.1.3 (2) that $1+\mathrm{J}(R)$ consists of units of R. Apply a right-sided version of Theorem 7.1.3 to the right ideal $\mathrm{J}(R)$ and conclude that $\mathrm{J}(R) \subseteq \mathrm{J}_r(R)$. The converse follows by symmetry. □

COROLLARY 7.1.5. *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 $1+I \subseteq \mathrm{Units}(R)$. □

COROLLARY 7.1.6. *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 6.6.3, 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 7.1.3 (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 $\mathrm{J}(R)^n = 0$. □

COROLLARY 7.1.7. *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 7.1.3 (4), $M = R$, a contradiction.

(2): Let $x \in \mathrm{J}(R)$ and $a \in R$. By Theorem 7.1.3, $1+ax \in \mathrm{Units}(R)$, 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 7.1.3, $M = 0$. By (3) implies (1) of Theorem 7.1.3, $\mathrm{J}(R)A \subseteq \mathrm{J}(A)$. □

1.1. Exercises.

EXERCISE 7.1.1. 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 generalization of Exercise 2.1.19:

(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 7.1.2. Let R be a ring and $\mathrm{J}(R) \supseteq B \supseteq A$ a chain of ideals. Prove this generalization of Exercise 3.2.1: $\mathrm{Units}(R) \supseteq 1+B \supseteq 1+A$ 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 7.1.3. 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 7.1.4. 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 6.4.2.)

EXERCISE 7.1.5. 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.)

2. Semisimple Modules and Semisimple Rings

THEOREM 7.2.1. *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 1.3.3, 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 $\left(\sum_{i\in J} M_i\right) + M_k$ 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

$$\Big(\sum_{i\in J} M_i\Big) \bigcap N = 0. \tag{7.1}$$

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 (7.1) we see that $x = 0$. Then $J \cup \{k\}$ satisfies (7.1) 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. □

DEFINITION 7.2.2. Let R be a ring and M an R-module. If M satisfies any of the properties of Theorem 7.2.1, then M is called *semisimple*.

THEOREM 7.2.3. *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 5.2.3, 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 6.2.4, $\mathrm{J}(R) = Re_1$ and $L = Re_2$ and $e_1e_2 = 0$ and $1 = e_1 + e_2$. By Nakayama's Lemma (Theorem 7.1.3), 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 7.2.1 (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 7.1.5 that $L_1^2 \neq 0$. By Lemma 6.2.4 (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 6.2.4 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 7.2.4. The ring R is called *semisimple* if R satisfies any of the equivalent conditions of Theorem 7.2.3.

EXAMPLE 7.2.5. Let R be an artinian ring. Then $R/\mathrm{J}(R)$ satisfies Theorem 7.2.3 (5), hence is semisimple.

3. Simple Rings and the Wedderburn-Artin Theorem

DEFINITION 7.3.1. 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 7.2.3 (5) hence is semisimple.

EXAMPLE 7.3.2. Let D be a division ring and M a finite dimensional D-vector space. Let $S = \mathrm{Hom}_D(M,M)$. By Exercise 6.6.11, S is artinian. By Corollary 5.9.4 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 7.3.5.

THEOREM 7.3.3. *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 7.2.3 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 $2 \le i \le m$ 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 7.2.3, 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 2.2.6, 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 7.1.3 (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 $n \ge 2$. 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 7.3.4. *(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 7.3.5. *(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 we can write R as an internal direct sum $R = L_1 \oplus \cdots \oplus L_n$ where each L_i is a minimal left ideal of R. But R is simple, so $L_1 \cong \ldots \cong L_n$ by Theorem 7.3.3. Set $M = L_1$ and $D = \operatorname{Hom}_R(M,M)$. By Lemma 7.3.4, D is a division ring. Since $L_1 = Re_1$ for some idempotent e_1, M is finitely generated. By Theorem 7.2.3, M is projective. By Lemma 5.2.10, 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 5.9.3 (1), $R \cong \operatorname{Hom}_D(M,M)$. By Corollary 5.9.3 (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 7.3.3, $M \cong M'$ as R-modules. □

3.1. Exercises.

EXERCISE 7.3.1. Let k be a field and A a finite dimensional k-algebra. Let N be a nilpotent left ideal of A such that $\dim_k(N) \leq 2$. Prove that N is commutative. That is, $xy = yx$ for all x and y in N.

EXERCISE 7.3.2. 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 3.3.10.

EXERCISE 7.3.3. 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 3.3.10.

EXERCISE 7.3.4. 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 3.3.10.

EXERCISE 7.3.5. 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 7.3.6. 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 7.3.7. Let R be a semisimple ring and M an R-module. Prove that M is artinian if and only if M is noetherian.

EXERCISE 7.3.8. Prove the converse of Theorem 7.3.3 (2). That is, a finite direct sum of simple rings is a semisimple ring.

4. Commutative Artinian Rings

THEOREM 7.4.1. *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 7.2.5. By Lemma 6.6.9, since M is artinian, so are the submodules $J^n M$ and the quotient modules $J^n M / J^{n+1} M$, for all $n \geq 0$. By Exercise 3.1.1, the quotient module $J^n M / J^{n+1} M$ is artinian over R/J. By Exercise 7.3.7, $J^n M / J^{n+1} M$ is noetherian as a R/J-module. Again by Exercise 3.1.1, $J^n M / J^{n+1} M$ is noetherian as an R-module. For each $n \geq 0$, the sequence

$$0 \to J^{n+1} M \to J^n M \to \frac{J^n M}{J^{n+1} M} \to 0$$

is exact. By Corollary 7.1.6, for some r, we have $J^{r+1} = (0)$. Taking $n = r$ in the exact sequence, Lemma 6.6.9 implies $J^r M$ is noetherian. A finite induction argument using Lemma 6.6.9 and the exact sequence proves $J^n M$ is noetherian for $n = r, \dots, 1, 0$. □

LEMMA 7.4.2. *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 6.3.7, $I(V(0)) = \mathrm{Rad}_R(0) = \mathfrak{m}$. 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 3.1.1, the R-submodules of $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ correspond to $R/\mathfrak{m}$-subspaces. By Exercise 6.6.10, $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ 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 6.6.9 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 7.4.3. *Let R be a commutative artinian ring.*

(1) Every prime ideal of R is maximal.
(2) The nil radical $\operatorname{Rad}_R(0)$ is equal to the Jacobson radical $\mathrm{J}(R)$.
(3) There are only finitely many maximal ideals in R.
(4) The nil radical $\operatorname{Rad}_R(0)$ is nilpotent.

PROOF. (1): Let P be a prime ideal in R. Then R/P is an artinian integral domain. By Exercise 6.6.6, R/P is a field.

(2): This is Exercise 7.4.1.

(3): Theorem 7.4.1 implies R is noetherian, and Proposition 6.6.14 implies $\operatorname{Spec} R$ has only a finite number of irreducible components. By Corollary 6.6.15, 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 7.1.6. □

PROPOSITION 7.4.4. *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 11.2.1).
(3) R is an R-module of finite length.

PROOF. By Proposition 6.6.20, it is enough to show (1) and (2) are equivalent.

(1) implies (2): By Theorem 7.4.1, R is noetherian. By Proposition 7.4.3, every prime ideal of R is maximal.

(2) implies (1): By Theorem 6.6.16, R has a decomposition $R = R_1 \oplus \cdots \oplus R_n$ where each R_i has only two idempotents. By Exercise 6.6.1 it suffices to show each R_i is artinian. Therefore, assume $\operatorname{Spec} R$ is connected. By Proposition 1.4.7, $\operatorname{Spec} R$ 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 7.4.2, R is artinian. □

PROPOSITION 7.4.5. *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 7.4.3 (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 7.1.3), $\mathfrak{m}^n = 0$. If P is a prime ideal of R, then $\mathfrak{m}^n \subseteq P$. By Exercise 6.3.4, $\mathfrak{m} = \operatorname{Rad}(\mathfrak{m}^n) \subseteq \operatorname{Rad}(P) = P$. This proves that $P = \mathfrak{m}$, so by Proposition 7.4.4, R is artinian. □

THEOREM 7.4.6. *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 7.4.3, $\operatorname{Max} R = \operatorname{Spec} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ is a finite set. So the topological space $\operatorname{Spec} R$ has the discrete topology. By Theorem 6.6.16, 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 6.2.5.

(3): Start with the decomposition $R \cong R_1 \oplus \cdots \oplus R_n$ of Part (1) and apply Exercise 6.1.4. □

4.1. Finitely Generated Projective of Constant Rank is Free.

COROLLARY 7.4.7. *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 7.4.6, R is the finite direct sum of local rings. By Exercise7.1.3, M is a free module of rank r. □

COROLLARY 7.4.8. *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 7.4.7, $M \otimes_R k = M \otimes_S (S \otimes_R k)$ is a free $S \otimes_R k$-module of constant rank s. Proposition 3.1.33 applies to the trio $k, S \otimes_R k, M \otimes_R k$. Applying Proposition 6.4.2 we get the rank formula over the local ring $R_{\mathfrak{p}}$. □

4.2. Exercises.

EXERCISE 7.4.1. Let R be a commutative artinian ring. Prove that tThe Jacobson radical $\mathrm{J}(R)$ is equal to the nil radical $\operatorname{Rad}_R(0)$.

EXERCISE 7.4.2. 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 7.4.3. 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 7.4.4. 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 7.4.5. 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 7.4.6. 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 7.4.7. 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 7.4.8. 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 $\mathfrak{m}R_{\mathfrak{m}}/\mathfrak{m}^2R_{\mathfrak{m}}$ is a k-vector space of dimension n.

EXERCISE 7.4.9. 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.

CHAPTER 8

Primary Decomposition in Noetherian Rings and Modules

1. Prime Ideals and Primary Ideals

1.1. Prime Ideals.

DEFINITION 8.1.1. 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 2.1.22 shows that this definition agrees with Definition 2.1.19.

LEMMA 8.1.2. *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 $I \subseteq P_1 \cup P_2 \cup \dots \cup P_n$, 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 $I \subseteq P_1 \cup \dots \cup P_n$ 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 $I \subseteq P_1 \cup \dots \cup P_{n-1}$, then by induction $I \subseteq P_i$ for some i. Therefore we assume $S = I - (P_1 \cup \dots \cup P_{n-1})$ 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. □

LEMMA 8.1.3. *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. □

1.2. Primary Ideals in a Commutative ring. In this section, R is a commutative ring.

LEMMA 8.1.4. *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 8.1.4 is called a *primary ideal*. In Definition 8.3.2, the more general notion of primary submodule is introduced. The reader should verify that a prime ideal in R is a primary ideal.

PROPOSITION 8.1.5. *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 6.3.7, 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 8.1.2. □

By Proposition 8.1.5 (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 8.1.6. *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 $d_i \ge e_i$, so $N^n = 0$.

(2): Apply (1) to the ring R/I. □

COROLLARY 8.1.7. *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 8.1.5.
(2) implies (3): Follows from Proposition 8.1.6.
(3) implies (2): Follows from Exercise 6.3.4. □

1.3. Exercises.

EXERCISE 8.1.1. 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 8.1.2. 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 8.1.3. 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 8.1.4. 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 8.1.5. 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 8.1.6. 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.

2. The Associated Primes of a Module

In this section R is a commutative noetherian ring.

LEMMA 8.2.1. *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 8.2.1, 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 8.2.2. *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 8.2.1. 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. □

PROPOSITION 8.2.3. *Let R be a commutative 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 8.2.2 (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 8.2.2 (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 8.2.2 (2), we know $N \subsetneq F$. By Proposition 8.2.2 (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, $\mathfrak{p} \in \Phi$. □

LEMMA 8.2.4. *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 6.3.9, 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 8.2.1, 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 8.2.5. *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 8.2.3. 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 6.1.4). If $\mathfrak{p} \in \operatorname{Assoc}_R(N)$, then $\mathfrak{p} \cap W \neq \emptyset$. By Lemma 8.2.4, $\operatorname{Assoc}_R(W^{-1}N) = \emptyset$. By Proposition 8.2.2 (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 8.2.6. *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 8.2.4, $W^{-1}P$ is an associated prime of $W^{-1}M = M_P$. By Proposition 8.2.2, it follows that $M_P \neq 0$.

(2): Let $P \in \operatorname{Supp}(M)$. Then $M_P \neq 0$. By Proposition 8.2.2, M_P has an associated prime in R_P. By Lemma 8.2.4, 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 $\operatorname{Assoc}_R(M)$. If P is a minimal member of $\operatorname{Supp}(M)$, then $\operatorname{Supp}(M_P)$ contains only one prime, namely PR_P. In this case, it follows that P is a minimal element in $\operatorname{Assoc}(M)$.

(3): Follows from the arguments in (1) and (2).

(4): By Exercise 8.2.1, the support of the module R/I is $V(I)$. □

THEOREM 8.2.7. *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 $P_i \in \operatorname{Spec} R$ 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 $\operatorname{Assoc}(M) \subseteq \{P_1, \dots, P_n\} \subseteq \operatorname{Supp}(M)$.
(3) $\operatorname{Assoc}(M)$ is a finite set.

PROOF. (1): Assume $M \neq (0)$. By Proposition 8.2.2, $\operatorname{Assoc}(M) \neq \emptyset$, 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 8.2.2, $\operatorname{Assoc}(M/N) \neq \emptyset$. By Lemma 8.2.1 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 8.2.2 (4), $\operatorname{Assoc}(M_i/M_{i-1}) = \{P_i\}$. Proposition 8.2.2 (5), applied $n-1$ times, yields

$$\begin{aligned}\operatorname{Assoc}(M) &\subseteq \operatorname{Assoc}(M_1) \cup \operatorname{Assoc}(M_2/M_1) \cup \cdots \cup \operatorname{Assoc}(M_n/M_{n-1})\\ &\subseteq \{P_1, \dots, P_n\}.\end{aligned}$$

By Exercise 8.2.1, the support of the R-module R/P_i is $V(P_i)$, which contains P_i. By Exercise 8.2.2, $P_i \in \operatorname{Supp}(M_i) \subseteq \operatorname{Supp}(M)$. This proves Part (2).

(3): This follows straight from Part (2). □

2.1. Exercises.

EXERCISE 8.2.1. 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 8.2.2. 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 8.2.3. 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 8.2.2 and the exact sequence $\bigoplus_{\alpha \in I} M_\alpha \to M \to 0$.)

EXERCISE 8.2.4. 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 8.2.1, Exercise 8.2.3, and the isomorphism $Rx_\alpha \cong R/\operatorname{annih}(x_\alpha)$.)

EXERCISE 8.2.5. 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 8.1.3 and Lemma 6.3.3.)

EXERCISE 8.2.6. 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 8.2.4 and Exercise 8.2.5.)

EXERCISE 8.2.7. 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 8.1.6.)

EXERCISE 8.2.8. 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 8.2.9. 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 8.2.10. Let A and R be as in Exercise 8.1.6. 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 8.2.11. 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 8.2.12. 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 8.2.13. 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 3.2.4).
(2) $\operatorname{Assoc}_R(M) = \{(0)\}$.
(3) $\operatorname{Hom}_R(M,M)$ is torsion free.

(Hint: Exercises 8.2.11, and 8.2.12.)

EXERCISE 8.2.14. 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 8.2.12.)

EXERCISE 8.2.15. Let R be an integral domain and M and N two R-modules. Prove that if N is torsion free (Definition 3.2.4), then $\operatorname{Hom}_R(M,N)$ is torsion free. (Hint: Prove this directly, it does not require any theorem from this chapter.)

3. Primary Decomposition Theorem

3.1. Primary Submodules.

PROPOSITION 8.3.1. *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 8.2.2 (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 8.2.6 (3), P is the unique minimal member of $\operatorname{Supp}(Rx)$. By Exercise 8.2.6, 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 $P \subseteq Q$. □

DEFINITION 8.3.2. 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 8.3.1. 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 8.1.4 and Proposition 8.3.1 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 8.3.3. *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 8.2.2 (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 $M/(S \cap T)$. □

3.2. Primary Decomposition.

DEFINITION 8.3.4. 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 8.3.3 says that we can merge by intersection all of the Y_i that have the same associated prime.

LEMMA 8.3.5. *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 8.2.2, 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 8.3.6. *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 8.2.4, $\operatorname{Assoc}_R\big((M/N)_Q\big) = \emptyset$. But Proposition 8.2.2 (2) implies $M_Q/N_Q = (M/N)_Q = 0$.

(2): By Proposition 8.3.1, 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 8.3.7. *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 8.3.6 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 6.1.1, we get

$$\begin{aligned} M \cap N_{P_i} &= M \cap (Y_1 \cap \cdots \cap Y_n)_{P_i} \\ &= M \cap \Big((Y_1)_{P_i} \cap \cdots \cap (Y_n)_{P_i}\Big) \\ &= M \cap (Y_i)_{P_i} \\ &= Y_i \end{aligned}$$

(2): Follows from (1). □

THEOREM 8.3.8. *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 1.3.3, there exists a maximal member, say Y, in $\mathscr{C}$. Because $P \in \operatorname{Assoc}(M)$ and $P \notin \operatorname{Assoc}(Y)$, Proposition 8.2.2 (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 8.2.2 (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 8.2.2 (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 8.2.7. □

3.3. Exercises.

EXERCISE 8.3.1. 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) $P^{(n)} = P^n R_P \cap R$.

CHAPTER 9

Completion of a Topological Module

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 9.1.1. 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 $p(x) = \operatorname{char.poly}_M(x)$ be the characteristic polynomial of M. Then $p(x)$ is a monic polynomial of degree n in $R[x]$. By Cayley-Hamilton (Theorem 3.4.12) we know $p(M) = 0$. This shows A is integral over R.

PROPOSITION 9.1.2. *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 3.3.2. 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 5.5.4,

$\beta\alpha(u)$ satisfies a monic polynomial $p \in R[x]$. Therefore, every $u \in R[a]$ is integral over R. □

THEOREM 9.1.3. *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 9.1.2 (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 Exercise 3.1.2, $S[a_n] = R[a_1, \dots, a_n]$ 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 9.1.2, 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 $p = s_0 + s_1x + \cdots + s_{n-1}x^{n-1} + x^n$. 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 Exercise 3.1.2, $T[a] = R[s_0, \dots, s_{n-1}, a]$ 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. □

LEMMA 9.1.4. *Let A be a faithful integral R-algebra and assume A has no zero divisors. Then A is a division ring if and only if R is a field.*

PROOF. Assume A is a division ring and $x \in R - (0)$. Then $x^{-1} \in A$ is integral over R. There exist $n \geq 1$ and $r_i \in R$ such that

$$x^{-n} + r_{n-1}x^{1-n} + \cdots + r_1x^{-1} + r_0 = 0.$$

Multiply by x^{n-1} and get

$$x^{-1} + r_{n-1} + r_{n-2}x + \cdots + r_1x^{n-2} + r_0x^{n-1} = 0$$

which shows $x^{-1} \in R$. Thus R is a field.

Assume R is a field and $y \in A - (0)$. Then y is integral over R. There exist $n \geq 1$ and $r_i \in R$ such that

$$y^n + r_{n-1}y^{n-1} + \cdots + r_1y + r_0 = 0.$$

If we choose the degree n to be minimal among all such dependence relations for y, then we can assume $r_0 \neq 0$. Since R is a field, divide this

$$r_0 = -y(y^{n-1} + r_{n-1}y^{n-2} + \cdots + r_1)$$

by r_0 to see that

$$y^{-1} = -r_0^{-1}(y^{n-1} + r_{n-1}y^{n-2} + \cdots + r_1)$$

is an element of A, so A is a division ring. □

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.

EXAMPLE 9.1.5. If R is a unique factorization domain (UFD) with quotient field K, then R is integrally closed in K. To see this, let $n/d \in K$ where we assume $\operatorname{GCD}(n,d) = 1$. Suppose $p(x) = x^m + r_{m-1}x^{m-1} + \cdots + r_1x + r_0$ is a monic polynomial in $K[x]$ and $p(n/d) = 0$. Then $d^m p(n/d) = 0$, which shows that $n^m \in Rd$. Since d and n have no common irreducible factor, we conclude that d is a unit of R. That is, $n/d \in R$.

LEMMA 9.1.6. *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 9.1.1, $S_W = R_W \otimes_R S$ 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 $t/w = (dt)/(dw) \in S_W$. □

PROPOSITION 9.1.7. *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 9.1.6, S_P is the integral closure of R_P in K for each $P \in \operatorname{Spec} R$. The rest follows from Exercise 6.5.1. □

LEMMA 9.1.8. *(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 4.3.5, let L/K be an extension of fields such that L is a splitting field for f over K. By Theorem 9.1.3 (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. □

THEOREM 9.1.9. *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 9.1.8, both f and h lie in $R[x]$. □

THEOREM 9.1.10. *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. See [**10**, Theorem 4.6.10]. □

REMARK 9.1.11. In the terminology of Definition 13.1.2, Theorem 9.1.10 says that S is an R-lattice in L.

1.3. Exercises.

EXERCISE 9.1.1. 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 9.1.2. 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 9.1.3. Let R be an integral domain with quotient field K. Let L/K be a finite field extension and let S be the integral closure of R in L. Show that L is equal to the quotient field of S.

EXERCISE 9.1.4. 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 9.1.5. Let S be a commutative faithfully flat R-algebra. Prove:

(1) If S is an integrally closed integral domain, then R is an integrally closed integral domain.
(2) 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 12.1.4, this says if S is a normal ring, then R is a normal ring.

EXERCISE 9.1.6. 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.

2. Some Theorems of Hilbert

2.1. The Hilbert Basis Theorem.

THEOREM 9.2.1. *(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 6.6.7, 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 6.6.12 and

Corollary 6.6.10 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 6.6.12.

(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 6.6.13 (1) that S is noetherian. □

Theorem 9.2.2 is stated here for reference only. It will be proved later as Corollary 9.4.26 (2).

THEOREM 9.2.2. *If R is a commutative noetherian ring, then the power series ring $R[[x_1, \dots, x_n]]$ over R in n variables is a noetherian ring.*

PROPOSITION 9.2.3. *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 9.1.3 (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

$$\begin{aligned} x_i &= \sum_{j=1}^{n} b_{ij}y_j \\ y_iy_j &= \sum_{k=1}^{n} b_{ijk}y_k \end{aligned} \tag{9.1}$$

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 9.2.1 (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 (9.1), the reader should verify that

$$c = p(\sum_{j=1}^{n} b_{1j}y_j, \sum_{j=1}^{n} b_{2j}y_j, \dots)$$

is in $B_0y_1 + B_0y_2 + \cdots + B_0y_n$. Therefore C is finitely generated as a B_0-module. By Corollary 6.6.12, 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 9.2.4. *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. (2) and (3) are equivalent: By Proposition 4.1.9.

(2) implies (1): follows from Theorem 4.1.4.

(1) implies (3): Let $F = k[x_1, \dots, x_n]$. If each x_i is algebraic over k, then Proposition 4.1.9 implies $\dim_k(F) < \infty$ and we are done. For contradiction's sake, assume otherwise. Re-order and assume x_1 is transcendental over k. Then $F = k(x_1)[x_2, \dots, x_n]$. If $x_2, \dots, x_n$ are algebraic over k, then $\dim_{k(x_1)}(F) < \infty$. Assume otherwise. Re-order and assume x_2 is transcendental over $k(x_1)$. Then $F = k(x_1, x_2)[x_3, \dots, x_n]$. After a finite iteration, we assume $x_1, \dots, x_r$ are algebraically independent over k and $F = k(x_1, \dots, x_r)[x_{r+1}, \dots, x_n]$ is algebraic over the field $K = k(x_1, \dots, x_r)$. Then Proposition 4.1.9 implies $\dim_K(F) < \infty$. By Proposition 4.1.3, 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 9.2.3 to the tower of rings $k \subseteq K \subseteq F$, we conclude that $K = k[y_1, \dots, y_s]$ is finitely generated as a k-algebra. 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 $g = g_1 g_2 \cdots g_s$ 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. □

COROLLARY 9.2.5. *(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 9.2.4 to the field $F = A/\mathfrak{m}$. □

2.2. Algebraic Varieties.

DEFINITION 9.2.6. Let k be any field. Let $n \geq 0$. Define *affine n-space over k* to be

$$\mathbb{A}^n_k = \{(a_1, \dots, a_n) \mid a_i \in k\}.$$

We write simply $\mathbb{A}^n$ if k is apparent. Let

$$A = k[x_1, \dots, x_n]$$

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 $Y = Z(T)$.

THEOREM 9.2.7. *Let k be an algebraically closed field and $A = k[x_1, \dots, x_n]$.*

(1) *If M is a maximal ideal in A, then there exist elements $a_1, a_2, \dots, a_n$ in k such that $M = (x_1 - a_1, \dots, x_n - a_n)$.*
(2) *If I is a proper ideal in A, then $Z(I)$ is nonempty.*

PROOF. (1): Since k is algebraically closed, Corollary 9.2.5 says the natural map $k \to A/M$ is onto. There exist $a_1, \dots, a_n \in k$ such that $a_i + M = x_i + M$ for $i = 1, \dots, n$. 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 $\{(a_1, \ldots, a_n)\}$. □

PROPOSITION 9.2.8. *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 $\mathbb{A}^n$, 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

$$Y_1 \cup Y_2 = Z(T_1T_2),$$

where $T_1T_2 = \{f_1f_2 \mid f_1 \in T_1, f_2 \in T_2\}$. 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 $(f_1f_2)(P) = 0$. Similarly for $P \in Y_2$.

Step 2: Let $P \in Z(T_1T_2)$ 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 $(f_1f_2)(P) = 0$ 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 9.2.9. Let k be any field. For any $Y \subseteq \mathbb{A}^n$, we define the ideal of Y in $A = k[x_1, \ldots, x_n]$ 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.

THEOREM 9.2.10. *(Hilbert's Nullstellensatz) Let k be an algebraically closed field and I an ideal in $A = k[x_1, \ldots, x_n]$. Then* $\operatorname{Rad}(I) = I(Z(I))$.

PROOF. By Exercise 9.2.1, $\operatorname{Rad}(I) \subseteq I(Z(I))$. Let $f \in A - \operatorname{Rad}(I)$. We prove that there exists $x \in Z(I)$ such that $f(x) \neq 0$. By Lemma 6.3.7, there exists a prime ideal $P \in \operatorname{Spec} A$ such that $I \subseteq P$ 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 9.2.5 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 $I \subseteq P \subseteq M$. By Theorem 9.2.7, $Z(M)$ is a singleton set $\{x\}$. This shows $x \in Z(I)$ and $f(x) \neq 0$. □

PROPOSITION 9.2.11. *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 9.2.10.
(5) The proof of Lemma 6.3.8 applies. □

COROLLARY 9.2.12. *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 9.2.11. The last part can be proved as in Lemma 6.3.10. □

EXAMPLE 9.2.13. 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 $\operatorname{Hom}_k(A,A)$. As in Example 3.5.3, the norm $N_k^A : A \to k$ is a homogeneous polynomial function on A of degree n and the trace $T_k^A : A \to k$ 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 9.2.6). That is, an element $a_1\alpha_1 + \cdots + a_n\alpha_n \in A$ corresponds to the point $(a_1,\dots,a_n) \in \mathbb{A}_k^n$. With this identification, the norm $N_k^A : A \to k$ corresponds to a homogeneous polynomial in $k[x_1,\dots,x_n]$ of degree n. Using Exercise 3.4.6 we see that an element α in A is invertible if and only if $N_k^A(\alpha) \neq 0$. 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.

2.3. Exercises.

EXERCISE 9.2.1. 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 9.2.2. 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 9.2.3. 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 9.2.4. 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 9.2.5. The purpose of this exercise is to prove the converse of Exercise 6.6.12 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. (Hint: Use Theorem 7.4.6 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 9.2.5.)

EXERCISE 9.2.6. 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 9.2.7. 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 9.2.8. 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) $R/\mathfrak{m} = \varinjlim (R_\alpha/\mathfrak{m}_\alpha)$.

3. *I*-adic Topology and Completion

3.1. 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

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq M_3 \dots.$$

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 1.4, 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 5.8.20. 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 9.3.1. *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). □

LEMMA 9.3.2. *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. □

DEFINITION 9.3.3. 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 9.3.4. *In the setting of Definition 9.3.3, 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 9.3.5. 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 9.3.4 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 9.3.2. 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 9.3.6. *In the setting of Definition 9.3.3, 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. □

3.2. Functorial Properties of Completion.

PROPOSITION 9.3.7. *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 5.8.12, 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 5.8.13, 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 5.8, α induces a homomorphism $\varprojlim A/A_n \to \varprojlim B/B_n$.

PROPOSITION 9.3.8. *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 5.7.2 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 5.8.19 to the exact sequence of morphisms of inverse systems $\{A/A_n\} \xrightarrow{\alpha} \{A/B_n\} \xrightarrow{\beta} \{C/C_n\}$. □

COROLLARY 9.3.9. *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 9.3.8 and Proposition 9.3.7. □

COROLLARY 9.3.10. *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 9.3.9 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 9.3.11. *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 $1+x$ is a unit of R for every $x \in I$. In the terminology of Nakayama's Lemma (Theorem 7.1.3), I is contained in the Jacobson radical of R.*

PROOF. 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, hence converges in R. Now $(1-x)s = 1-(x, x^2, x^3, \dots)$ is equal to 1 since the Cauchy sequence $(x, x^2, x^3, \dots)$ converges to 0. □

COROLLARY 9.3.12. *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 9.3.10 (1), $\hat{R}/\hat{\mathfrak{m}} \cong R/\mathfrak{m}$, so $\hat{\mathfrak{m}}$ is a maximal ideal of $\hat{R}$. By Corollary 9.3.10 (2), $\hat{R}$ is separated and complete with respect to the topology associated to the filtration $(\mathfrak{m}^i)\widehat{\ }$. By Lemma 5.8.18, 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 9.3.11 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. □

3.3. Exercises.

EXERCISE 9.3.1. 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 9.3.2. 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 9.3.9.)
(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 9.3.3. 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 9.3.4. 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 9.3.5. 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 5.8.20.)
(3) Assume moreover that R is noetherian and $N = \operatorname{Rad}(I)$ is the nil radical of I. Then 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: Proposition 8.1.6.)

4. Graded Rings and Modules

In this section all rings are commutative.

4.1. Graded Rings and Graded Modules. 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 9.4.1) 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 9.4.2), and is called the *exceptional ideal* of R.

EXAMPLE 9.4.1. 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 9.4.3). 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 9.4.2. *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 9.2.1 (3).

(1) implies (2): By Corollary 6.6.13 (1), $R_0 = R/R_+$ is noetherian. By Corollary 6.6.7, 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 $y \in S$. □

4.2. The Grading Associated to a Filtration.

EXAMPLE 9.4.3. 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 9.4.4. 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 9.4.3, 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 9.4.5. 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 9.4.6. 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. 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 9.4.7. 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 9.3.7, 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 9.4.8. *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 6.6.13, R/I is noetherian. By Corollary 6.6.7, I is finitely generated. Therefore $\operatorname{gr}_I(R)$ is a finitely generated R/I-algebra and by Proposition 9.4.2, $\operatorname{gr}_I(R)$ is noetherian.

(2): Since M is a finitely generated R-module and R is noetherian, Corollary 6.6.12 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. □

4.3. The Artin-Rees Theorem.

LEMMA 9.4.9. *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 9.4.10. 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 9.4.2. Let M be an R module and $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$ an I-filtration of M (Definition 9.4.5). 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 9.4.11. *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 $y = r_1x_1 + \cdots + r_mx_m$. 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 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 9.4.12. *(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 6.6.7, I is finitely generated. But S is generated as an R-algebra by I, so Proposition 9.4.2 implies S is noetherian. By Corollary 6.6.12, each M_n is finitely generated as an R-module. By Lemma 9.4.11, $T = \bigoplus_{n\geq 0} M_n$ 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 6.6.12, U is finitely generated over S. We are done by Lemma 9.4.11.

Part (2) follows from Part (1) because the filtration $\{I^n M\}_{n\geq 0}$ is a stable filtration of M. □

COROLLARY 9.4.13. *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 9.4.12, $\{(I^n M) \cap N_{n\geq 0}\}$ is a stable I-filtration of N. The rest comes from Lemma 9.4.9. □

COROLLARY 9.4.14. *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 $\{I^nB\}_{n\geq 0}$. Give C the filtration $\{\beta(I^nB)\}_{n\geq 0}$, which is the same as the I-adic filtration on C, by Exercise 9.3.1. Give A the filtration $\{\alpha^{-1}(I^nB)\}_{n\geq 0}$. By Corollary 9.3.9, 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 9.4.13, $A^* = \hat{A}$, so we are done. □

4.4. 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 9.4.15. *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 3.1.24, 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 9.4.14, the bottom row is exact. By Exercise 9.3.2, $\hat{R} \otimes_R F \cong \hat{F}$, so β is an isomorphism. It follows from Theorem 5.7.2 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 5.7.2 that γ is an isomorphism.

(3): Follows from (2) and Corollary 6.6.12. □

COROLLARY 9.4.16. *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 9.4.15, 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 9.4.15, 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 9.3.10 and Part (2). The second statement follows from Proposition 9.3.11.

(4): By Corollary 9.3.10, 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). □

COROLLARY 9.4.17. *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 9.3.12. □

COROLLARY 9.4.18. *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 9.4.14, the sequence of completions $0 \to \hat{A} \to \hat{B}$ is exact. By Proposition 9.4.15, the sequence $0 \to \hat{R}\otimes_R A \to \hat{R}\otimes_R B$ is exact. It follows from Proposition 6.8.3 that $\hat{R}$ is flat as an R-module. □

4.5. The Krull Intersection Theorem.

THEOREM 9.4.19. *(Krull Intersection Theorem) Let A be a commutative noetherian ring, I an ideal in A, and M a finitely generated A-module. If $N = \bigcap_{n\geq 0} I^n M$, then $IN = N$.*

PROOF. By Theorem 9.4.12, there exists 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. □

COROLLARY 9.4.20. *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 9.4.19, if $N = \bigcap_{n\geq 0} I^n M$, then $IN = N$. By Nakayama's Lemma, Theorem 7.1.3, $N = 0$.

(2): Follows from (1) with $M = R$.

(3): By Theorem 9.4.19, if $N = \bigcap_{n\geq 0} I^n$, then $IN = N$. By Nakayama's Lemma, Lemma 5.3.1, $I + \operatorname{annih}_R(N) = R$. Since $I \neq R$ and $N \subseteq R$ and R is a domain we conclude that $\operatorname{annih}_R(N) = R$. That is, $N = 0$. □

THEOREM 9.4.21. *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.*

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 $n \geq 1$ (Proposition 2.1.22). Then $I^n + \mathfrak{m} = R$ for all $n \geq 1$. By Lemma 9.3.2, $\mathfrak{m}$ is not closed.

(2) implies (3): By Corollary 9.4.18, $\hat{R}$ is flat. Let $\mathfrak{m}$ be a maximal ideal in R. By Exercise 9.3.4, $\hat{\mathfrak{m}} = \varprojlim \mathfrak{m}/I^i$ is a maximal ideal in $\hat{R}$. Since $\mathfrak{m}\hat{R} \subseteq \hat{\mathfrak{m}}$, it follows from Lemma 6.5.1 (4) that $\hat{R}$ is a faithfully flat R-algebra.

(3) implies (2): Let $\mathfrak{m}$ be a maximal ideal of R. By Lemma 6.5.5, there is a maximal ideal M in $\hat{R}$ such that $M \cap R = \mathfrak{m}$. By Corollary 9.4.16 (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 9.4.20.

(4) implies (5): Apply Lemma 9.3.2.

(5) implies (1): Is trivial. □

If R and I satisfy any of the equivalent conditions in Theorem 9.4.21, then we say R, I is a *Zariski pair*.

4.6. Exercises.

EXERCISE 9.4.1. 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 9.4.2. 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 9.4.3. 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.

EXERCISE 9.4.4. Let R be a commutative ring and $S = R[x_1,\dots,x_m]$ the polynomial ring over R in m variables $x_1,\dots,x_m$. 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 9.4.5. Let k be a field and $A = k[x_1,\dots,x_m]$ the polynomial ring in m variables over k. As in Exercise 9.4.4, $A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$ 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 3.1.4).

EXERCISE 9.4.6. 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 $\operatorname{gr}_J(R)$ 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 9.3.7. 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 9.4.7. 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 9.4.8. 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 9.4.9. 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 $R[[x_1,\dots,x_n]]/(x_1 - a_1,\dots,x_n - a_n)$.

4.7. 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 9.3.2, a morphism from $\{A_n\}$ to $\{B_n\}$ is an R-module homomorphism $\alpha : A \to B$ such that for each $n \geq 0$, $\alpha(A_n) \subseteq B_n$. For each $n \geq 0$ 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 9.3.7, α induces a homomorphism on the completions, $\alpha^* : A^* \to B^*$. The maps $\{\gamma_n\}_{n\geq 0}$ define a graded homomorphism

$$\operatorname{gr}(\alpha) : \operatorname{gr}(A) \to \operatorname{gr}(B)$$

of graded R-modules. (Here the grading of R is trivial. Every element is homogeneous of degree zero.)

LEMMA 9.4.22. *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* $\operatorname{gr}(\alpha) : \operatorname{gr}(A) \to \operatorname{gr}(B)$ *the graded homomorphism of graded R-modules. Then*

(1) if $\operatorname{gr}(\alpha)$ *is one-to-one, then α^* is one-to-one, and*
(2) if $\operatorname{gr}(\alpha)$ *is onto, then α^* is onto.*

PROOF. The Snake Lemma (Theorem 5.7.2) 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 $n \geq 0$. Since $\beta_0 = 0$, an inductive argument shows that $\ker \beta_n = 0$ for all $n \geq 0$. By Proposition 9.3.8, the homomorphism on the inverse limits is one-to-one.

(2): Assume $\operatorname{coker} \gamma_n = 0$ for all $n \geq 0$. It is immediate that $\theta_{n+1} : \ker \beta_{n+1} \to \ker \beta_n$ is onto for all $n \geq 0$. Since $\beta_0 = 0$, an inductive argument shows that $\operatorname{coker} \beta_n = 0$ for all $n \geq 0$. Applying Proposition 5.8.19 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 9.4.23. 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 9.4.24. 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 9.4.23 are isomorphic as graded $\operatorname{gr}_J(R)$-modules.

PROPOSITION 9.4.25. *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 9.4.22, 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 6.6.6 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. □

COROLLARY 9.4.26. *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 9.4.16 and Proposition 9.4.8, 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 9.4.25, every ideal of $\hat{R}$ is finitely generated and by Corollary 6.6.7, $\hat{R}$ is noetherian.

(2): By The Hilbert Basis Theorem (Theorem 9.2.1) $A = R[x_1, \dots, x_m]$ is noetherian. By Exercise 9.4.7, S is the completion of A for the I-adic topology, where $I = Ax_1 + \cdots + Ax_m$. □

COROLLARY 9.4.27. *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 9.4.25, M is generated by $\{x_1, \dots, x_m\}$. □

COROLLARY 9.4.28. *Let R, I be a Zariski pair (Theorem 9.4.21). 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 9.4.26, $\hat{R}$ is noetherian. By Corollary 9.4.13 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 9.3.10 there exist elements b_i in R such that $b_i - \beta_i \in \hat{I}^{n_0}$ for each i. Set $a = \sum_i a_i b_i$. 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 9.4.16, $\hat{I} \subseteq \mathrm{J}(\hat{R})$. By Nakayama's Lemma (Corollary 5.3.5), $\alpha\hat{R} = a\hat{R}$. Using Lemma 6.5.4, we get $\mathfrak{a} = \mathfrak{a}\hat{R} \cap R = \alpha\hat{R} \cap R = a\hat{R} \cap R = aR$. □

4.8. Exercises.

EXERCISE 9.4.10. 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 9.4.11. 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 9.4.12. In Exercise 9.4.11, show that the graded $\mathrm{gr}_I(R)$-module associated to the twisted filtration $\{R(-\ell)_n\}_{n\geq 0}$ is the twisted module $\mathrm{gr}_I(R)(-\ell)$. In other words, show that the graded $\mathrm{gr}_I(R)$-modules $\mathrm{gr}\,(R(-\ell))$ and $\mathrm{gr}_I(R)(-\ell)$ are isomorphic.

EXERCISE 9.4.13. 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.

5. Going Up and Going Down Theorems

In this section we prove the Going Up and Going Down Theorems, which are also known as the Cohen-Seidenberg Theorems.

PROPOSITION 9.5.1. *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 6.3.8, 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 $q_1 \cap A = p_1$. □

DEFINITION 9.5.2. If $\phi : A \to B$ is a homomorphism of commutative rings which satisfies one of the equivalent properties of Proposition 9.5.1, then we say *going down holds* for ϕ.

THEOREM 9.5.3. *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 6.8.2, B_{q_2} is a flat A_{p_2}-algebra. By Exercise 6.5.12, B_{q_2} is a faithfully flat A_{p_2}-algebra. By Lemma 6.5.5, $\phi_2^\sharp : \operatorname{Spec} B_{q_2} \to \operatorname{Spec} A_{p_2}$ 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. □

THEOREM 9.5.4. *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 A is a local ring with maximal ideal p, then the prime ideals of B lying over p are precisely the maximal ideals of B.*

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): Let M be a maximal ideal of B and set $\mathfrak{m} = M \cap A$. Then $A/\mathfrak{m} \to B/M$ is one-to-one, B/M is a field and B/M is integral over $A/\mathfrak{m}$ (Exercise 9.1.2). If follows from Lemma 9.1.4 that $A/\mathfrak{m}$ is a field, or in other words, $\mathfrak{m}$ is equal to the maximal ideal p of A. Conversely, let $q \in \operatorname{Spec} B$ be a prime of B lying over p. Then A/p is a field, $A/p \to B/q$ is one-to-one, B/q is an integral domain, and B/q is integral over A/p. It follows from Lemma 9.1.4 that B/q is a field and q is maximal.

(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. Because $A_p \neq 0$, the ring B_p contains at least one maximal ideal, which 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 8.1.2, 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 $\nu \ge 0$. 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 9.5.5. *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 9.5.4 (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 6.6.12). By Proposition 7.4.3, $S/\mathfrak{m}S$ is semilocal. □

5.1. Lifting of Idempotents. If R is a ring, the set of idempotents of R will be 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 $A \to B$, there is a function $\operatorname{idemp}(A) \to \operatorname{idemp}(B)$.

COROLLARY 9.5.6. *Let R be a ring and I a two-sided ideal of R such that $I \subseteq \mathrm{J}(R)$.*

(1) If R is commutative, then the natural map $\operatorname{idemp}(R) \to \operatorname{idemp}(R/I)$ *is one-to-one.*
(2) If I consists of nilpotent elements, then $\operatorname{idemp}(R) \to \operatorname{idemp}(R/I)$ *is onto.*
(3) 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 $\operatorname{idemp}(R) \to \operatorname{idemp}(R/I)$ *is onto.*

PROOF. (1): Let $e_0, e_1 \in \operatorname{idemp}(R)$ and assume $x = e_0 - e_1 \in I$. We show that $x = 0$. Look at

$$\begin{aligned} x^3 &= e_0^3 - 3e_0^2e_1 + 3e_0e_1^2 - e_1^3 \\ &= e_0 - 3e_0e_1 + 3e_0e_1 - e_1 \\ &= e_0 - e_1 \\ &= x. \end{aligned}$$

Then $x(x^2 - 1) = 0$. By Theorem 7.1.3, $x^2 - 1$ is a unit, which implies that $x = 0$.

(2): Assume I consists of nilpotent elements. By Corollary 7.1.5, $I \subseteq \mathrm{J}(R)$. 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 $e_0e_1 = e_1e_0 = 0$, $\bar{e}_0 = \bar{x}^n = \bar{x}$, and $\bar{e}_1 = (1-\bar{x})^n = 1-\bar{x}$. This says that $e_0+e_1-1 \in I$, so by Theorem 7.1.3, $u = e_0+e_1$ is a unit in R. We have $1 = e_0u^{-1}+e_1u^{-1} = u^{-1}e_0 + u^{-1}e_1$, hence $e_0 = e_0^2u^{-1} = u^{-1}e_0^2$, and $e_0u = e_0^2 = ue_0$. We have shown that e_0 commutes with u. From this it follows that e_0u^{-1} is an idempotent of R. Since $\bar{u} = 1$, $\bar{e}_0\bar{u}^{-1} = \bar{x}$.

(3): Let $\bar{x} \in R/I$ be an idempotent. For $n \geq 1$, I/I^n is nilpotent. By (2), $\operatorname{idemp}(R/I^n) \to \operatorname{idemp}(R/I)$ 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 9.5.7. *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 $\operatorname{idemp}(A) \to \operatorname{idemp}(A \otimes_R (R/I))$ *is onto. That is, an idempotent $\bar{e}$ in A/IA lifts to an idempotent e in A.*

(2) If A is commutative, then $\operatorname{idemp}(A) \to \operatorname{idemp}(A \otimes_R (R/I))$ *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 9.4.15, $A \to \varprojlim A/(I^nA)$ is an isomorphism, so A is separated and complete in the IA-adic topology. By Proposition 9.3.11, IA is contained in the Jacobson radical of A. By Corollary 9.5.6 (3), there is an idempotent e in A which maps onto $\bar{e}$.

(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 9.5.4, $\operatorname{Spec} A \to \operatorname{Spec} C$ 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 6.3.14 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 5.8.19, 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. □

Using Corollary 9.5.6, we give sufficient conditions for lifting a finitely generated projective module.

PROPOSITION 9.5.8. *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 9.5.6, 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

$$\begin{tikzcd}
P_1 \arrow[r] \arrow[d, dotted, "\exists f"'] & Q_1 \arrow[r] \arrow[d, "g"] & 0 \\
P_2 \arrow[r] & Q_2 \arrow[r] & 0
\end{tikzcd}$$

where the rows are exact. Since P_1 is a projective R-module, there exists a map f which makes the diagram commutative (Proposition 5.2.3).

(3): Is left to the reader. □

CHAPTER 10

Homological Algebra

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 10.1.2 for the definition of additive functor.)

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 $n_0 \leq i \leq n_1$, 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

$$\mathrm{B}_n(A_\bullet) = \operatorname{im} d_{n+1}, \quad \text{and}$$
$$\mathrm{Z}_n(A_\bullet) = \ker d_n.$$

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 10.1.1. (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 5.3.5). 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 10.1.2. 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 $\mathfrak{F}(\cdot) : \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_\mathbb{Z}(\mathfrak{F}(A), \mathfrak{F}(B))$ 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 $\mathfrak{F}(\cdot) : \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_\mathbb{Z}(\mathfrak{F}(B), \mathfrak{F}(A))$ is a $\mathbb{Z}$-module homomorphism.

LEMMA 10.1.3. *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. □

1.2. Exercises.

EXERCISE 10.1.1. 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 10.1.2. 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 10.1.3. 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 10.1.4. 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 10.1.5. 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 10.1.6. 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 10.1.4. *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 5.7.2).

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 10.1.3 says that the kernel of d_n is $\mathrm{H}_n(\,)$ and the cokernel is $\mathrm{H}_{n-1}(\,)$. Apply the Snake Lemma. □

THEOREM 10.1.5. *In the context of Theorem 10.1.4, the connecting homomorphism* $\partial : \mathrm{H}_n(C_\bullet) \to \mathrm{H}_{n-1}(A_\bullet)$ *is natural. More specifically, if*

$$\begin{tikzcd}
0 \arrow[r] & A_\bullet \arrow[r, "f"] \arrow[d, "\chi"] & B_\bullet \arrow[r, "g"] \arrow[d, "\rho"] & C_\bullet \arrow[r] \arrow[d, "\sigma"] & 0 \\
0 \arrow[r] & A'_\bullet \arrow[r, "f'"] & B'_\bullet \arrow[r, "g'"] & C'_\bullet \arrow[r] & 0
\end{tikzcd}$$

is a commutative diagram of chain complexes with exact rows, then there is a commutative diagram

$$\begin{tikzcd}
\mathrm{H}_n(A_\bullet) \arrow[r, "\mathrm{H}(f)"] \arrow[d, "\mathrm{H}(\chi)"] & \mathrm{H}_n(B_\bullet) \arrow[r, "\mathrm{H}(g)"] \arrow[d, "\mathrm{H}(\rho)"] & \mathrm{H}_n(C_\bullet) \arrow[r, "\partial"] \arrow[d, "\mathrm{H}(\sigma)"] & \mathrm{H}_{n-1}(A_\bullet) \arrow[d, "\mathrm{H}(\chi)"] \\
\mathrm{H}_n(A'_\bullet) \arrow[r, "\mathrm{H}(f')"] & \mathrm{H}_n(B'_\bullet) \arrow[r, "\mathrm{H}(g')"] & \mathrm{H}_n(C'_\bullet) \arrow[r, "\partial'"] & \mathrm{H}_{n-1}(A'_\bullet)
\end{tikzcd}$$

with exact rows for each $n \in \mathbb{Z}$.

PROOF. Most of this follows straight from Lemma 10.1.3 and Theorem 10.1.4. It is only necessary to check that the third square is commutative. For this, use the definition of ∂ given in the proof of Theorem 5.7.2. 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. As in Example 3.3.1, 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 10.1.6. *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 10.1.7. *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

$$\begin{tikzcd}
X_0 \arrow[d, dotted, "\exists f_0"'] \arrow[dr, "f\varepsilon"] & & \\
Y_0 \arrow[r, "\pi"] & N \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{tikzcd}
X_1 \arrow[r, "d_1"] \arrow[d, dotted, "\exists f_1"'] & X_0 \arrow[r, "\varepsilon"] \arrow[d, "f_0"] & M \arrow[d, "f"] \\
Y_1 \arrow[r, "d_1"] & Y_0 \arrow[r, "\pi"] & N
\end{tikzcd}$$

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

$$\begin{tikzcd}
X_1 \arrow[d, dotted, "\exists f_1"'] \arrow[dr, "f_0 d_1"] & & \\
Y_1 \arrow[r, "d_1"] & \operatorname{im} d_1 \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{tikzcd}
X_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, dotted, "\exists f_{n+1}"'] & X_n \arrow[r, "d_n"] \arrow[d, "f_n"] & X_{n-1} \arrow[d, "f_{n-1}"] \\
Y_{n+1} \arrow[r, "d_{n+1}"] & Y_n \arrow[r, "d_n"] & Y_{n-1}
\end{tikzcd}$$

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

$$\begin{tikzcd}
X_{n+1} \arrow[d, dotted, "\exists f_{n+1}"'] \arrow[dr, "f_n d_{n+1}"] & & \\
Y_{n+1} \arrow[r, "d_{n+1}"] & \operatorname{im} d_{n+1} \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & X_0 \arrow[dl, dotted, "\exists k_0"'] \arrow[d, "f_0 - g_0"] & \\
Y_1 \arrow[r, "d_1"] & \operatorname{im} d_1 \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & X_n \arrow[r, "d_n"] \arrow[d, "f_n - g_n"'] & X_{n-1} \arrow[r, "d_{n-1}"] \arrow[d, "f_{n-1}-g_{n-1}"] \arrow[dl, "k_{n-1}"'] & X_{n-2} \arrow[dl, "k_{n-2}"'] \\
Y_{n+1} \arrow[r, "d_{n+1}"'] & Y_n \arrow[r, "d_n"'] & Y_{n-1} &
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & X_n \arrow[dl, dotted, "\exists k_n"'] \arrow[d, "f_n - g_n - k_{n-1}d_n"] & \\
Y_{n+1} \arrow[r, "d_{n+1}"] & \operatorname{im} d_{n+1} \arrow[r] & 0
\end{tikzcd}$$

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). □

1.5. Exercises.

EXERCISE 10.1.7. 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 10.1.8. 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 10.1.9. (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 10.1.10. (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 10.1.11. Assume we are given a commutative diagram

$$\begin{tikzcd}
{} \arrow[r] & A_n \arrow[r, "f_n"] \arrow[d, "\alpha_n"] & B_n \arrow[r, "g_n"] \arrow[d, "\beta_n"] & C_n \arrow[r, "h_n"] \arrow[d, "\gamma_n", "\cong"'] & A_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\alpha_{n-1}"] & B_{n-1} \arrow[r, "g_{n-1}"] \arrow[d, "\beta_{n-1}"] & C_{n-1} \arrow[r] \arrow[d, "\gamma_{n-1}", "\cong"'] & {} \\
{} \arrow[r] & X_n \arrow[r, "r_n"] & Y_n \arrow[r, "s_n"] & Z_n \arrow[r, "t_n"] & X_{n-1} \arrow[r, "r_{n-1}"] & Y_{n-1} \arrow[r, "s_{n-1}"] & Z_{n-1} \arrow[r] & {}
\end{tikzcd}$$

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 10.1.8, 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 10.1.7 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 10.1.7, 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 10.1.8, we show that this definition does not depend on the choice of $P_\bullet$ and $Q_\bullet$.

THEOREM 10.1.8. *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 10.1.7 (1) from both directions to get morphisms $f : P_\bullet \to Q_\bullet$ and $g : Q_\bullet \to P_\bullet$. Theorem 10.1.7 (2) (from both directions) says $fg \sim 1$ and $gf \sim 1$. By Exercise 10.1.7, $\mathfrak{F}(fg) \sim 1$ 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 10.1.7, $\delta\alpha \sim \beta\gamma$.

The rest of the details are left to the reader. □

THEOREM 10.1.9. *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 $\ell \geq 1$

$$\cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \to \cdots \xrightarrow{d_{\ell+1}} P_\ell \xrightarrow{d_\ell} K_{\ell-1} \to 0 \tag{10.1}$$

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, (10.1) becomes

$$\cdots \to P(-\ell)_{n-\ell+1} \xrightarrow{d(-\ell)_{n-\ell+1}} P(-\ell)_{n-\ell} \to \cdots \xrightarrow{d(-\ell)_1} P(-\ell)_0 \xrightarrow{d(-\ell)_0} K_{\ell-1} \to 0 \tag{10.2}$$

By Theorem 10.1.8 we may compute the $(n-\ell+1)$th left derived of $K_{\ell-1}$ using the projective resolution (10.2). For $\ell \geq 1$ the sequences (10.1) and (10.2) 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. □

1.7. The Long Exact Sequence.

LEMMA 10.1.10. *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

$$\begin{tikzcd}
 & P_0 \arrow[d, "\alpha"] & & R_0 \arrow[d, "\gamma"] & \\
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d] & B \arrow[r, "\tau"] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & & 0 &
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & P_0 \arrow[r, "\sigma_0"] \arrow[d, "\alpha"] & Q_0 \arrow[r, "\tau_0"] \arrow[d, "\beta"] & R_0 \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d] & B \arrow[r, "\tau"] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

commutes and the rows and columns are exact. The Snake Lemma (Theorem 5.7.2) 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. □

THEOREM 10.1.11. *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 10.1.10 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,

$$0 \to \mathfrak{F}(P_\bullet) \xrightarrow{\sigma} \mathfrak{F}(Q_\bullet) \xrightarrow{\tau} \mathfrak{F}(R_\bullet) \to 0 \tag{10.3}$$

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 10.1.4 applied to (10.3).

(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 10.1.12. *(The Cube Lemma) Let*

$$\begin{tikzcd}
K \arrow[rrrrr, dotted, "a"] \arrow[ddddd, dotted, "b"'] \arrow[dr] & & & & & L \arrow[dl] \arrow[ddddd, dotted, "d"] \\
& A \arrow[rrr] \arrow[dr, "\alpha"] \arrow[ddd] & & & B \arrow[dl, "\beta"'] \arrow[ddd] & \\
& & E \arrow[r] \arrow[d] & F \arrow[d] & & \\
& & G \arrow[r] & H & & \\
& C \arrow[ur, "\gamma"] \arrow[rrr] & & & D \arrow[ul, "\delta"'] & \\
M \arrow[ur] \arrow[rrrrr, dotted, "c"] & & & & & N \arrow[ul]
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, dotted, "a"'] & A \arrow[r, "\alpha"] \arrow[d] & E \arrow[d] \\
0 \arrow[r] & L \arrow[r] & B \arrow[r, "\beta"] & F
\end{tikzcd}$$

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 10.1.13. *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 10.1.7. 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

$$\begin{tikzcd}
 & & & R_0 \arrow[lld, "e_2"'] \arrow[ld, "f"] \arrow[ddd, "c_0"] \\
 & B \arrow[r, "\tau"'] \arrow[d, "b"] & C \arrow[d, "c"] & \\
P'_0 \arrow[r, "\sigma' d'"] & B' \arrow[r, "\tau'"] & C' & \\
 & & & R'_0 \arrow[llu, "e'_2"] \arrow[lu, "f'"']
\end{tikzcd}$$

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 10.1.12 there are unique homomorphisms connecting the kernels to the rest of the diagram. The overall diagram

$$\begin{tikzcd}
& K \arrow[rr] \arrow[dl] \arrow[dd] & & L \arrow[rr] \arrow[dl] \arrow[dd] & & M \arrow[dl] \arrow[dd] \\
K' \arrow[rr, crossing over] \arrow[dd] & & L' \arrow[rr, crossing over] \arrow[dd] & & M' \arrow[dd] & \\
& P_0 \arrow[rr] \arrow[dl] \arrow[dd] & & Q_0 \arrow[rr] \arrow[dl] \arrow[dd] & & R_0 \arrow[dl] \arrow[dd] \\
P_0' \arrow[rr, crossing over] \arrow[dd] & & Q_0' \arrow[rr, crossing over] \arrow[dd] & & R_0' \arrow[dd] & \\
& A \arrow[rr] \arrow[dl] & & B \arrow[rr] \arrow[dl] & & C \arrow[dl] \\
A' \arrow[rr] & & B' \arrow[rr] & & C' &
\end{tikzcd}$$

commutes, which completes the basis step. The reader should verify the inductive step and complete the proof. □

THEOREM 10.1.14. *In the long exact sequence of Theorem 10.1.11, 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 10.1.13 to get the two short exact sequences of projective resolutions. The split exact rows remain exact after applying $\mathfrak{F}$. Use Theorem 10.1.5. □

1.8. Exercises.

EXERCISE 10.1.12. 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 10.1.13. 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 10.1.14. 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 10.1.15. *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

$$0 \to K_j \to C_j \to K_{j-1} \to 0 \tag{10.4}$$

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, (10.4) gives rise to the exact sequence

$$0 \to X_j \to \mathfrak{F}K_j \to \mathfrak{F}C_j \to \mathfrak{F}K_{j-1} \to 0 \tag{10.5}$$

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 (10.5) 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 10.1.2 there is an exact sequence

$$0 \to \mathrm{Z}_j(\mathfrak{F}C_\bullet) \to \mathfrak{F}C_j \to \mathrm{B}_{j-1}(\mathfrak{F}C_\bullet) \to 0. \tag{10.6}$$

Combine (10.5) and (10.6) 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 10.1.11, the short exact sequence (10.4) gives rise to the long exact sequence

$$\cdots \to \mathrm{L}_{n+1}\mathfrak{F}(C_j) \to \mathrm{L}_{n+1}\mathfrak{F}(K_{j-1}) \xrightarrow{\partial} \mathrm{L}_n\mathfrak{F}(K_j) \to \mathrm{L}_n\mathfrak{F}(C_j) \to \cdots. \tag{10.7}$$

Because the modules C_j are acyclic, the boundary maps in (10.7) are isomorphisms

$$\mathrm{L}_{n+1}\mathfrak{F}(K_{j-1}) \cong \mathrm{L}_n\mathfrak{F}(K_j) \tag{10.8}$$

for all $n \geq 1$ and $j \geq 0$. Iterate (10.8) to get

$$\mathrm{L}_{n+1}\mathfrak{F}(M) = \mathrm{L}_{n+1}\mathfrak{F}(K_{-1}) \cong \mathrm{L}_n\mathfrak{F}(K_0) \cong \mathrm{L}_{n-1}\mathfrak{F}(K_1) \cong \cdots \cong \mathrm{L}_1\mathfrak{F}(K_{n-1}). \tag{10.9}$$

When $n = 0$, (10.7) looks like

$$0 \to \mathrm{L}_1\mathfrak{F}(K_{j-1}) \to \mathfrak{F}K_j \to \mathfrak{F}C_j \to \mathfrak{F}K_{j-1} \to 0. \tag{10.10}$$

Comparing (10.10) and (10.9) 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 10.1.16. 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 10.1.17. 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 5.4.18).

EXAMPLE 10.1.18. 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 5.5.5). If the first variable is fixed, the functor is left exact covariant in the second variable (Proposition 5.5.5).

LEMMA 10.1.19. *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 10.1.13. □

THEOREM 10.1.20. *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 10.1.13 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

$$0 \to K_i \to P_i \to K_{i-1} \to 0 \tag{10.11}$$

$$0 \to L_j \to Q_j \to L_{j-1} \to 0 \tag{10.12}$$

To sequence (10.11) apply Lemma 10.1.19 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 10.1.14, $\mathrm{L}_1\mathfrak{F}_1(P_i,L_j) = 0$ and $\mathrm{L}_1\mathfrak{F}_1(P_i,L_{j-1}) = 0$ because P_i is projective.

To sequence (10.12) apply Lemma 10.1.19 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 10.1.14, $\mathrm{L}_1\,\mathfrak{F}_2(K_i,Q_j) = 0$ and $\mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},Q_j) = 0$ because Q_j is projective. The diagram

$$\begin{tikzcd}
 & \mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_j) \arrow[d] & 0 \arrow[d] & \mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_{j-1}) \arrow[d] \\
\mathrm{L}_1\,\mathfrak{F}_2(K_i,L_{j-1}) \arrow[r] & \mathfrak{F}(K_i,L_j) \arrow[r, "\sigma"] \arrow[d, "\alpha"] & \mathfrak{F}(K_i,Q_j) \arrow[r] \arrow[d, "\beta"] & \mathfrak{F}(K_i,L_{j-1}) \arrow[d, "\gamma"] \\
0 \arrow[r] & \mathfrak{F}(P_i,L_j) \arrow[r, "\tau"] \arrow[d] & \mathfrak{F}(P_i,Q_j) \arrow[r] \arrow[d] & \mathfrak{F}(P_i,L_{j-1}) \arrow[d] \\
\mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},L_{j-1}) \arrow[r] & \mathfrak{F}(K_{i-1},L_j) \arrow[r] & \mathfrak{F}(K_{i-1},Q_j) \arrow[r] & \mathfrak{F}(K_{i-1},L_{j-1})
\end{tikzcd}$$

commutes, where the three rows and three columns are the exact sequences from above. Apply the Snake Lemma (Theorem 5.7.2) to see that

$$\mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_{j-1}) \cong \mathrm{L}_1\,\mathfrak{F}_2(K_{i-1},L_{j-1}) \tag{10.13}$$

Since β and τ are one-to-one it follows that

$$\mathrm{L}_1\,\mathfrak{F}_1(K_{i-1},L_j) = \mathrm{L}_1\,\mathfrak{F}_2(K_i,L_{j-1}) \tag{10.14}$$

Combine (10.14) and (10.13) 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

$$\mathrm{L}_1\,\mathfrak{F}_1(A,L_{n-1}) \cong \mathrm{L}_1\,\mathfrak{F}_1(K_{-1},L_{n-1}) \cong \mathrm{L}_1\,\mathfrak{F}_1(K_{n-1},L_{-1}) \cong \mathrm{L}_1\,\mathfrak{F}_1(K_{n-1},B) \tag{10.15}$$

Combine (10.15) with (10.13) and Theorem 10.1.9 to get

$$\begin{aligned}
\mathrm{L}_{n+1}\,\mathfrak{F}_1(A,B) &\cong \mathrm{L}_1\,\mathfrak{F}_1(K_{n-1},B) \quad \text{(by Theorem 10.1.9)} \\
&\cong \mathrm{L}_1\,\mathfrak{F}_1(A,L_{n-1}) \quad (10.15) \\
&\cong \mathrm{L}_1\,\mathfrak{F}_2(A,L_{n-1}) \quad (10.13) \\
&\cong \mathrm{L}_{n+1}\,\mathfrak{F}_2(A,B) \quad \text{(by Theorem 10.1.9)}
\end{aligned}$$

□

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

$$\mathrm{B}^n(A^\bullet) = \operatorname{im} d^{n-1}, \quad \text{and}$$
$$\mathrm{Z}^n(A^\bullet) = \ker d^n.$$

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 10.2.1. (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 5.6.4). 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 10.2.2. As in Example 10.1.2, 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 10.2.3. *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 10.1.3. The details are left to the reader. □

2.2. Exercises.

EXERCISE 10.2.1. 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 10.2.2. 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 10.2.3. 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 10.2.4. 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 10.2.5. 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

$$\mathrm{H}^n\left(\bigoplus_{j\in J}(A_j)^\bullet\right) \cong \bigoplus_{j\in J}\mathrm{H}^n\big((A_j)^\bullet\big).$$

EXERCISE 10.2.6. 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 10.2.4. *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 10.1.4. The details are left to the reader. □

THEOREM 10.2.5. *In the context of Theorem 10.2.4, 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 10.1.5. 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 10.2.6. *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 10.1.6. The details are left to the reader. □

THEOREM 10.2.7. *Consider the diagram of R-modules*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varepsilon"] \arrow[d, "f"] & X^0 \arrow[r, "d^0"] \arrow[d, dotted, "\exists f^0"] & X^1 \arrow[r, "d^1"] \arrow[d, dotted, "\exists f^1"] & X^2 \arrow[r, "d^2"] \arrow[d, dotted, "\exists f^2"] & \cdots \\
0 \arrow[r] & N \arrow[r, "\varphi"] & Y^0 \arrow[r, "d^0"] & Y^1 \arrow[r, "d^1"] & Y^2 \arrow[r, "d^2"] & \cdots
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varepsilon"] \arrow[dr, "\varphi f"'] & X^0 \arrow[d, dotted, "\exists f^0"] \\
 & & Y^0
\end{tikzcd}$$

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

$$\begin{tikzcd}
M \arrow[r, "\varepsilon"] \arrow[d, "f"] & X^0 \arrow[r, "d^0"] \arrow[d, "f^0"] & X^1 \arrow[d, dotted, "\exists f^1"] \\
N \arrow[r, "\varphi"] & Y^0 \arrow[r, "d^0"] & Y^1
\end{tikzcd}$$

The top row is exact, the bottom row is a cochain complex. Because $d^0f^0\varepsilon = d^0\varphi f = 0$, it follows that $\ker(d^0) = \operatorname{im}(\varepsilon) \subseteq \ker(d^0f^0)$. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & X^0/\operatorname{im}(\varepsilon) \arrow[r, "d^0"] \arrow[dr, "d^0f^0"'] & X^1 \arrow[d, dotted, "\exists f^1"] \\
 & & Y^1
\end{tikzcd}$$

with top row exact. Since Y^1 is injective, there exists $f^1 : X^1 \to Y^1$ such that $d^0f^0 = f^1d^0$.

Recursively construct f^{n+1} using f^n and f^{n-1}. Start with the commutative diagram

$$\begin{tikzcd}
X^{n-1} \arrow[r, "d^{n-1}"] \arrow[d, "f^{n-1}"] & X^n \arrow[r, "d^n"] \arrow[d, "f^n"] & X^{n+1} \arrow[d, dotted, "\exists f^{n+1}"] \\
Y^{n-1} \arrow[r, "d^{n-1}"] & Y^n \arrow[r, "d^n"] & Y^{n+1}
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & X^n/\operatorname{im}(d^{n-1}) \arrow[r, "d^n"] \arrow[dr, "d^{n-1}f^{n-1}"'] & X^{n+1} \arrow[d, dotted, "\exists f^{n+1}"] \\
& & Y^{n+1}
\end{tikzcd}$$

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 $i \le 0$.

To construct k^1, start with the commutative diagram

$$\begin{tikzcd}
M \arrow[r, "\varepsilon"] \arrow[d, "f"'] & X^0 \arrow[r, "d^0"] \arrow[d, "f^0-g^0"'] & X^1 \arrow[dl, dotted, "\exists k^1"] \\
N \arrow[r, "\varphi"] & Y^0 &
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & X^0/\ker(d^0) \arrow[r, "d^0"] \arrow[d, "f^0-g^0"'] & X^1 \arrow[dl, dotted, "\exists k^1"] \\
& Y^0 &
\end{tikzcd}$$

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

$$\begin{tikzcd}
& X^{n-1} \arrow[r, "d^{n-1}"] \arrow[dl, "k^{n-1}"'] \arrow[d, "f^{n-1}-g^{n-1}"] & X^n \arrow[r, "d^n"] \arrow[dl, "k^n"'] \arrow[d, "f^n-g^n"] & X^{n+1} \arrow[dl, dotted, "\exists k^{n+1}"] \\
Y^{n-2} \arrow[r, "d^{n-2}"'] & Y^{n-1} \arrow[r, "d^{n-1}"'] & Y^n &
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & X^n/\ker(d^n) \arrow[r, "d^n"] \arrow[d, "f^n-g^n-d^{n-1}k^n"'] & X^{n+1} \arrow[dl, dotted, "\exists k^{n+1}"] \\
& Y^n &
\end{tikzcd}$$

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). □

2.5. Exercises.

EXERCISE 10.2.7. 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 10.2.8. 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 10.2.8, 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 10.2.7 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 10.2.7, 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 10.2.8, we show that this definition does not depend on the choice of $I^\bullet$ and $J^\bullet$.

THEOREM 10.2.8. *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 10.2.7 (1) from both directions to get morphisms $f : I^\bullet \to J^\bullet$ and $g : J^\bullet \to I^\bullet$. Theorem 10.2.7 (2) (from both directions) says $fg \sim 1$ and $gf \sim 1$. By Exercise 10.2.7, $\mathfrak{F}(fg) \sim 1$ 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 10.2.7, $\delta\alpha \sim \beta\gamma$.

The rest of the details are left to the reader. □

THEOREM 10.2.9. *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

$$0 \to K^\ell \to I^\ell \xrightarrow{d^\ell} I^{\ell+1} \xrightarrow{d^{\ell+1}} \cdots \to I^n \xrightarrow{d^n} I^{n+1} \to \cdots \tag{10.16}$$

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, (10.16) becomes

(10.17)

$$0 \to K^\ell \to I(-\ell)^0 \xrightarrow{d(-\ell)^0} I(-\ell)^1 \xrightarrow{d(-\ell)^1} \cdots \to I(-\ell)^{n-\ell} \xrightarrow{d(-\ell)^{n-\ell}} I(-\ell)^{n-\ell+1} \to \cdots$$

By Theorem 10.2.8 we may compute the $(n-\ell)$th right derived of K^ℓ using the injective resolution (10.17). The sequences (10.16) and (10.17) 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 10.1.8, 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 10.1.7 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 10.2.8, 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 10.1.8, this definition does not depend on the choice of $P_\bullet$ and $Q_\bullet$.

THEOREM 10.2.10. *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 10.1.8. The details are left to the reader. □

THEOREM 10.2.11. *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

$$\cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \to \cdots \xrightarrow{d_{\ell+1}} P_\ell \xrightarrow{d_\ell} K_{\ell-1} \to 0 \tag{10.18}$$

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, (10.18) becomes

$$\cdots \to P(-\ell)_{n-\ell+1} \xrightarrow{d(-\ell)_{n-\ell+1}} P(-\ell)_{n-\ell} \to \cdots \xrightarrow{d(-\ell)_1} P(-\ell)_0 \xrightarrow{d(-\ell)_0} K_{\ell-1} \to 0 \tag{10.19}$$

By Theorem 10.2.10, we may compute the $(n-\ell)$th right derived group of $K_{\ell-1}$ using the projective resolution (10.19). The sequences (10.18) and (10.19) 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 10.2.12. *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 5.7.2) 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 10.2.13. *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*

$$0 \to \mathrm{R}^0\mathfrak{F}(C) \xrightarrow{\tau} \mathrm{R}^0\mathfrak{F}(B) \xrightarrow{\sigma} \mathrm{R}^0\mathfrak{F}(A) \xrightarrow{\delta^0} \mathrm{R}^1\mathfrak{F}(C) \xrightarrow{\tau} \mathrm{R}^1\mathfrak{F}(B) \xrightarrow{\sigma} \mathrm{R}^1\mathfrak{F}(A) \xrightarrow{\delta^1} \cdots$$
$$\cdots \xrightarrow{\sigma} \mathrm{R}^{n-1}\mathfrak{F}(A) \xrightarrow{\delta^{n-1}} \mathrm{R}^n\mathfrak{F}(C) \xrightarrow{\tau} \mathrm{R}^n\mathfrak{F}(B) \xrightarrow{\sigma} \mathrm{R}^n\mathfrak{F}(A) \xrightarrow{\delta^n} \mathrm{R}^{n+1}\mathfrak{F}(C) \to \cdots.$$

(3) *The 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 10.2.12 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,

$$0 \to \mathfrak{F}(I^\bullet) \xrightarrow{\sigma} \mathfrak{F}(J^\bullet) \xrightarrow{\tau} \mathfrak{F}(K^\bullet) \to 0 \tag{10.20}$$

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 10.2.4 applied to (10.20).

(2): Start with projective resolutions $P_\bullet \to A$ for A and $R_\bullet \to C$ for C. Use Lemma 10.1.10 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,

$$0 \to \mathfrak{F}(R_\bullet) \xrightarrow{\sigma} \mathfrak{F}(Q_\bullet) \xrightarrow{\tau} \mathfrak{F}(P_\bullet) \to 0 \tag{10.21}$$

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 10.2.4 applied to (10.21).

(3): This follows from Theorem 10.2.4. 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. □

LEMMA 10.2.14. *(The Cube Lemma) Let*

$$\begin{tikzcd}
A \arrow[rrrrrr] \arrow[dr, "\alpha"] \arrow[ddddd] & & & & & & B \arrow[dl, "\beta"'] \arrow[ddddd] \\
& E \arrow[rrrr] \arrow[dr] \arrow[ddd] & & & & F \arrow[dl] \arrow[ddd] & \\
& & K \arrow[rr, dotted, "a"] \arrow[d, dotted, "b"'] & & L \arrow[d, dotted, "d"] & & \\
& & M \arrow[rr, dotted, "c"] & & N & & \\
& G \arrow[rrrr] \arrow[ur] & & & & H \arrow[ul] & \\
C \arrow[rrrrrr] \arrow[ur, "\gamma"] & & & & & & D \arrow[ul, "\delta"']
\end{tikzcd}$$

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

$$\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d] & E \arrow[r] \arrow[d] & K \arrow[r] \arrow[d, dotted, "a"'] & 0 \\
B \arrow[r, "\beta"] & F \arrow[r] & L \arrow[r] & 0
\end{tikzcd}$$

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

$$E \to K \overset{a}{\to} L \overset{d}{\to} N$$

which factors into

$$E \to F \to L \overset{d}{\to} N$$

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 10.2.15. *Suppose*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\sigma"] \arrow[d, "a"] & B \arrow[r, "\tau"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A_{\prime} \arrow[r, "\sigma_{\prime}"] & B_{\prime} \arrow[r, "\tau_{\prime}"] & C_{\prime} \arrow[r] & 0
\end{tikzcd}$$

is a commutative diagram of R-modules, with exact rows. Suppose we are given injective resolutions for the four corners $A \to I^{\bullet}$, $C \to K^{\bullet}$, $A_{\prime} \to I_{\prime}{}^{\bullet}$, and $C_{\prime} \to K_{\prime}{}^{\bullet}$. Then there exist injective resolutions $B \to J^{\bullet}$ and $B' \to J_{\prime}{}^{\bullet}$ and morphisms such that the diagram of cochain complexes

$$\begin{tikzcd}
0 \arrow[r] & I^{\bullet} \arrow[r, "\sigma"] \arrow[d, "a"] & J^{\bullet} \arrow[r, "\tau"] \arrow[d, "b"] & K^{\bullet} \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & I_{\prime}^{\bullet} \arrow[r, "\sigma_{\prime}"] & J_{\prime}^{\bullet} \arrow[r, "\tau_{\prime}"] & K_{\prime}^{\bullet} \arrow[r] & 0
\end{tikzcd}$$

is commutative with exact rows.

PROOF. The morphisms $a : I^{\bullet} \to I_{\prime}^{\bullet}$ and $c : K^{\bullet} \to K_{\prime}^{\bullet}$ exist by Theorem 10.2.7. The injective resolutions $B \to J^{\bullet}$, $B_{\prime} \to J_{\prime}^{\bullet}$ 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

$$\begin{tikzcd}
& A \arrow[rr, "\sigma"] \arrow[dl, "a"'] \arrow[dd, "d"] & & B \arrow[rr, "\tau"] \arrow[dl, "b"'] & & C \arrow[dl, "c"'] \arrow[dd, "f"] \\
A_{\prime} \arrow[rr, "\sigma_{\prime}"] \arrow[ddd, "d_{\prime}"'] & & B_{\prime} \arrow[rr, "\tau_{\prime}"] & & C_{\prime} \arrow[dd, "f_{\prime}"] & \\
& I^0 \arrow[dl, "a^0"'] & & & & K^0 \arrow[dl, "c^0"'] \\
I_{\prime}^0 & & & & K_{\prime}^0 &
\end{tikzcd}$$

The maps $d, d_{\prime}, f, f_{\prime}, \sigma, \sigma_{\prime}$ are one-to-one and $\tau, \tau_{\prime}$ are onto. The R-modules $I^0, K^0, I_{\prime}^0, K_{\prime}^0$ 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 $I_{\prime}^0$ is injective, there exists $e_{\prime}^1 : B_{\prime} \to I_{\prime}^0$ such that $e_{\prime}^1\sigma_{\prime} = d_{\prime}$. Let $e_{\prime}^2 = f_{\prime}\tau_{\prime}$.

The diagram

$$\begin{tikzcd}
I^0 \arrow[ddd, "a^0"'] & & & \\
& A \arrow[ul, "d"'] \arrow[r, "\sigma"] \arrow[d, "a"'] & B \arrow[ull, "e^1"'] \arrow[r, "f\tau"] \arrow[d, "b"] & K^0 \\
& A_\prime \arrow[dl, "d_\prime"'] \arrow[r, "\tau'"] & B_\prime \arrow[dll, "e^1_\prime"] & \\
I^0_\prime & & &
\end{tikzcd}$$

is not necessarily commutative. The row $A \to B \to K^0$ is exact. Notice that

$$\begin{aligned}
(a^0e^1 - e^1_\prime b)\sigma &= a^0 d - e^1_\prime \tau_\prime a \\
&= a^0 d - d_\prime a \\
&= 0
\end{aligned}$$

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 10.2.14 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 10.2.16. *In the long exact sequence of Theorem 10.2.13, 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 10.2.15 to get the two short exact sequences of injective resolutions. The split exact rows remain exact after applying $\mathfrak{F}$. Use Theorem 10.2.5.

(2) Use Lemma 10.1.13 to get the two short exact sequences of projective resolutions. The split exact rows remain exact after applying $\mathfrak{F}$. Use Theorem 10.2.5. □

2.8. Exercises.

EXERCISE 10.2.9. 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 10.2.10. 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 10.2.11. 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 10.2.12. 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 10.2.13. 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 10.2.14. 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 10.2.17 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 10.2.17. *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

$$0 \to K^j \to C^j \to K^{j+1} \to 0 \tag{10.22}$$

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, (10.22) 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 $\mathrm{B}^j(\mathfrak{F}C^\bullet) \subseteq \mathrm{im}\{\mathfrak{F}K^{j+1} \to \mathfrak{F}C^{j+1}\}$. 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 10.2.13, the short exact sequence (10.22) gives rise to the long exact sequence

$$\cdots \to \mathrm{R}^n\mathfrak{F}(C^j) \to \mathrm{R}^n\mathfrak{F}(K^{j+1}) \xrightarrow{\delta^n} \mathrm{R}^{n+1}\mathfrak{F}(K^j) \to \mathrm{R}^{n+1}\mathfrak{F}(C^j) \to \cdots. \tag{10.23}$$

Because the modules C^j are acyclic, the connecting homomorphisms in (10.23) are isomorphisms

$$\mathrm{R}^n\mathfrak{F}(K^{j+1}) \cong \mathrm{R}^{n+1}\mathfrak{F}(K^j) \tag{10.24}$$

for all $n \geq 1$ and $j \geq 0$. Iterate (10.24) to get

$$\mathrm{R}^{n+1}\,\mathfrak{F}(M) = \mathrm{R}^{n+1}\,\mathfrak{F}(K^0) \cong \mathrm{R}^n\,\mathfrak{F}(K^1) \cong \mathrm{R}^{n-1}\,\mathfrak{F}(K^2) \cong \cdots \cong \mathrm{R}^1\,\mathfrak{F}(K^n). \tag{10.25}$$

When $n = 0$, (10.23) looks like

$$0 \to \mathfrak{F}K^j \to \mathfrak{F}C^j \to \mathfrak{F}K^{j+1} \xrightarrow{\delta^0} \mathrm{R}^1\,\mathfrak{F}K^j \to 0. \tag{10.26}$$

Comparing (10.26) and (10.25) 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

$$0 \to K_j \to C_j \to K_{j-1} \to 0, \tag{10.27}$$

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, (10.27) 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 10.2.13, the short exact sequence (10.27) gives rise to the long exact sequence

$$(10.28) \qquad \cdots \to \mathrm{R}^n\,\mathfrak{F}(C_j) \to \mathrm{R}^n\,\mathfrak{F}(K_j) \xrightarrow{\delta^n} \mathrm{R}^{n+1}\,\mathfrak{F}(K_{j-1}) \to \mathrm{R}^{n+1}\,\mathfrak{F}(C_j) \to \cdots.$$

Because the modules C^j are acyclic, the connecting homomorphisms δ^n are isomorphisms

$$(10.29) \qquad \mathrm{R}^n\,\mathfrak{F}(K_j) \cong \mathrm{R}^{n+1}\,\mathfrak{F}(K_{j-1})$$

for all $n \geq 1$ and $j \geq 0$. Iterate (10.29) to get

$$(10.30) \qquad \mathrm{R}^{n+1}\,\mathfrak{F}(M) = \mathrm{R}^{n+1}\,\mathfrak{F}(K_{-1}) \cong \mathrm{R}^n\,\mathfrak{F}(K_0) \cong \mathrm{R}^{n-1}\,\mathfrak{F}(K_1) \cong \cdots \cong \mathrm{R}^1\,\mathfrak{F}(K_{n-1}).$$

When $n = 0$, (10.28) looks like

$$(10.31) \qquad 0 \to \mathfrak{F}K_{j-1} \to \mathfrak{F}C_j \to \mathfrak{F}K_j \xrightarrow{\delta^0} \mathrm{R}^1\,\mathfrak{F}K_{j-1} \to 0.$$

Comparing (10.31) and (10.30) 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 10.1.16 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 10.2.18. *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 10.2.11 and Exercises 10.2.12. □

THEOREM 10.2.19. *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 10.2.11 and Exercises 10.2.12, 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

$$0 \to K_i \to P_i \to K_{i-1} \to 0 \tag{10.32}$$
$$0 \to L^j \to Q^j \to L^{j+1} \to 0 \tag{10.33}$$

To sequence (10.32) apply Lemma 10.2.18 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 10.2.14, $\mathrm{R}^1\mathfrak{F}_1(P_i,L^j) = \mathrm{R}^1\mathfrak{F}_1(P_i,L^{j+1}) = 0$ because P_i is projective. To sequence (10.33) apply Lemma 10.2.18 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 10.2.13, $\mathrm{R}^1\mathfrak{F}_2(K_i,Q^j) = \mathrm{R}^1\mathfrak{F}_2(K_{i-1},Q^j) = 0$ 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 5.7.2) to see that

$$\mathrm{R}^1\mathfrak{F}_2(K_{i-1},L^j) \cong \mathrm{R}^1\mathfrak{F}_1(K_{i-1},L^j) \tag{10.34}$$

Since β and σ are onto, it follows that

$$\mathrm{R}^1\mathfrak{F}_2(K_i,L^j) = \mathrm{R}^1\mathfrak{F}_1(K_{i-1},L^{j+1}). \tag{10.35}$$

Combine (10.35) and (10.34) 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

$$\mathrm{R}^1\mathfrak{F}_1(A,L^{n-1}) \cong \mathrm{R}^1\mathfrak{F}_1(K_{-1},L^{n-1}) \cong \mathrm{R}^1\mathfrak{F}_1(K_{n-2},L^0) \cong \mathrm{R}^1\mathfrak{F}_1(K_{n-2},B) \tag{10.36}$$

Combine (10.36), (10.34), Theorem 10.2.9, and Theorem 10.2.11 to get

$$\begin{aligned}
\mathrm{R}^n\mathfrak{F}_2(A,B) &\cong \mathrm{R}^1\mathfrak{F}_2(A,L^{n-1}) \quad \text{(Theorem 10.2.9)}\\
&\cong \mathrm{R}^1\mathfrak{F}_1(A,L^{n-1}) \quad (10.34)\\
&\cong \mathrm{R}^1\mathfrak{F}_1(K_{n-2},B) \quad (10.36)\\
&\cong \mathrm{R}^n\mathfrak{F}_1(A,B) \quad \text{(Theorem 10.2.11)}
\end{aligned}$$

□

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 10.1.9), and right exact (Lemma 5.4.18) in both variables. If P is a projective right R-module, then $\mathfrak{T}_2(P,\cdot)$ is an exact functor (Exercise 5.4.6). By Exercise 10.1.12, $\mathrm{L}_n\mathfrak{T}_2(P,B) = 0$ 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 10.3.1. For $n \geq 0$ define

$$\operatorname{Tor}_n^R(A,B) = \mathrm{L}_n \mathfrak{T}_1(A,B) \cong \mathrm{L}_n \mathfrak{T}_2(A,B)$$

where the last isomorphism is due to Theorem 10.1.20. 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

$$\begin{aligned}\operatorname{Tor}_n^R(A,B) &= \mathrm{H}_n(P_\bullet \otimes_R B)\\ &= \mathrm{H}_n(A \otimes_R Q_\bullet).\end{aligned}$$

LEMMA 10.3.2. *Let M be a right R-module and N a left R-module.*

(1) *If M is flat or N is flat, then $\operatorname{Tor}_n^R(M,N) = 0$ 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*

$$\cdots \to \operatorname{Tor}_n^R(M,A) \to \operatorname{Tor}_n^R(M,B) \to \operatorname{Tor}_n^R(M,C) \xrightarrow{\partial} \operatorname{Tor}_{n-1}^R(M,A) \to \cdots$$
$$\cdots \to \operatorname{Tor}_1^R(M,C) \xrightarrow{\partial} M \otimes_R A \to M \otimes_R B \to M \otimes_R C \to 0$$

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*

$$\begin{aligned}\operatorname{Tor}_n^R(M,N) &= \mathrm{H}_n(C_\bullet \otimes_R N)\\ &= \mathrm{H}_n(M \otimes_R D_\bullet).\end{aligned}$$

(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 10.1.12.

(2) and (3): Follow straight from Exercise 10.1.13.

(4): By Part (1) flat modules are acyclic for the tensor functor. This follows from Theorem 10.1.15.

(5): Start with a projective resolution $P_\bullet \to M$ and use Lemma 5.4.16 to show

$$\mathrm{H}_n(P_\bullet \otimes_R N) \cong \mathrm{H}_n(N \otimes_{R^o} P_\bullet).$$

(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

$$\begin{aligned}(10.37)\quad & 0 \to \operatorname{Tor}^R_{n+1}(M_i,N) \xrightarrow{\partial} \operatorname{Tor}^R_n(M_i,K) \to 0 \to \cdots \\ & \cdots \to 0 \to \operatorname{Tor}^R_1(M_i,N) \xrightarrow{\partial} M_i \otimes_R K \to M_i \otimes_R P \to M \otimes_R N \to 0\end{aligned}$$

Another long exact sequence is

$$\begin{aligned}(10.38)\quad & 0 \to \operatorname{Tor}^R_{n+1}\left(\bigoplus_i M_i,N\right) \xrightarrow{\partial} \operatorname{Tor}^R_n\left(\bigoplus_i M_i,K\right) \to 0 \to \cdots \\ & \cdots \to 0 \to \operatorname{Tor}^R_1\left(\bigoplus_i M_i,N\right) \xrightarrow{\partial} \bigoplus_i M_i \otimes_R K \to \bigoplus_i M_i \otimes_R P \to \bigoplus_i M_i \otimes_R N \to 0.\end{aligned}$$

Take direct sums of (10.37) and combine with (10.38). In degrees one and zero, we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus_i \operatorname{Tor}^R_1(M_i,N) \arrow[r, "\partial"] \arrow[d, "\gamma"] & \bigoplus_i \left(M_i \otimes_R K\right) \arrow[r] \arrow[d, "\alpha"] & \bigoplus_i \left(M_i \otimes_R P\right) \arrow[d, "\beta"] \\
0 \arrow[r] & \operatorname{Tor}^R_1\left(\bigoplus_i M_i,N\right) \arrow[r, "\partial"] & \bigoplus_i M_i \otimes_R K \arrow[r] & \bigoplus_i M_i \otimes_R P
\end{tikzcd}$$

which is commutative and has exact rows. By Lemma 5.4.15, α and β are isomorphisms. Therefore γ is an isomorphism. In degrees $n+1$ and n, we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus_i \operatorname{Tor}^R_{n+1}(M_i,N) \arrow[r, "\partial"] \arrow[d, "\gamma"] & \bigoplus_i \operatorname{Tor}^R_n(M_i,K) \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & \operatorname{Tor}^R_{n+1}\left(\bigoplus_i M_i,N\right) \arrow[r, "\partial"] & \operatorname{Tor}^R_n\left(\bigoplus_i M_i,K\right) \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{aligned}(10.39)\quad & 0 \to \operatorname{Tor}^R_{n+1}\left(\varinjlim M_i,N\right) \xrightarrow{\partial} \operatorname{Tor}^R_n\left(\varinjlim M_i,K\right) \to 0 \to \cdots \\ & \cdots \to 0 \to \operatorname{Tor}^R_1\left(\varinjlim M_i,N\right) \xrightarrow{\partial} \varinjlim M_i \otimes_R K \to \varinjlim M_i \otimes_R P \to \varinjlim M_i \otimes_R N \to 0.\end{aligned}$$

Take direct limits of (10.37) and combine with (10.39). By Theorem 5.8.6, in degrees one and zero, we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \varinjlim \operatorname{Tor}_1^R(M_i,N) \arrow[r, "\partial"] \arrow[d, "\gamma"] & \varinjlim (M_i \otimes_R K) \arrow[r] \arrow[d, "\alpha"] & \varinjlim \left(M_i \otimes_R P\right) \arrow[d, "\beta"] \\
0 \arrow[r] & \operatorname{Tor}_1^R\left(\varinjlim M_i,N\right) \arrow[r, "\partial"] & \varinjlim M_i \otimes_R K \arrow[r] & \varinjlim M_i \otimes_R P
\end{tikzcd}$$

which is commutative and has exact rows. By Corollary 5.8.10, 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 10.3.3. *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. □

LEMMA 10.3.4. *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 10.1.4, $\mathrm{H}_n(P_\bullet\otimes_R N)\otimes_R S = \mathrm{H}_n\big((P_\bullet\otimes_R N)\otimes_R S\big)$. □

LEMMA 10.3.5. *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 10.3.3, 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 6.6.12 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

$$\begin{aligned}\operatorname{Tor}_n^R(M,N)\otimes_S S_P &= \mathrm{H}_n(A_\bullet\otimes_R M)\otimes_S S_P\\ &= \mathrm{H}_n\big(A_\bullet\otimes_R M\otimes_S S_P\big) \quad \text{(by Exercise 10.1.4)}\\ &= \operatorname{Tor}_n^R\big(M_P,N\big).\end{aligned}$$

Continue from the same starting point,

$$\begin{aligned}\operatorname{Tor}_n^R(M,N)\otimes_S S_P &= \mathrm{H}_n(A_\bullet\otimes_R M)\otimes_S S_P\\ &= \mathrm{H}_n\big(A_\bullet\otimes_R M\otimes_S S_P\big) \quad \text{(by Exercise 10.1.4)}\\ &= \mathrm{H}_n\big((A_\bullet\otimes_R R_Q)\otimes_{R_Q}(M\otimes_S S_P)\big)\\ &= \operatorname{Tor}_n^{R_Q}\big(M_P,N_Q\big)\end{aligned}$$

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 10.3.6. *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 10.3.5, $\operatorname{Tor}_1^{R_Q}\big(M_P,N_Q\big) = \big(\operatorname{Tor}_1^R(M,N)\big)_P = 0$.

(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 10.3.5 that $\big(\operatorname{Tor}_1^R(M,N)\big)_\mathfrak{m} = \operatorname{Tor}_1^{R_\mathfrak{n}}\big(M_\mathfrak{m},N_\mathfrak{n}\big)=0$. □

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 3.2.4 for the definition of torsion module.

LEMMA 10.3.7. *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 there is 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

$$\cdots \to \operatorname{Tor}_n^R(K,M) \to \operatorname{Tor}_n^R(K/R,M) \xrightarrow{\partial_n} \operatorname{Tor}_{n-1}^R(K/R,M) \to \dots$$
$$\cdots \to \operatorname{Tor}_1^R(K,M) \to \operatorname{Tor}_1^R(K/R,M) \xrightarrow{\partial_1} R \otimes_R M \to K \otimes_R M \to K/R \otimes_R M \to 0 \tag{10.40}$$

of R-modules (Lemma 10.3.2). Clearly R is flat, and by Lemma 6.1.4, K is flat. It follows from Lemma 10.3.3 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 6.1.1, $M \to K \otimes_R M$ is one-to-one, so $\partial_1 = 0$.

(3): By Exercise 5.4.20, $K \otimes_R M = 0$. The isomorphism is given by the connecting homomorphism ∂, which is natural by Theorem 10.1.14. □

3.3. Exercises.

EXERCISE 10.3.1. 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 10.3.2. Use Lemma 10.3.5 to give another proof of Proposition 6.8.2.

EXERCISE 10.3.3. 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 5.5.5, 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 5.5.5, if P is a projective R-module, the functor $\mathfrak{E}_2(P,\cdot)$ is exact. By Exercise 10.2.9, $\mathrm{R}^n\,\mathfrak{E}_2(P,B) = 0$ for all $n \geq 1$ and all B. By Theorem 5.6.2, if Q is an injective R-module, the functor $\mathfrak{E}_1(\cdot,Q)$ is exact. By Exercise 10.2.10, $\mathrm{R}^n\,\mathfrak{E}_1(A,Q) = 0$ for all $n \geq 1$ and all A.

DEFINITION 10.3.8. Let A and B be left R-modules. For $n \geq 0$ define

$$\operatorname{Ext}_R^n(A,B) = \mathrm{R}^n\,\mathfrak{E}_1(A,B) \cong \mathrm{R}^n\,\mathfrak{E}_2(A,B)$$

where the last isomorphism is due to Theorem 10.2.19. 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

$$\begin{aligned}\operatorname{Ext}_R^n(A,B) &= \mathrm{H}^n\big(\operatorname{Hom}_R(P_\bullet,B)\big)\\ &= \mathrm{H}^n\big(\operatorname{Hom}_R(A,Q^\bullet)\big).\end{aligned}$$

PROPOSITION 10.3.9. *Let M and N be left R-modules.*

(1) $\operatorname{Ext}_R^0(M,\cdot) = \operatorname{Hom}_R(M,\cdot)$ *and* $\operatorname{Ext}_R^0(\cdot,N) = \operatorname{Hom}_R(\cdot,N)$.

(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*

$$0 \to \operatorname{Hom}_R(M,A) \to \operatorname{Hom}_R(M,B) \to \operatorname{Hom}_R(M,C) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(M,A) \to \cdots$$
$$\cdots \to \operatorname{Ext}^n_R(M,A) \to \operatorname{Ext}^n_R(M,B) \to \operatorname{Ext}^n_R(M,C) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R(M,A) \to \cdots$$

and

$$0 \to \operatorname{Hom}_R(C,N) \to \operatorname{Hom}_R(B,N) \to \operatorname{Hom}_R(A,N) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(C,N) \to \cdots$$
$$\cdots \to \operatorname{Ext}^n_R(C,N) \to \operatorname{Ext}^n_R(B,N) \to \operatorname{Ext}^n_R(A,N) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R(C,N) \to \cdots$$

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 10.2.11 (1) and Exercise 10.2.12 (1).

(2): Follows straight from Exercise 10.2.11 (2) and Exercise 10.2.12 (2).

(3): Follows straight from Exercise 10.2.14, Proposition 5.5.5 (2), and the exact sequence of Part (2).

(4): Follows straight from Exercise 10.2.13, Theorem 5.6.2, 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

$$(10.41)\quad 0 \to \operatorname{Hom}_R(M_i,N) \to \operatorname{Hom}_R(M_i,Q) \to \operatorname{Hom}_R(M_i,C) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(M_i,N) \to 0 \to$$
$$\cdots \to 0 \to \operatorname{Ext}^n_R(M_j,C) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R(M_j,N) \to 0 \to \cdots$$

Another long exact sequence is

$$(10.42)\quad 0 \to \operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \to \operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i, Q\Big) \to$$
$$\operatorname{Hom}_R\Big(\bigoplus_{i\in I} M_i, C\Big) \xrightarrow{\delta^0} \operatorname{Ext}^1_R\Big(\bigoplus_{i\in I} M_i, N\Big) \to 0 \to$$
$$\cdots \to 0 \to \operatorname{Ext}^n_R\Big(\bigoplus_{i\in I} M_i, C\Big) \xrightarrow{\delta^n} \operatorname{Ext}^{n+1}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \to 0 \to \cdots$$

Take direct products of (10.41) and combine with (10.42). In degrees zero and one we get the diagram

$$\begin{tikzcd}
\operatorname{Hom}_R\left(\bigoplus_{i\in I} M_i, Q\right) \arrow[r] \arrow[d, "\alpha"] & \operatorname{Hom}_R\left(\bigoplus_{i\in I} M_i, C\right) \arrow[r, "\delta^0"] \arrow[d, "\beta"] & \operatorname{Ext}^1_R\left(\bigoplus_{i\in I} M_i, N\right) \arrow[r] \arrow[d, "\gamma"] & 0 \\
\prod_{i\in I} \operatorname{Hom}_R(M_i, Q) \arrow[r] & \prod_{i\in I} \operatorname{Hom}_R(M_i, C) \arrow[r, "\delta^0"] & \prod_{i\in I} \operatorname{Ext}^1_R(M_i, N) \arrow[r] & 0
\end{tikzcd}$$

which commutes and has exact rows. By Proposition 5.5.8, α and β are isomorphisms. Therefore γ is an isomorphism. In degrees n and $n+1$ we get the diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ext}^n_R\left(\bigoplus_{i\in I} M_i, C\right) \arrow[r, "\delta^n"] \arrow[d, "\beta"] & \operatorname{Ext}^{n+1}_R\left(\bigoplus_{i\in I} M_i, N\right) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & \prod_{i\in I} \operatorname{Ext}^n_R(M_j, C) \arrow[r, "\delta^n"] & \prod_{i\in I} \operatorname{Ext}^{n+1}_R(M_j, N) \arrow[r] & 0
\end{tikzcd}$$

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). □

LEMMA 10.3.10. *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 10.3.3 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 $M \otimes_R S$.

$$\begin{aligned}
\operatorname{Ext}^n_S(M \otimes_R S, N \otimes_R S) &= \mathrm{H}^n(\operatorname{Hom}_S(P_\bullet \otimes_R S, N \otimes_R S)) \\
&= \mathrm{H}^n(\operatorname{Hom}_R(P_\bullet, N) \otimes_R S) \quad \text{(Proposition 6.5.7)} \\
&= \mathrm{H}^n(\operatorname{Hom}_R(P_\bullet, N)) \otimes_R S \quad \text{(Exercise 10.2.4)} \\
&= \operatorname{Ext}^n_R(M,N) \otimes_R S
\end{aligned}$$

□

LEMMA 10.3.11. *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 5.5.10.

PROOF. (1): Let $C \to I_\bullet$ be an injective resolution of C. By the adjoint isomorphism,

$$\operatorname{Hom}_S(B \otimes_R A, I_\bullet) \cong \operatorname{Hom}_R(A, \operatorname{Hom}_S(B, I_\bullet)) \tag{10.43}$$

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 (10.43). Since A is projective, $\operatorname{Hom}_R(A,\cdot)$ is an exact covariant functor. Using Exercise 10.1.4, the nth homology group of the complex on the right hand side of (10.43) 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,

$$\operatorname{Hom}_S(B \otimes_R P_\bullet, C) \cong \operatorname{Hom}_R(P_\bullet, \operatorname{Hom}_S(B,C)) \tag{10.44}$$

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 (10.44), 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 (10.44). □

4. Cohomological Dimension of a Ring

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 $\operatorname{proj.dim}_R(M) \leq n$. 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 10.4.1. *(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

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r, "\phi"] \arrow[d, dotted, "\exists\rho"] & P \arrow[r, "\psi"] \arrow[d, dotted, "\exists\eta"] & M \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & L \arrow[r, "\alpha"] & Q \arrow[r, "\beta"] & M \arrow[r] & 0
\end{tikzcd}$$

with rows given. By Proposition 5.2.3 (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

$$0 \to K \xrightarrow{\delta} P \oplus L \xrightarrow{\pi} Q \to 0 \tag{10.45}$$

is exact. Since Q is projective, sequence (10.45) splits. □

DEFINITION 10.4.2. 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 10.4.3. 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 10.4.4. *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 $n \geq 0$, K_n and L_n are projectively equivalent.*

PROOF. Use induction on n. For $n = 0$, this is Lemma 10.4.1. The rest is left to the reader. □

THEOREM 10.4.5. *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, $\operatorname{Ext}^k_R(M,N) = 0$ *for all $k \geq n+1$.*
(3) For all R-modules N, $\operatorname{Ext}^{n+1}_R(M,N) = 0$.
(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 $\operatorname{Ext}^k_R(M,N) = 0$ 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

$$0 \to K_{n-1} \to P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0 \tag{10.46}$$

is exact. By Theorem 10.2.11, the groups $\operatorname{Ext}^{n+1}_R(M,N)$ and $\operatorname{Ext}^1_R(K_{n-1},N)$ are naturally isomorphic. By (3), both groups are zero and by Proposition 10.3.9 (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 10.4.4, 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 5.2.3 (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 (10.46) is a projective resolution of M of length less than or equal to n. □

LEMMA 10.4.6. *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 10.4.1.

(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 10.2.9, $\operatorname{Ext}_R^{n+1}(R/I, M)$ 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 10.4.2, K^n is an injective R-module. There exists an injective resolution of M of length less than or equal to n. □

LEMMA 10.4.7. *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 10.3.9 (3).

(2) implies (1): By Corollary 6.6.12, M is finitely presented, so there exists an exact sequence

$$0 \to A \xrightarrow{\alpha} B \to M \to 0 \tag{10.47}$$

such that B is a finitely generated free R-module and A is a finitely generated R-module. By (2), $\operatorname{Ext}_R^1(M, A) = 0$. The long exact sequence of Proposition 10.3.9 (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 (10.47) splits, so M is projective by Proposition 5.2.3 (1). □

LEMMA 10.4.8. *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,* $\operatorname{Ext}_R^{n+1}(M, R/I) = 0$.

PROOF. (1) implies (2): Follows from Exercise 10.4.1.

(2) implies (1): Let N be an arbitrary finitely generated R-module. By Exercise 10.4.6, it suffices to show $\operatorname{Ext}_R^{n+1}(M, N) = 0$. Proceed by induction on the number of generators of N. Suppose $N = Rx_1 + \cdots + Rx_m$. Let $N_0 = Rx_1$. By (2), $\operatorname{Ext}_R^{n+1}(M, N_0) = 0$ and by induction on m, $\operatorname{Ext}_R^{n+1}(M, N/N_0) = 0$. The long exact sequence of Proposition 10.3.9 (2) becomes

$$\cdots \to \operatorname{Ext}_R^{n+1}(M, N_0) \to \operatorname{Ext}_R^{n+1}(M, N) \to \operatorname{Ext}_R^{n+1}(M, N/N_0) \to \dots$$

which proves $\operatorname{Ext}_R^{n+1}(M, N) = 0$. □

COROLLARY 10.4.9. *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 $\operatorname{inj.dim}_R(M)\le n$. 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 10.4.6 and Lemma 10.3.10, $0=\operatorname{Ext}^{n+1}_R(R/I,M)_P=\operatorname{Ext}^{n+1}_{R_P}(R_P/IR_P,M_P)$. Lemma 10.4.6 implies $\operatorname{inj.dim}_{R_P}(M_P)\le n$.

Suppose $n=\operatorname{inj.dim}_R(M)$ is finite. By Lemma 10.4.6, there exists an ideal I in R such that $\operatorname{Ext}^n_R(R/I,M)\ne 0$. By Proposition 6.1.6 there exists a maximal ideal $\mathfrak{m}\in\operatorname{Max}R$ such that $\operatorname{Ext}^n_R(R/I,M)_\mathfrak{m}=\operatorname{Ext}^n_{R_\mathfrak{m}}(R_\mathfrak{m}/IR_\mathfrak{m},M_\mathfrak{m})\ne 0$. In follows from Lemma 10.4.6, $\operatorname{inj.dim}_{R_\mathfrak{m}}(M_\mathfrak{m})\ge n$.

(2): Is left to the reader. □

PROPOSITION 10.4.10. *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 $n\ge 0$, $\operatorname{proj.dim}(M)\le n$ 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 10.4.4, 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 10.3.2 (3) is

$$\operatorname{Tor}^R_1(M,k)\to K\otimes_R k\to k^\nu\xrightarrow{f}M\otimes_R k\to 0.$$

Therefore, $K\otimes_R k=0$. By Corollary 5.3.2, $K=0$, hence M is free.

(2): Assume $n\ge 0$ and $\operatorname{Tor}^R_{n+1}(M,k)=0$. If $n=0$, this is Part (1). Assume $n>0$. By Exercise 10.3.3, 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 10.1.9, $0=\operatorname{Tor}^R_{n+1}(M,k)=\operatorname{Tor}^R_1(K_{n-1},k)$. 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, $\operatorname{proj.dim}(M)\le n$. The converse is Exercise 10.4.1.

(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 10.3.2 (3) and Lemma 10.3.4 (1), there is a long-exact sequence

$$\dots\xrightarrow{\ell_a}\operatorname{Tor}^R_{n+1}(M,k)\to\operatorname{Tor}^R_{n+1}(M/aM,k)\xrightarrow{\partial}$$
$$\operatorname{Tor}^R_n(M,k)\xrightarrow{\ell_a}\operatorname{Tor}^R_n(M,k)\to\operatorname{Tor}^R_n(M/aM,k)\xrightarrow{\partial}$$

of R-modules. Left multiplication by a annihilates k, hence the long-exact sequence breaks down into short exact sequences

$$0\to\operatorname{Tor}^R_{n+1}(M,k)\to\operatorname{Tor}^R_{n+1}(M/aM,k)\xrightarrow{\partial}\operatorname{Tor}^R_n(M,k)\xrightarrow{\ell_a}0. \tag{10.48}$$

Let $d = \operatorname{proj.dim}_R(M)$. By Part (2) and Exercise 10.4.1,

$$\operatorname{Tor}_n^R(M,k) \begin{cases} = 0 & \text{if } n > d \\ \neq 0 & \text{if } n = d. \end{cases}$$

By (10.48),

$$\operatorname{Tor}_n^R(M/aM,k) \begin{cases} = 0 & \text{if } n > d+1 \\ \neq 0 & \text{if } n = d+1. \end{cases}$$

By Part (2), $\operatorname{proj.dim}_R(M/aM) = d+1$. □

LEMMA 10.4.11. *Let R be a commutative noetherian ring. The following are equivalent, for any finitely generated R-module M.*

(1) $\operatorname{proj.dim}_R(M) \le n$.
(2) $\operatorname{Tor}_{n+1}^R(M,R/\mathfrak{m}) = 0$ *for all* $\mathfrak{m} \in \operatorname{Max} R$.

PROOF. By Corollary 10.4.9, (1) is equivalent to $\operatorname{proj.dim}_{R_\mathfrak{m}}(M_\mathfrak{m}) \le n$ for all $\mathfrak{m} \in \operatorname{Max} R$. By Proposition 10.4.10, 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 10.3.4 this is equivalent to (2). □

PROPOSITION 10.4.12. *(M. Auslander) Let R be a commutative ring and $n \ge 0$. The following are equivalent.*

(1) $\operatorname{proj.dim}_R(M) \le n$ *for all R-modules M.*
(2) $\operatorname{proj.dim}_R(M) \le n$ *for all finitely generated R-modules M.*
(3) $\operatorname{inj.dim}_R(M) \le n$ *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 10.4.6, 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 10.2.9, $\operatorname{Ext}_R^{n+1}(R/I,M) = \operatorname{Ext}_R^1(R/I,K^n)$. Since R/I is finitely generated, by (2) and Exercise 10.4.1, $\operatorname{Ext}_R^{n+1}(R/I,M) = 0$. By Exercise 10.4.2, K^n is an injective R-module. This proves (3).

(3) implies (4): Follows from Exercise 10.4.1.

(4) implies (1): Follows from Theorem 10.4.5. □

DEFINITION 10.4.13. 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 10.4.12.

LEMMA 10.4.14. *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 10.4.12.
(b) implies (c), by Proposition 10.4.12.
(c) implies (d): Follows from Exercise 10.4.1.
(b) implies (e): Follows from Exercise 10.4.1.
(e) implies (b): Follows from Lemma 10.4.11.
(d) implies (b): Follows from Exercise 10.4.6.
(2): Follows from Part (1) and Corollary 10.4.9. □

THEOREM 10.4.15. *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) $\operatorname{coh.dim} R \leq n$.
   (b) $\operatorname{Tor}^R_{n+1}(k,k) = 0$.
(2) $\operatorname{coh.dim} R = \operatorname{proj.dim}_R(k)$.

PROOF. (1): (a) implies (b): Follows directly from Definition 10.4.13.
(b) implies (a): Assume $\operatorname{Tor}^R_{n+1}(k,k) = 0$. By Proposition 10.4.10 (2), $\operatorname{proj.dim}_R(k) \leq n$. By Exercise 10.4.1, $\operatorname{Tor}^R_{n+1}(M,k) = 0$. By Proposition 10.4.10 (2), $\operatorname{proj.dim}_R(M) \leq n$. By Lemma 10.4.14, $\operatorname{coh.dim} R \leq n$.
(2): Is left to the reader. □

PROPOSITION 10.4.16. *Let $\phi : R \to S$ be a local homomorphism of commutative noetherian local rings. If S is a flat R-module, then* $\operatorname{coh.dim}(R) \leq \operatorname{coh.dim}(S)$.

PROOF. Let M and N be arbitrary finitely generated R-modules. By Lemma 10.3.4,

$$\operatorname{Tor}^R_n(M,N) \otimes_R S = \operatorname{Tor}^S_n(M \otimes_R S, N \otimes_R S) \tag{10.49}$$

for all $n \geq 0$. If $\operatorname{coh.dim}(S) = d$ is finite, then by Lemma 10.4.14, the groups in (10.49) are zero for $n > d$. By Exercise 6.5.12, S is a faithfully flat R-module, hence $\operatorname{Tor}^R_{d+1}(M,N) = 0$. By Lemma 10.4.14, $\operatorname{coh.dim}(R) \leq d$. □

4.1. Exercises.

EXERCISE 10.4.1. 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 10.4.2. Let R be a commutative ring and E an R-module. Then E is injective if and only if $\operatorname{Ext}^1_R(R/I,E) = (0)$ for all ideals I in R.

EXERCISE 10.4.3. 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 10.4.4. 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 10.4.5. 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 10.4.6. 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 10.4.7. Let k be a field. Prove that $\operatorname{coh.dim}(k) = 0$.

EXERCISE 10.4.8. 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 10.4.9. 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 $\operatorname{proj.dim}_R(S) \leq \operatorname{proj.dim}_R(M)$.

CHAPTER 11

Krull Dimension of a Commutative Ring

1. Graded Rings and Modules

Throughout this section all rings are commutative. We refer the reader to Section 9.4 for the definitions of graded rings and modules.

1.1. Associated Prime Ideals of a Graded Module.

LEMMA 11.1.1. *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. □

If N satisfies the equivalent properties of Lemma 11.1.1, 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 11.1.2. *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. □

LEMMA 11.1.3. *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 8.2.2 (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 11.1.1 (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 11.1.1 (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 8.1.3 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 8.2.6 (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. □

The next result is the graded counterpart of Theorem 8.2.7.

THEOREM 11.1.4. *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* $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_r = M$ *of* M *by graded submodules, a set of homogeneous prime ideals* $P_i \in \operatorname{Spec} R$*, and integers* n_i *such that* $M_i/M_{i-1} \cong (R/P_i)(-n_i)$ *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 8.2.2, $\operatorname{Assoc}(M) \neq \emptyset$. By Lemma 11.1.3 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 8.2.2, $\operatorname{Assoc}(M/N) \neq \emptyset$. By Lemma 11.1.3 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 $\operatorname{annih}\big(M_i/M_{i-1}\big) = \operatorname{annih}\big((R/P_i)(-n_i)\big) = P_i$. Because $M_0 = (0)$, $x \in \prod_{i=1}^r P_i$ 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 $P \supseteq \prod_{i=1}^r P_i$. Proposition 2.1.22 implies $P \supseteq P_i$ 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

$$\big(M_i/M_{i-1}\big)_P = \big((R/P_i)(-n_i)\big)_P. \tag{11.1}$$

If $P = P_i$, then the right-hand side of (11.1) 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 (11.1) is (0). That is, $(M_{i-1})_P = (M_i)_P$. 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 11.1.5. 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 8.3.8 for a graded ring and module.

THEOREM 11.1.6. *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 8.3.8, substituting graded submodules.) □

1.2. Numerical Polynomials.

DEFINITION 11.1.7. 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 11.1.8. *In the context of Definition 11.1.7,*

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. □

PROPOSITION 11.1.9. *In the context of Definition 11.1.7,*

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 11.1.8 (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 11.1.8 (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 11.1.8 (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 $p(x) + c$. □

1.3. The Hilbert Polynomial.

EXAMPLE 11.1.10. Let A be a commutative artinian ring. By Proposition 7.4.4, A is an A-module of finite length, say $\ell(A)$. If $S = A[x_0, \ldots, x_r]$, 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 $x_0, \ldots, x_r$. The reader should verify that $\operatorname{Rank}_A(S_d) = \rho(d) = \binom{r+d}{d} = \binom{r+d}{r}$. By Exercise 7.4.2, 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 11.1.11. Let A be a commutative artinian ring and $S = A[x_0, \ldots, x_r]$. 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 $\{\xi_1, \ldots, \xi_m\} \subseteq M^h$ 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 6.6.22, $\ell(M_d) \leq \sum_{i=1}^{m} \ell(S_{d-d_i})$. By Example 11.1.10, it follows that $\ell(M_d)$ is finite.

DEFINITION 11.1.12. Let A be a commutative artinian ring and $S = A[x_0, \ldots, x_r]$. 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 11.1.11, $\varphi_M(d) \in \mathbb{Z}$ for all d.

THEOREM 11.1.13. *(Hilbert-Serre) Let A be a commutative artinian ring and $S = A[x_0, \ldots, x_r]$. 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 6.6.22 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 11.1.4 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 6.6.22 implies $\varphi_M(d) = \varphi_M(d-1) + \varphi_{M'}(d)$. In the notation of Proposition 11.1.9, 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 11.1.9, $P_M(z)$ exists. □

2. Krull Dimension of a Commutative Noetherian Ring

2.1. 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 11.2.1. Let R be a commutative ring.

(1) If R is artinian, then by Proposition 7.4.3, every prime ideal is maximal, so $\dim(R) = 0$.

(2) If R is a PID, then by Lemma 2.3.4, nonzero prime ideals are maximal, so $\dim(R) \leq 1$. If R is not a field, $\dim(R) = 1$.

(3) If P is a minimal prime over-ideal of (0), then $\operatorname{ht}(P) = 0$.

LEMMA 11.2.2. *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 $\dim(R/I) + \operatorname{ht}(I) \leq \dim(R)$.

(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 $P = (0)$.

PROOF. Is left to the reader. □

DEFINITION 11.2.3. 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 11.2.4. *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 7.4.4.

(2) implies (1): Follows from Proposition 6.6.20 and Exercise 6.6.2.

(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 6.1.7 says $M_P \neq (0)$. Therefore $P \in \operatorname{Supp}(M)$ and because P is minimal, Theorem 8.2.6 says $P \in \operatorname{Assoc}(M)$. By Lemma 8.2.1, M contains a submodule isomorphic to R/P. The integral domain R/P contains a nonzero prime ideal, so by Proposition 7.4.4, the R-module R/P has infinite length. Therefore $\ell(M) = \infty$. □

2.2. The Krull Dimension of a Noetherian Semilocal Ring.

DEFINITION 11.2.5. Let R be a commutative noetherian semilocal ring with Jacobson radical $J = \operatorname{J}(R)$. Let I be an ideal which is contained in J. By Exercise 7.4.6, 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 11.2.6. Let R be a commutative noetherian local ring and $I \subseteq \mathfrak{m}$ an ideal contained in the maximal ideal of R. By Corollary 8.1.7, I is an ideal of definition for R if and only if I is $\mathfrak{m}$-primary.

PROPOSITION 11.2.7. *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 9.4.3, the associated graded ring for the I-adic filtration of R is $R^* = \mathrm{gr}_I(R) = \bigoplus_{n\geq 0} I^n/I^{n+1}$. As in Example 9.4.4, the associated graded R^*-module for the I-adic filtration of M is $M^* = \mathrm{gr}_I(M) = \bigoplus_{n\geq 0} I^nM/I^{n+1}M$. By Proposition 9.4.8, M^* is a finitely generated R^*-module. Because I is finitely generated, we can write $I = Ru_0 + \cdots + Ru_m$. Let $S = (R/I)[x_0,\dots,x_m]$. 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 11.1.10, 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 11.1.11 we computed $P_{M^*}(d) = \ell(I^dM/I^{d+1}M) \leq \sum P_{R^*}(d)$ 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 $I^dM \subseteq I^{d-1}M \subseteq \cdots \subseteq IM \subseteq M$, we compute

$$\ell(M/I^dM) = \sum_{j=0}^{d-1} \ell(I^jM/I^{j+1}M)$$

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 $\ell(M/I^dM) \leq \ell(M/J^{\nu d}M)$. 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. □

PROPOSITION 11.2.8. *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 $C/I^nC = B/(A + I^nB)$, we have

$$\ell(C/I^nC) = \ell(B/(A+I^nB)) \leq \ell(B/I^nB)$$

hence $\mathrm{d}(C) \leq \mathrm{d}(B)$. From the exact sequence

$$0 \to (A+I^nB)/I^nB \to B/I^nB \to B/(A+I^nB) \to 0$$

and $(A+I^nB)/I^nB = A/(A\cap I^nB)$, we have

$$\begin{aligned}\chi_{B,I}(n) - \chi_{C,I}(n) &= \ell(B/I^nB) - \ell(B/(A+I^nB))\\ &= \ell((A+I^nB)/I^nB)\\ &= \ell(A/(A\cap I^nB)).\end{aligned}$$

By Artin-Rees, Corollary 9.4.13, there exists an integer n_0 such that $I^{n+n_0}A \subseteq A \cap (I^nB) \subseteq I^{n-n_0}A$ for all $n > n_0$. This implies

$$\ell(A/I^{n+n_0}A) \geq \ell(A/(A+I^nB)) \geq \ell(A/I^{n-n_0}A)$$

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. □

PROPOSITION 11.2.9. *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 $\operatorname{ht}(P)$ 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 9.4.20, this implies $J^N = (0)$. By Proposition 7.4.2, R is artinian and as we have seen in Example 11.2.1, $\dim(R) = 0$.

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 11.2.8 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 11.2.10. *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 $x_1, \ldots, x_r$ 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 11.2.8, $\mathrm{d}(M) \leq \mathrm{d}(M/xM)$. 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 11.2.4 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 8.3.8 says $\operatorname{annih}(M)$ has a primary decomposition. By Theorem 8.2.6, there are only finitely many minimal prime over-ideals of $\operatorname{annih}(M)$. Suppose $P_1, \dots, P_t$ are those minimal prime over-ideals of $\operatorname{annih}(M)$ such that $\dim(R/P_i) = r$. Assume $\operatorname{Max}(R) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_u\}$, 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 8.1.3, for all i there is no containment relation $\mathrm{J}(R) \subseteq P_i$. By Lemma 8.1.2, $\mathrm{J}(R)$ 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 $\operatorname{annih}(M/xM) \supseteq xR + \operatorname{annih}(M)$. If $P \in \operatorname{Spec}(R)$ and $\operatorname{annih}(M) \subseteq P$, 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 11.2.10 (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 11.2.11. *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 11.2.1, $\mathrm{d}(M/(x_1M + \cdots + x_rM)) = 0$ and by Lemma 11.2.10 (1), $\mathrm{d}(M/(x_1M + \cdots + x_{r-1}M) \leq 1$. Iterate this argument to get $\mathrm{d}(M) \leq r$, which implies $\mathrm{d}(M) \leq \delta(M)$. By Lemma 11.2.10 (2) we have $\delta(M) \leq \dim(M)$. To finish, it is enough to prove $\dim(M) \leq \mathrm{d}(M)$.

By Theorem 8.2.7 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 $\operatorname{Assoc}(M) \subseteq \{P_1, \dots, P_n\} \subseteq \operatorname{Supp}(M)$. By Exercise 8.2.8, every minimal prime over-ideal of $\operatorname{annih}(M)$ is included in the set $\{P_1, \dots, P_n\}$. By Proposition 11.2.8, $\mathrm{d}(M_i)$ 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 $\{\mathrm{d}(R/P_i) \mid 1 \leq i \leq n\}$. By Proposition 11.2.9, it follows that $\mathrm{d}(M)$ is greater than or equal to the maximum number in the set $\{\dim(R/P_i) \mid 1 \leq i \leq n\}$. A chain of prime ideals in $\operatorname{Spec}(R/\operatorname{annih}(M))$ corresponds to a chain in $\operatorname{Spec}(R)$ of prime ideals containing $\operatorname{annih}(M)$. 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 $\{\dim(R/P_i) \mid 1 \leq i \leq n\}$. This completes the proof. □

COROLLARY 11.2.12. *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 $\mathrm{ht}(P) \leq n$.
(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 11.2.11, $n \geq \delta(R_P) = \dim(R_P)$. By Lemma 11.2.2, $\mathrm{ht}(P) = \dim(R_P)$.

(2): By Part (1), $\mathrm{ht}(P) \leq 1$. If $\mathrm{ht}(P) = 0$, then P is a minimal prime in $\mathrm{Spec}(R)$. By Theorem 8.2.6 and Proposition 8.2.2, every element of P is a zero divisor. This is a contradiction, since $x \in P$. □

COROLLARY 11.2.13. *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) $\dim(R) \leq \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.

(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 11.2.11.

(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 6.4.1, $Rx_1 + \cdots + Rx_t = \mathfrak{m}$. By Part (1), $\dim(R) = \delta(R) \leq t$.

(3): By Corollary 11.2.12 (2), $\mathrm{ht}(Rx) = 1$. By Lemma 11.2.2, $\dim(R/xR) \leq \dim(R) - 1$. The reverse inequality follows from Lemma 11.2.10 (1) and Part (1).

(4): By Corollary 9.4.16, $R/\mathfrak{m}^n = \hat{R}/\hat{\mathfrak{m}}^n$, so the Hilbert polynomials $\chi_{R,\mathfrak{m}}$ and $\chi_{\hat{R},\hat{\mathfrak{m}}}$ are equal. □

DEFINITION 11.2.14. Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and assume $\dim(R) = d$. According to Corollary 11.2.13 (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 11.2.15. *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 $1 \leq i \leq d$.

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 $\dim(R_i) = \delta(R_i) \leq d - i$. 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 $\delta(R) = d \leq i + e$, or $e = \dim(R_i) \geq d - i$. □

2.3. Exercises.

EXERCISE 11.2.1. Let R be a commutative noetherian semilocal ring and M a nonzero R-module of finite length. Then $\mathrm{d}(M) = 0$.

EXERCISE 11.2.2. 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 11.2.3. Let R be a commutative ring and I an ideal of R. Then $\dim(R/I) = \dim(R/\mathrm{Rad}(I))$.

EXERCISE 11.2.4. 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 11.2.5. 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
$$\dim_{W^{-1}R}(W^{-1}M) \le \dim_R(M).$$
(Hint: Corollary 6.8.11.)

2.4. 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 6.3.3. 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 6.4.3. By Exercise 6.4.2, 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 11.2.16. *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) $\operatorname{ht}(Q) \le \operatorname{ht}(P) + \operatorname{ht}(Q/PS)$.
(2) $\dim(S_Q) \le \dim(R_P) + \dim(S_Q \otimes_R k_P)$ *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) $\dim(S) \ge \dim(R)$*, and*
   (b) for any ideal $I \subseteq R$, $\operatorname{ht}(I) = \operatorname{ht}(IS)$.

PROOF. (1): Follows from (2) by Lemma 11.2.2 and Exercise 6.4.2.

(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 $\dim(S) \le \dim(R) + \dim(S/PS)$. 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 11.2.3, $\dim(S/IS) = \dim(S/PS)$. 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 $\dim(S) \le r + n = \dim(S/PS) + \dim(R)$.

(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 9.5.1, 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 $\operatorname{ht}(Q) \ge r + n$.

(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), $\dim(S) \ge \dim(S_\mathfrak{n}) \ge \dim(R_\mathfrak{m}) = \dim(R)$.

(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 11.2.9 (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 11.2.17. *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 9.5.4 (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 $\dim(S) \leq \dim(R)$. By Theorem 9.5.4 (3), a chain of length n in $\operatorname{Spec}(R)$ lifts to a chain of length n in $\operatorname{Spec}(S)$. Thus $\dim(S) \leq \dim(R)$.

(2): We have $Q \subseteq (Q \cap R)S$ and by Theorem 9.5.4 (2), Q is a minimal prime over-ideal of $(Q \cap R)S$. Apply Theorem 11.2.16 (1).

(3): Since going down holds for $R \to S$, by Theorem 11.2.16 (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 $\operatorname{ht}(J) = \operatorname{ht}(Q) = \operatorname{ht}(Q \cap R) \geq \operatorname{ht}(J \cap R)$. Pick P to be a minimal prime over-ideal for $J \cap R$. By Exercise 9.1.2, S/J is an integral extension of $R/(J \cap R)$. By Theorem 9.5.4 (1), there exists $Q \in \operatorname{Spec}(S)$ such that $Q \supseteq J$ and $Q \cap R = P$. Then $\operatorname{ht}(J \cap R) = \operatorname{ht}(P) = \operatorname{ht}(Q) \geq \operatorname{ht}(J)$. □

THEOREM 11.2.18. *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* $\dim(S \otimes_R k_p) \geq \dim(S \otimes_R k_q)$.

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 $\operatorname{ht}(Q_{n+m}/Q_0) \geq n + m$. Apply Theorem 11.2.16 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

$$\begin{aligned} n + m &\leq \operatorname{ht}(Q_{n+r}/Q_0) \\ &\leq \operatorname{ht}(p/q) + \operatorname{ht}(Q_{n+m}/(Q_0 + pS)) \\ &\leq \operatorname{ht}(p/q) + \operatorname{ht}(Q_{n+m}/pS) \\ &\leq \operatorname{ht}(p/q) + \dim(S \otimes_R k_p). \end{aligned}$$

From which it follows that $\dim(S \otimes_R k_q) \leq \dim(S \otimes_R k_p)$. □

3. Emmy Noether's Normalization Lemma

THEOREM 11.3.1. *Let R be a commutative noetherian ring and $x_1, \ldots, x_n$ some indeterminates.*

(1) $\dim(R[x_1, \ldots, x_n]) = \dim(R) + n$.
(2) If R is a field, $\dim(R[x_1, \ldots, x_n]) = n$ *and the ideal $(x_1, \ldots, x_j)$ is a prime ideal of height j for all $j = 1, \ldots, n$.*

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 11.2.16, $\dim(S) \ge \dim(S_Q) = \dim(R_P)+1 = \dim(R)+1$. Conversely, pick $Q \in \operatorname{Spec}(S)$ such that $\operatorname{ht}(Q) = \dim(S)$. Set $P = Q \cap R$. By Theorem 11.2.16, $\dim(S) = \dim(S_Q) = \dim(R_P)+1 \le \dim(R)+1$. □

THEOREM 11.3.2. *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 $\mu(x_1^{e_1}\cdots x_n^{e_n}) = e_1 + e_2v^2 + \cdots + e_nv^n$. 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

$$\begin{aligned} y_1 &= f(x_1, y_2 + x_1^{v^2}, \dots, y_n + x_1^{v^n}) \\ &= \sum_{i=1}^{t} a_i f_i(x_1, y_2 + x_1^{v^2}, \dots, y_n + x_1^{v^n}) \\ &= \sum_{i=1}^{t} a_i x_1^{e_{1i}} (y_2 + x_1^{v^2})^{e_{2i}} \cdots (y_n + x_1^{v^n})^{e_{ni}} \\ &= \sum_{i=1}^{t} a_i \big(x_1^{\mu(f_i)} + g_i(x_1, y_2, \dots, y_n)\big) \end{aligned}$$

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

$$y_1 = a_1 x_1^{\mu(f_i)} + g(x_1, y_2, \dots, y_n) \tag{11.2}$$

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 (11.2) 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. It follows from results in Section 4.10 that 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 9.5.4 (5), going down holds between B and A. By Theorem 11.3.1, the ideal (y_1) in $k[y_1,\dots,y_n]$ is prime of height one. By Theorem 11.2.17, $\operatorname{ht}(I) = \operatorname{ht}(I \cap B)$. Since $(y_1) \subseteq I \cap B$, putting all this together proves that $(y_1) = I \cap B$.

Step 2: $r > 1$. By Exercise 11.2.4, 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 11.2.17, $\operatorname{ht}(I) = \operatorname{ht}(I') = r$. 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 11.3.3. *(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 11.3.2, 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 11.2.17, 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 4.10. □

COROLLARY 11.3.4. *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 11.3.3, 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 9.5.4 (5) and Theorem 11.2.17 (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 11.2.17 (1), $\dim(A/p) = \dim(B/p\cap B)$. By Theorem 11.3.2, 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). □

4. More Flatness Criteria

In this section we prove some necessary results on flatness. The material in this section is from various sources, including [**20**], [**13**], [**19**], and [**24**].

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 11.4.1. *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. □

We say that Z is a *constructible set* in X if Z is a finite union of locally closed sets in X. By Lemma 11.4.1, 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 11.4.2. *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. □

PROPOSITION 11.4.3. *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 1.4.7 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 1.4.4, $\overline{V_i \cap F_i} = F_i$. 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 1.4.5 (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 11.4.4. *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 6.3.3. 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 6.3.8, 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 11.4.5. *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 $x_1, \dots, x_n$ in S such that $S = R[x_1, \dots, x_n]$. Further, assume $x_1, \dots, x_r$ are algebraically independent over R, while each of the elements $x_{r+1}, \dots, x_n$ satisfies an algebraic relation over $T = R[x_1, \dots, x_r]$. For each $j = r+1, \dots, n$ 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 $x_1, \dots, x_r$. 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 $PT = P[x_1, \dots, x_r]$ 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 9.5.4, there exists a prime ideal Q in S_{PT} lying over $(PT)T_{PT}$. On the left side of this diagram

$$\begin{tikzcd}
 & S_{PT} = S \otimes_T T_{PT} \arrow[dl, dash] \arrow[dr, dash] & \\
S \arrow[dr, dash] \arrow[dd, dash] & & T_{PT} \arrow[dl, dash] \\
 & T = R[x_1, \dots, x_r] \arrow[dl, dash] & \\
R & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & Q \arrow[dl, dash] \arrow[dr, dash] & \\
Q \cap S \arrow[dr, dash] \arrow[dd, dash] & & (PT)T_{PT} \arrow[dl, dash] \\
 & Q \cap T = PT \arrow[dl, dash] & \\
P & &
\end{tikzcd}$$

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, $P = Q \cap R = Q \cap S \cap R = \theta^\sharp(Q \cap S)$. □

LEMMA 11.4.6. *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 6.3.9, $\operatorname{Spec} R[a^{-1}]$ maps homeomorphically onto $U(a)$. By Exercise 6.3.8, $\operatorname{Spec} R/I$ 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 6.3.6, $\operatorname{Spec} S$ decomposes into the disjoint union $\operatorname{Spec} S_1 \cup \cdots \cup \operatorname{Spec} S_n$. The image of $\operatorname{Spec} S$ is Z. □

THEOREM 11.4.7. *(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 11.4.3, assume $\operatorname{im} \theta^\sharp \cap Y$ is dense in Y. By Lemma 6.3.10,

$Y = V(P)$ 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 11.4.4, $\bar{\theta}$ is one-to-one. By Lemma 11.4.5, $\operatorname{im}\theta^\sharp \cap Y$ contains a nonempty open subset of Y. Proposition 11.4.3 implies $\operatorname{im}\theta^\sharp$ is constructible.

Step 2: Let Z be a constructible set in $\operatorname{Spec} S$. By Lemma 11.4.6 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 11.4.8. *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 5.8.4, $S = \varinjlim_\alpha S_\alpha$, 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 11.4.7, 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 11.4.9. *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 11.4.3, $Y_i \cap Z$ is a dense subset of Y_i. For each α, $Y_i \cap Z_\alpha$ is dense in Y_i. By Proposition 11.4.3, $Y_i \cap Z_\alpha$ 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 11.4.10. *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 9.5.3, going down holds and by Lemma 6.5.4, $\phi^\sharp$ is onto. This case reduces to (3).

If condition (2) is satisfied, then by Theorem 9.5.4, 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 11.4.8, Y is pro-constructible. By Lemma 11.4.9, 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 9.5.1, 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 11.4.11. *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 11.4.7, $\phi^\sharp(U)$ 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 9.5.1, 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 11.4.9, $\operatorname{Spec} R - \phi^\sharp(U)$ is closed. □

4.2. Local Criteria for Flatness. Let R be a commutative ring and I an ideal of R. Let M be an R-module. In Example 9.4.3 and Example 9.4.4 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 11.4.12. 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 9.4.20 (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 11.4.13. *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 10.3.3.

(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 10.3.2 (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 5.7.2) 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 5.4.22).

(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 6.8.4 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 9.4.13 there exists $\nu \ge n$ such that $J \cap I^\nu \subseteq I^n J$. Consider the commutative diagram

(11.3)
$$\begin{tikzcd}
J \otimes_R M \arrow[r, "\phi"] \arrow[d, "\mu"] & \big(J/(J \cap I^\nu)\big) \otimes_R M \arrow[r, "\psi"] \arrow[d, "\tau"] & \big(J/I^nJ\big) \otimes_R M \arrow[d] \\
M \arrow[r] & M/I^\nu M \arrow[r] & M/I^nM
\end{tikzcd}$$

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 6.8.4, 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 $\big(J/J \cap I^{\nu}\big) \otimes_{R/I^{\nu}} \big(M/I^{\nu}M\big) = \big(J/J \cap I^{\nu}\big) \otimes_R M$, this implies the sequence

$$0 \to \big(J/J \cap I^{\nu}\big) \otimes_R M \xrightarrow{\tau} M/I^{\nu}M$$

is exact. In (11.3), since τ is one-to-one it follows that $\ker(\mu) \subseteq \ker(\psi\phi) = I^n(J \otimes_R M)$. □

COROLLARY 11.4.14. *Let $f : R \to S$ be a local homomorphism of local noetherian rings. Let M be a finitely generated S-module and t an element of R that is not a zero divisor. The following are equivalent.*

(1) M is a flat R-module.
(2) M/tM is a flat R/tR-module, and $\ell_t : M \to M$ is one-to-one.

PROOF. According to Example 11.4.12 (1), M is ideal-wise separated for $I = tR$. Use Exercise 6.8.5 and apply the equivalence of Parts (1) and (3) in Theorem 11.4.13. □

PROPOSITION 11.4.15. *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

$$x \in \bigcap_{n\geq 1} \mathfrak{m}^n A \subseteq \bigcap_{n\geq 1} \mathfrak{n}^n A,$$

which proves $x = 0$, by Corollary 9.4.20. Fix $n \geq 1$ and assume $x \in \mathfrak{m}^n A$. 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 6.8.4 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 11.4.12 (1) the hypotheses of Theorem 11.4.13 (4) are satisfied. Therefore $\operatorname{coker}(\sigma)$ is a flat R-module. □

COROLLARY 11.4.16. *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 10.3.6, $M_\mathfrak{m}$ 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 6.1.6, $R_\mathfrak{n}/(\mathfrak{n}R_\mathfrak{n})$ 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 11.4.15 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 11.4.15 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 6.1.6, $\ell_f : M \to M$ is one-to-one. By Corollary 10.3.6, M/fM is a flat R-module. □

COROLLARY 11.4.17. *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 11.4.16. □

COROLLARY 11.4.18. *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. 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 11.4.15. □

In Corollary 11.4.19, the reader is referred to Definition 12.3.1 for the definition of a regular sequence for an R-module contained in an ideal of R.

COROLLARY 11.4.19. *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 11.4.18 and induction on r. □

4.3. Theorem of Generic Flatness.

THEOREM 11.4.20. *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 8.2.7, 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 9.1.3 (1), $S_1 = S[\alpha^{-1}]$ is finitely generated as an $R_1 = R[\alpha^{-1}]$-module. Let $u_1, \dots, u_v$ be a maximal subset in S_1 which is linearly independent over R_1. Define $\phi : R_1^{(v)} \to S_1$ by $(a_1, \dots, a_v) \mapsto \sum a_i u_i$. 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 11.3.3), there exist $y_1, \dots, y_n$ in SK which are algebraically independent over K and such that SK is integral over $K[y_1, \dots, y_n]$. For some element β of $R-(0)$, $\beta y_i \in S$. Re-label if necessary, and assume $R[y_1, \dots, y_n] \subseteq S$. There exist $s_1, \dots, s_k$ such that $S = R[s_1, \dots, s_k]$. Each s_i is integral over $K[y_1, \dots, y_n]$, so there exists a polynomial $p_i(x) \in K[y_1, \dots, y_n][x]$ such that $p_i(s_i) = 0$. There exists a nonzero element α in $R-(0)$ such that $\alpha p_i(x) \in R[y_1, \dots, y_n][x]$ for all i. Therefore, $R[\alpha^{-1}][y_1, \dots, y_n] \subseteq S[\alpha^{-1}]$ is an integral extension of integral domains. Let $R_1 = R[\alpha^{-1}]$, $S_1 = S[\alpha^{-1}]$, and $T = R_1[y_1, \dots, y_n]$. Then S_1 is a finitely generated integral extension of T, so by Theorem 9.1.3 (1), S_1 is finitely generated as a T-module. Let $u_1, \dots, u_v$ be a maximal subset in S_1 which is linearly independent over T. Define $\phi : T^{(v)} \to S_1$ by $(a_1, \dots, a_v) \mapsto \sum a_i u_i$. 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 $f = \alpha g$. □

COROLLARY 11.4.21. *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 11.4.21 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 11.4.22. *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 11.4.9 (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 11.4.12 (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 11.4.13), 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 11.4.20 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 6.1.7, 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 10.3.5, $\operatorname{Tor}_1^R(M, R_0) \otimes_S S_P = 0$. Again by Lemma 10.3.5, $\operatorname{Tor}_1^R(M, R_0)$ is a finitely generated S-module. By Lemma 6.1.7, 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 10.3.5, $\operatorname{Tor}_1^R\big(M_Q, R_0\big) = 0$ 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 $V(P)$. □

5. Complete I-adic Rings and Inverse Limits

The material in this section is from various sources, including [**6**], [**24**], [**13**].

PROPOSITION 11.5.1. *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 9.3.7, Corollary 9.3.10, and the definition of inverse limit (Definition 5.8.12).

(2): For all $\ell \le k$, the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{n}^{i+1}_{i+\ell} \arrow[r] \arrow[d] & A_{i+\ell} \arrow[r, "\phi^{i+\ell}_{i}"] \arrow[d, "\phi^{i+\ell}_{i+k}"] & A_i \arrow[r] \arrow[d, "\phi^{i}_{i}"] & 0 \\
0 \arrow[r] & \mathfrak{n}^{i+1}_{i+k} \arrow[r] & A_{i+k} \arrow[r, "\phi^{i+k}_{i}"] & A_i \arrow[r] & 0
\end{tikzcd}$$

commutes and the vertical arrows are onto. By Proposition 5.8.19, if we define $\mathfrak{m}_{i+1}$ to be the kernel of $\alpha_i : A \to A_i$, then

$$\mathfrak{m}_{i+1} = \varprojlim_{k} \mathfrak{n}^{i+1}_{i+k}.$$

Similarly, if we set N_{i+1} to be the kernel of $\beta_i : M \to M_i$, then

$$N_{i+1} = \varprojlim_{k} \mathfrak{n}^{i+1}_{i+k} M_{i+k}.$$

It follows from the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{m}_{i+k+1} \arrow[r] \arrow[d] & A \arrow[r, "\alpha_{i+k}"] \arrow[d, "="] & A_{i+k} \arrow[r] \arrow[d, "\phi^{i+k}_{i}"] & 0 \\
0 \arrow[r] & \mathfrak{m}_{i+1} \arrow[r] & A \arrow[r, "\alpha_i"] & A_i \arrow[r] & 0
\end{tikzcd}$$

that

$$\alpha_{i+k}(\mathfrak{m}_{i+1}) = \ker \phi^{i+k}_{i} = \mathfrak{n}^{i+1}_{i+k}. \tag{11.4}$$

Likewise,

$$\beta_{i+k}(N_{i+1}) = \mathfrak{n}^{i+1}_{i+k} M_{i+k}. \tag{11.5}$$

For $i \ge 1$ and $j \ge 1$,

$$\begin{aligned}
\beta_{i+j-1}(\mathfrak{m}_i N_j) &= \alpha_{i+j-1}(\mathfrak{m}_i)\beta_{i+j-1}(N_j) \\
&= \mathfrak{n}^{i}_{i+j-1}\mathfrak{n}^{j}_{i+j-1} M_{i+j-1} \\
&= \mathfrak{n}^{i+j}_{i+j-1} M_{i+j-1} \\
&= 0
\end{aligned}$$

since $\mathfrak{n}^{i+j}_{i+j-1}$ 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

$$N_i = \mathfrak{a}^i M' + N_{i+1} \tag{11.6}$$

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 (11.6) it suffices to prove

$$\beta_i(N_i) = \beta_i(\mathfrak{a}^i M') = \alpha_i(\mathfrak{a}^i)\beta_i(M') = \mathfrak{a}_i^i M'_i. \tag{11.7}$$

Since $\beta_0(N_0) = \beta_0(M) = M_0$ is equal to $M'_0 = \beta_0(M') = M_0$, we see that (11.7) 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 $\mathfrak{n}_i M_i = \ker \psi_0^i$, it follows that $M_i = M'_i + \mathfrak{n}_i M_i$. Combining these results, we have

$$\mathfrak{n}_i^i M_i = (\mathfrak{a}_i + \mathfrak{n}_i^2)^i (M'_i + \mathfrak{n}_i M_i). \tag{11.8}$$

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 (11.5), we see that (11.8) collapses to

$$\beta_i(N_i) = \mathfrak{n}_i^i M_i = \mathfrak{a}_i^i M'_i.$$

Together with (11.7), this proves (11.6).

From (11.4), $\mathfrak{m}_1 = \alpha_1^{-1}(\mathfrak{n}_1)$. Therefore, $\mathfrak{a} \subseteq \mathfrak{m}_1$, and $\mathfrak{a}^i \subseteq \mathfrak{m}_1^i \subseteq \mathfrak{m}_i$. From (11.6), this shows $N_i \subseteq m_i M' + N_{i+1}$. On the other hand, $m_i M \subseteq N_i$, from which it follows that

$$N_i = m_i M' + N_{i+1}.$$

It follows from Corollary 9.4.27 that $M' = M$. □

COROLLARY 11.5.2. *In the context of Proposition 11.5.1, 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 11.5.1. 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 (11.6) 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 9.4.27, 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 (11.6), $\mathfrak{m}_1 = \mathfrak{a} + \mathfrak{m}_1^2$, which proves Part (3). □

EXAMPLE 11.5.3. 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 9.3.10). The reader should verify that the inverse system of rings $\{R/I^n\}$ satisfies the hypotheses of Corollary 11.5.2, 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 11.5.4. *Let $\{A_i, \phi^i_j\}$ 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 $\phi^i_j : A_i \to A_j$ 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 5.8.6 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 5.8.6) and commutes with tensor products (Proposition 5.8.8). Hence the sequence $\mathfrak{m}_i \otimes_{A_i} A \to \mathfrak{m} \to 0$ is exact.

(3): By Exercise 5.8.8 and Exercise 6.5.12, 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

$$\begin{aligned}\mathfrak{m}^n/\mathfrak{m}^{n+1} &\cong (\mathfrak{m}_i^n A)\,/\,\big(\mathfrak{m}_i^{n+1}A\big)\\ &\cong \big(\mathfrak{m}_i^n/\mathfrak{m}_i^{n+1}\big)\otimes_{A_i} A\\ &\cong \big(\mathfrak{m}_i^n/\mathfrak{m}_i^{n+1}\big)\otimes_{A_i/\mathfrak{m}_i}(A_i/\mathfrak{m}_i \otimes_{A_i} A)\\ &\cong \big(\mathfrak{m}_i^n/\mathfrak{m}_i^{n+1}\big)\otimes_{A_i/\mathfrak{m}_i} A/\mathfrak{m}\end{aligned}$$

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 11.5.3 and Proposition 9.4.2, $\hat{A}$ is noetherian.

The maximal ideal of $\hat{A}$ is $\hat{\mathfrak{m}}$. By Proposition 9.4.15, 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 11.4.12 (1), the A_i-module $\hat{A}$ is idealwise separated for $\mathfrak{m}_i$. By (6) implies (1) of Theorem 11.4.13, it follows that $\hat{A}$ is flat over A_i. By Exercise 6.5.12, $\hat{A}$ is faithfully flat over A_i. By Exercise 5.8.9, $\hat{A}$ is faithfully flat over A. By Exercise 6.6.7, A is noetherian. □

CHAPTER 12

Normal Integral Domains

1. Normal Rings and Regular Rings

1.1. Normal Integral Domains.

DEFINITION 12.1.1. 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 12.1.2. *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 9.1.2, 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 6.6.12, $R[u]$ is finitely generated. By Proposition 9.1.2, u is integral over R. The converse follows from Part (1). □

EXAMPLE 12.1.3. If R is a noetherian normal integral domain, then Lemma 12.1.2 (3) implies that R is completely normal. In particular, if R is a UFD, then R is normal by Example 9.1.5. 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 12.1.4. 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 11.2.14) for each $P \in \operatorname{Spec} R$.

LEMMA 12.1.5. *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 6.6.15, 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 6.1.6, $I = 0$. By Exercise 8.2.9, $P_1 \cap \cdots \cap P_n = (0)$. 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 6.3.9, 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 2.2.8).

(3): Is left to the reader. □

LEMMA 12.1.6. *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 12.1.3, $K[x]$ 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 12.1.2 (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 9.1.7, 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 9.2.1). 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 12.1.2 (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 $u \in R[x]$. □

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 9.4.3, 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 12.1.7. *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 9.4.20, 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 12.1.2. 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 9.4.8, $\operatorname{gr}_I(R)$ is noetherian. By Lemma 12.1.2, $\lambda(c)/\lambda(b)$ 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.

THEOREM 12.1.8. *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 11.2.14, $\mathfrak{m}$ is generated by a regular system of parameters, say $\mathfrak{m} = x_1 R + \cdots + x_n R$. By Example 9.4.3, $\operatorname{gr}_{\mathfrak{m}}(R) = R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \cdots$ is a $k = R/\mathfrak{m}$-algebra which is generated by $\lambda(x_1), \dots, \lambda(x_n)$. As in the proof of Proposition 11.2.7, 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 11.1.10,

$$\sum_{d=0}^{m} \ell(S_d) = \binom{n}{n} + \cdots + \binom{m-1+n}{n} = \binom{m+n}{n},$$

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 11.1.8. At the same time, Theorem 11.2.11 says the function $\ell(A/\mathfrak{m}^{m+1})$ is a polynomial in m of degree n. This contradiction implies $I = (0)$.

Conversely, assume $\mathrm{gr}_{\mathfrak{m}}(R)$ 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 11.2.13 says R has Krull dimension n. Also, $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k(kt_1 + \cdots + kt_n) = n$. By Exercise 11.2.2, R is regular. □

COROLLARY 12.1.9. *If R is a commutative noetherian regular local ring, then R is a normal integral domain.*

PROOF. This follows from Theorem 12.1.7 and Theorem 12.1.8. □

COROLLARY 12.1.10. *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 9.3.12 and Corollary 9.4.26.

(2): This is Corollary 11.2.13 (4).

(3): Follows from Theorem 9.4.21.

(4): By Corollary 9.4.16, the associated graded rings $\mathrm{gr}_{\mathfrak{m}}(R)$ and $\mathrm{gr}_{\hat{\mathfrak{m}}}(\hat{R})$ are isomorphic as graded rings. Part (4) follows from Theorem 12.1.8. □

1.3. Exercises.

EXERCISE 12.1.1. 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.

EXERCISE 12.1.2. 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. Show:

(1) R and A have the same quotient field, namely $K = k(x)$, and A is equal to the integral closure of R in K.
(2) A is a finitely generated R-module.
(3) $R : A$, the conductor ideal (see Exercise 3.1.4) from A to R, is the maximal ideal of R generated by x^2 and x^3. (See also Exercise 9.4.5.)

2. Valuations and Valuation Rings

2.1. Valuation Rings. In this section we employ the notation R^* to designate the group of invertible elements of a ring.

LEMMA 12.2.1. *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 12.2.1, 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 $u \le v$ and $x \le y$, then $u + x \le v + y$. We say G is a *totally ordered group*, if the partial order is a chain.

EXAMPLE 12.2.2. 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 $x \neq 0$, $y \neq 0$, and $x + y \neq 0$, then $\nu(x+y) \ge \min(\nu(x), \nu(y))$.

The reader should verify that $\nu(1) = 0$.

LEMMA 12.2.3. *Suppose F is a field and $\nu : F^* \to G$ is a valuation on F. Let*

$$R = \{0\} \cup \{x \in F^* \mid \nu(x) \ge 0\}.$$

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 12.2.1). □

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 12.2.4. *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 12.2.1, $x^{-1} \in R$. 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 12.2.5. *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 12.2.6. *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 2.4.3, 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

$$1 = a_0 + a_1\alpha + \cdots + a_m\alpha^m. \tag{12.1}$$

Among all such relations, pick one such that m is minimal. Likewise, there is a relation

$$1 = b_0 + b_1\alpha^{-1} + \cdots + b_n\alpha^{-n} \tag{12.2}$$

where $b_0, \dots, b_n \in \mathfrak{m}$ and n is minimal. Without loss of generality assume $m \geq n$. Multiply (12.2) 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 (12.1), 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 4.3.7, there exists a homomorphism $R[\alpha] \to \Omega$ which extends $f : R \to \Omega$. Since (R, f) is maximal, we conclude that $R = R[\alpha]$. □

THEOREM 12.2.7. *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 1.3.3, $\mathfrak{C}$ contains a maximal member, say (A, g). By Lemma 12.2.6, 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 12.2.4 (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. □

2.2. Exercises.

EXERCISE 12.2.1. This exercise outlines a proof to the last part of Lemma 12.2.3. 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 12.2.4 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*, or DVR for short, if there exists a discrete valuation on the field of fractions of A such that A is the associated valuation ring.

LEMMA 12.2.8. *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, Axiom 1.2.1, 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 Theorem 2.3.7.

(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 11.2.1. □

THEOREM 12.2.9. *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 12.2.8.

(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 Lemma 2.3.4 (2), up to associates π is the unique irreducible element of R. Using Theorem 2.3.7, the reader should verify the following. Any $x \in K^*$ can be factored uniquely as $x = u\pi^{\nu(x)}$ for some integer $\nu(x)$ and $u \in R^*$. The function $\nu : K^* \to \mathbb{Z}$ is a discrete valuation on K. R is the valuation ring associated to ν.

(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 11.2.14.

(3) implies (4): Corollary 12.1.9.

(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 8.1.7, 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 9.1.2 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 7.4.5, 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. □

2.3.1. *Completion of a Discrete Valuation Ring.*

THEOREM 12.2.10. *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 12.1.10, $\hat{R}$ is a DVR with maximal ideal $\hat{\mathfrak{m}} = \pi\hat{R}$ and $R \to \hat{R}$ is faithfully flat. It follows from Theorem 12.2.9 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

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 12.3.1. 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.

LEMMA 12.3.2. *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 $1 \leq i < r$, $\xi_i + a_r\zeta_i \in (a_1, \dots, a_{r-1})M$. Consequently each ξ_i is in $(a_1, \dots, a_r)M$. □

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 12.3.3. *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 $k \geq 1$. 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 $f \in IM[x_1,\dots,x_n]$. □

DEFINITION 12.3.4. 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 ideal quotient defined in Exercise 2.1.20. 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 3.1.4).

THEOREM 12.3.5. *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 12.3.3, 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 12.3.2. 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 $(a_1,\dots,a_{n-1})^k M : a_n$. 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 $(a_1,\dots,a_{n-1})^k M \subseteq I^k M$. Now g is homogeneous of degree $k-1$ and by induction on k and the proof of Lemma 12.3.3, 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 $(a_1,\dots,a_{n-1})^k M$, 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 $I^k M$, 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 12.3.3, 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 12.3.1 are satisfied. Since M is separated for the I-adic topology we have $\bigcap_{k>0} I^k M = (0)$. 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 $I^2 M$. 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 $\xi \in I^k M$ 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 12.3.3 (2). Let f be a homogeneous polynomial of degree k in $M[x_2,\dots,x_n]$. Assume $f(a_2,\dots,a_n) \in a_1 M$. For some $\xi \in M$, we can write $f(a_2,\dots,a_n) = a_1\xi$. Since $\bigcap I^i M = (0)$, there exists $i \geq 0$ such that $\xi \in I^i M - I^{i+1}M$. 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 $I^k M \subseteq I^{i+2}M$. 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 $a_1 g(a_1,\dots,a_n) = f(a_2,\dots,a_n) \in I^k M$. 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 12.3.6. *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 12.3.7. *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 12.3.8. *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 8.1.2, there exists $P \in \operatorname{Assoc}_R(M)$ such that $I \subseteq P$. By Lemma 8.2.1, 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 5.3.2, $N_P \otimes_{R_P} k_P \neq (0)$. 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

$$0 \to M \xrightarrow{\ell_{a_1}} M \to M/a_1M \to 0. \tag{12.3}$$

By Proposition 10.3.9 (2) there is a long exact sequence

$$\cdots \to \operatorname{Ext}^i_R(N,M) \xrightarrow{\ell_{a_1}} \operatorname{Ext}^i_R(N,M) \to \operatorname{Ext}^i_R(N,M/a_1M) \xrightarrow{\delta^i} \operatorname{Ext}^{i+1}_R(N,M) \to \dots \tag{12.4}$$

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 (12.3) is exact. Let N be a finitely generated R-module with $\operatorname{Supp}(N) \subseteq V(I)$. In degree zero, the long exact sequence (12.4) 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 8.2.7, $\operatorname{Supp}(N) \subseteq V(I)$ 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 (12.4) 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 12.3.9. 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 12.3.8, $\operatorname{depth}_I(M)$ 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 [**14**] Grothendieck calls $\operatorname{depth}(M)$ the "profondeur de M" and writes $\operatorname{prof}(M)$. In [**3**] and [**4**] Auslander, Buchsbaum and Goldman call $\operatorname{depth}(M)$ the "codimension of M" and write $\operatorname{codim}(M)$. Our terminology and notation agrees with that used by Matsumura (see [**20**, p. 102]).

LEMMA 12.3.10. *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 12.3.8, $\operatorname{Ext}^i_R(N,M) = (0)$ 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 8.2.7 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 $P \ne \mathfrak{m}$ 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 11.2.13, $\dim(S) = n-1$. 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 5.3.2, $\operatorname{Ext}^i(R/P,M) = (0)$. □

COROLLARY 12.3.11. *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 $\operatorname{Hom}_R(R/P,M) \ne (0)$. By Lemma 12.3.10, $\operatorname{depth}(M) - \dim(R/P) \le 0$.
(2): Is left to the reader. □

LEMMA 12.3.12. *Let R be a commutative noetherian local ring,* $\mathfrak{m}$ *the maximal ideal of R, M a nonzero finitely generated R-module, and* $a_1,\dots,a_r$ *a regular sequence for M in* $\mathfrak{m}$. *Then* $\dim(M/(a_1,\dots,a_r)M) = \dim(M) - r$.

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 8.2.6, 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 12.3.5, $\operatorname{Supp}(M/a_1M) = \operatorname{Supp}(M) \cap \operatorname{Supp}(R/(a_1))$. 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 $\dim(M/(a_1,\dots,a_r)M) \le \dim(M) - r$. For the reverse inequality, $\dim(M) \ge \dim(M/a_1M) \ge \dim(M) - 1$, by Lemma 11.2.10. Iterate r times to see that $\dim(M/(a_1,\dots,a_r)M) \ge \dim(M) - r$. □

3.2. Exercises.

EXERCISE 12.3.1. Let R be a noetherian commutative ring, I a proper ideal of R, M an R module, and $a_1, \dots, a_r$ a regular sequence for M in I.

(1) There exists $n \geq r$ and elements $a_{r+1}, \dots, a_n$ such that $a_1, \dots, a_n$ is a maximal regular sequence for M.
(2) $\operatorname{depth}_I(M/(a_1, \dots, a_r)M) = \operatorname{depth}_I(M) - r$.

EXERCISE 12.3.2. 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 12.3.3. 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 12.3.4. 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 12.3.5. 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 12.3.6. 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 12.3.13. Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. By Corollary 12.3.11, 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 12.3.14. *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.
(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 12.3.11, $\operatorname{depth}(M) \leq \dim(R/P)$. Since $\operatorname{Assoc}_R(M) \subseteq \operatorname{Supp}(M)$, $\operatorname{annih}_R(M) \subseteq P$. Then $\dim(M) = \dim(R/\operatorname{annih}_R(M)) \geq \dim(R/P)$.

(2): Since $(a_1, \dots, a_r) \subseteq \mathfrak{m}$, by Corollary 5.3.2, $M/(a_1, \dots, a_r)M$ is nonzero if and only if M is nonzero. Assume M is nonzero. It follows from Lemma 12.3.12 that $\dim(M/(a_1, \dots, a_r)M) = \dim(M) - r$. Then $\operatorname{depth}(M/(a_1, \dots, a_r)M) = \operatorname{depth}(M) - r$, by Exercise 12.3.1.

(3): Assume $M_P \neq (0)$, hence $\operatorname{annih}_R(M) \subseteq P$. By Exercise 12.3.4, $\operatorname{depth}_P(M) \leq \operatorname{depth}_{\mathfrak{m}_P}(M_P)$. By Corollary 12.3.11, $\operatorname{depth}_{\mathfrak{m}_P}(M_P) \leq \dim(M_P)$. 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 8.2.2 and Lemma 8.1.2 that $P \subseteq Q$ for some $Q \in \operatorname{Assoc}_R(M)$. By Exercise 8.2.8 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 11.2.4, $\dim(M_P) = 0$.

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 12.3.12, $\dim((M/aM)_P) = \dim(M_P) - 1$. By Exercise 12.3.1, $\operatorname{depth}_P(M/aM) = \operatorname{depth}_P(M) - 1$. 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 12.3.15. *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 $1 \leq i \leq r$.
   (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 11.2.12. 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 11.2.12, $\operatorname{ht}(I) \leq i$. 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 11.2.4, 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 11.2.15,

$\dim(R/(x_1)) = n-1$. If P is an associated prime of (0), then $\dim(R/P) = n$, by Theorem 12.3.14 (1). This implies x_1 is not in P. By Proposition 8.2.2, x_1 is not a zero divisor of R. By Theorem 12.3.14 (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 11.2.4, 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 12.3.14 (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 12.3.14 (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 12.3.12, $\dim(R/I) = \dim(R) - r$.

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 12.3.14 (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 11.2.2, and Exercise 6.3.9, $\operatorname{ht}(P) = \operatorname{ht}(Q) + \operatorname{ht}(P/Q)$. □

DEFINITION 12.3.16. 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 12.3.14, a noetherian commutative ring R is Cohen-Macaulay if $R_\mathfrak{m}$ is Cohen-Macaulay for every maximal ideal $\mathfrak{m}$ of R.

THEOREM 12.3.17. *Let R be a noetherian commutative ring. The following are equivalent.*

(1) R is a Cohen-Macaulay ring.

(2) For every $r \ge 0$, if $I = (a_1,\dots,a_r)$ 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 $r \ge 0$, if $J = (a_1,\dots,a_r)$ 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 12.3.7, R_P is Cohen-Macaulay. Assume $r > 0$. By Exercise 11.2.4, there exist elements $a_1,\dots,a_r$ in P such that $\operatorname{ht}(a_1,\dots,a_i) = i$ for all $i = 1,\dots,r$. 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 $1 \le i < r$, $R/(a_1,\dots,a_i)$ has no embedded primes. Since $\operatorname{ht}(a_1,\dots,a_{i+1}) = i+1$, a_{i+1} belongs to no associated prime of $(a_1,\dots,a_i)$. So a_{i+1} is not a zero divisor of $R/(a_1,\dots,a_i)$. This shows $a_1,\dots,a_r$ is a regular sequence for R in P. We have $r \le \operatorname{depth}_P(R) \le \operatorname{depth}_{PR_P}(R_P)$, by Exercise 12.3.4. By Corollary 12.3.11, $\operatorname{depth}_{PR_P}(R_P) \le \dim R_P$, which is equal to $\operatorname{ht}(P) = r$, by Lemma 11.2.2. 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 12.3.14, the zero ideal of $R_{\mathfrak{m}}$ has no embedded primes. Let $r > 0$ and $J = (a_1, \dots, a_r)$ an ideal generated by r elements in $R_{\mathfrak{m}}$ such that $\operatorname{ht}(J) = r$. By Theorem 12.3.15, the sequence $a_1, \dots, a_r$ is a regular sequence for $R_{\mathfrak{m}}$ in $\mathfrak{m}R_{\mathfrak{m}}$. By Theorem 12.3.14, $R_{\mathfrak{m}}/J$ 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 8.2.4, $PR_{\mathfrak{m}}$ is an associated prime of $R_{\mathfrak{m}}/IR_{\mathfrak{m}}$ which is an embedded prime. □

THEOREM 12.3.18. *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 12.3.14. 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 9.5.3, going down holds for $R \to S$.

Suppose $\dim(R) = r$ and $a_1, \dots, a_r$ 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 $\ell_{a_i} : R/(a_1, \dots, a_{i-1}) \to R/(a_1, \dots, a_{i-1})$ with the flat R-algebra S_Q, ℓ_{a_i} is still one-to-one. Therefore, $a_1, \dots, a_r$ is a regular sequence for S_Q in QS_Q. This proves $r \le \operatorname{depth}(S_Q)$.

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 11.2.16 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 11.2.16, $\dim(S_Q) = \dim(R) + 1 = r + 1$. 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, $\operatorname{depth}_Q(S) \ge r + 1$. This implies S_Q is Cohen-Macaulay. □

3.4. Exercises.

EXERCISE 12.3.7. 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 12.3.8. Let R be a local PID. Then R is a Cohen-Macaulay local ring.

EXERCISE 12.3.9. 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 12.3.10. Let k be a field. As in Exercises 8.1.6, 8.2.10, and 9.4.5, 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 12.3.11. 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 12.3.19. *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 12.1.8, $k[t_1, \dots, t_r] \cong \operatorname{gr}_{\mathfrak{m}}(R)$. The sequence $x_1, \dots, x_r$ is a quasi-regular sequence for R in $\mathfrak{m}$. By Corollary 12.3.6, $x_1, \dots, x_r$ is a regular sequence for R in $\mathfrak{m}$.

(2): By Part (1), $\operatorname{depth}(R) \geq r = \dim(R)$.

(3): By Proposition 11.2.15, $\dim(R/P_i) = r - i$. Since $\mathfrak{m}/P_i$ is generated by $x_{i+1}, \dots, x_r$, R/P_i is a regular local ring. By Corollary 12.1.9, 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 11.2.2, $r = \dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ 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 12.3.15, $\operatorname{ht}(P) = \dim(R) - \dim(R/P) = i$. 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 10.4.10 applied recursively to $k = R/(x_1, \dots, x_d)$, $\operatorname{proj.dim}_R(k) = \operatorname{proj.dim}(R) + d = d$. By Theorem 10.4.15, $\operatorname{coh.dim}(R) = d$. □

THEOREM 12.3.20. *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 12.3.18, 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 11.2.16 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 11.2.16, $\dim(S_Q) = \dim(R) + 1 = r + 1$. Hence S_Q is regular in this case as well. □

COROLLARY 12.3.21. *(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 11.3.1, $R = k[x_1, \dots, x_n]$ has dimension n. Let $\mathfrak{m}$ be a maximal ideal of R. By Theorem 12.3.20, $R_{\mathfrak{m}}$ is a regular local ring of dimension n. By Theorem 12.3.19, $\operatorname{coh.dim}(R_P) = n$. By Lemma 10.4.14 (2), $\operatorname{coh.dim}(R) = n$. □

LEMMA 12.3.22. *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 7.1.3), $\mathfrak{m} = 0$. 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 8.2.2,

$$\mathfrak{m} - \mathfrak{m}^2 \subseteq P_1 \cup \cdots \cup P_n.$$

Since $\mathfrak{m}$ is not a subset of $\mathfrak{m}^2$, it follows from Lemma 8.1.2 that $\mathfrak{m} \subseteq P_i$ for some i. Since $\mathfrak{m}$ is maximal, $\mathfrak{m}$ is equal to P_i. □

LEMMA 12.3.23. *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 12.3.24. *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 10.3.3, 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 5.7.2) 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 12.3.25. *(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 12.3.19. 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 12.3.22, $\mathfrak{m}$ is an associated prime of R. By Lemma 8.2.1, 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 6.4.2, $\mathfrak{m}$ is not a projective R-module. By Definition 10.4.13, $\operatorname{coh.dim}(R) \ge \operatorname{proj.dim}_R(\mathfrak{m}) \ge 1$. By Theorem 10.4.15, $\operatorname{proj.dim}_R(k) = \operatorname{coh.dim}(R) \ge 1$. By Proposition 10.4.10, $\operatorname{Tor}_{n+1}^R(R/xR, k) = 0$. 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 $\operatorname{Tor}_i^R(R,k) = 0$ for $i \ge 1$, the associated long exact sequence of Lemma 10.3.2 (3) implies the boundary map $\partial : \operatorname{Tor}_{n+1}^R(R/xR, k) \to \operatorname{Tor}_n^R(k,k)$ is an isomorphism. This implies $\operatorname{Tor}_n^R(k,k) = 0$, which is a contradiction to Theorem 10.4.15.

Step 2: The proof is by induction on $d = \dim(R)$. If $d = 0$, then R is regular, by Definition 11.2.14. 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 11.2.13 (3), $\dim(R/aR) = d-1$. By (1), $\operatorname{proj.dim}_R(\mathfrak{m}) \leq \operatorname{coh.dim}(R)$ is finite. By Lemma 12.3.24, $\mathfrak{m}/a\mathfrak{m}$ is an R/aR-module of finite projective dimension. By Lemma 12.3.23, $\mathfrak{m}/aR$ is an R/aR-module direct summand of $\mathfrak{m}/a\mathfrak{m}$. By Exercise 10.4.9, $\mathfrak{m}/aR$ is an R/aR-module of finite projective dimension. By the induction hypothesis, R/aR is a regular local ring. By Exercise 12.3.12, R is regular. □

COROLLARY 12.3.26. *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. □

PROPOSITION 12.3.27. *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 12.3.19 (5)). Therefore, $\operatorname{proj.dim}_R(M) \leq n$ (Definition 10.4.13) and $\operatorname{proj.dim}_R(k) = n$ (Theorem 10.4.15). The proof is by induction on $d = \operatorname{depth}(M)$. First assume $d = 0$. By Exercise 12.3.2, 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 10.3.2). By Proposition 10.4.10 (2), $\operatorname{Tor}^R_{n+1}(M/N,k) = 0$ and by Theorem 10.4.15, $\operatorname{Tor}^R_n(N,k) \neq 0$. Since $\operatorname{Tor}^R_n(M,k) \neq 0$, Proposition 10.4.10 (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 12.3.1) and $\operatorname{proj.dim}(M/xM) = \operatorname{proj.dim}(M) + 1$ (Proposition 10.4.10 (3)). By induction, we are done. □

3.6. Exercises.

EXERCISE 12.3.12. Let R be a commutative noetherian local ring with maximal ideal $\mathfrak{m}$ and let a be an R-regular element in $\mathfrak{m}$. If R/aR is regular, then R is regular and $a \notin \mathfrak{m}^2$.

EXERCISE 12.3.13. Let S be a commutative faithfully flat R-algebra. If R and S are both noetherian, and S is regular, then R is regular.

4. Noetherian Normal Integral Domains

4.1. A Noetherian Normal Integral Domain is a Krull Domain. Let R denote a noetherian integral domain and K the field of fractions. 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 12.4.1. *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 8.2.1, 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 $y \notin xR$. □

LEMMA 12.4.2. *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 6.6.6, R is not artinian. By Proposition 7.4.5, $\mathfrak{m} \neq \mathfrak{m}^2$. 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 11.2.13, $\dim R = 1$. By Theorem 12.2.9, R is a DVR. □

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 12.2.9, 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 12.2.9.

THEOREM 12.4.3. *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 $\dim(R) \leq 2$, then R is Cohen-Macaulay.

PROOF. (1): Let $P \in \operatorname{Assoc}_R(R/xR)$. By Lemma 11.2.2, it suffices to prove $\dim(R_P) = 1$. By this observation and Lemma 8.2.4, 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 12.4.1 we have $R \subsetneq P^{-1}$. For contradiction's sake, assume $\operatorname{ht}(P) > 1$. Lemma 12.4.2 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 9.1.2, 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 12.2.9, R_P is a DVR and every proper ideal is equal to $P^m R_P$, for some $m > 0$. By Exercise 8.1.3, there is a unique ν such that $I = P^\nu R_P \cap R$, which is equal to $P^{(\nu)}$, by Exercise 8.3.1.

(3): This follows from Part (1), and Theorem 12.3.17. □

In the terminology of [**12**], Corollary 12.4.4 says that R is a *Krull domain*.

COROLLARY 12.4.4. *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 $\nu_P(\alpha) \geq 0$ 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 12.4.3, the reduced primary decomposition of $R\alpha$ is

$$\alpha R = P_1^{(n_1)} \cap \cdots \cap P_s^{(n_s)}$$

where $s \geq 0$, $P_1,\dots,P_s$ are height one primes of R, $n_i \geq 1$, 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 6.1.1,

$$\alpha R_P = \begin{cases} \mathfrak{m}_{P_i}^{n_i} & \text{if } P \in \{P_1,\dots,P_s\} \\ R_P & \text{if } P \notin \{P_1,\dots,P_s\}. \end{cases}$$

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.

THEOREM 12.4.5. *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 12.2.9 says R_P is a regular local ring. Suppose $\operatorname{ht}(P) \geq 2$. By Exercise 11.2.4, 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 12.4.3 (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 12.3.3, P is not an associated prime of R. That is, $\operatorname{Assoc}(R)$ contains no embedded primes. By Exercise 12.4.2 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 6.1.6, R_{P_i} is the quotient field of R/P_i. Since $\operatorname{Assoc}(R) = \{P_1,\dots,P_n\}$, by Proposition 8.2.2, 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 6.3.11,

$\operatorname{Rad}_{RW^{-1}}(0) = (0)$. By Proposition 7.4.3 and Theorem 7.2.3, RW^{-1} is semisimple. By Theorem 7.3.3 (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

$$(rw^{-1})^u + a_{u-1}(rw^{-1})^{u-1} + \cdots + a_1(rw^{-1}) + a_0 = 0 \tag{12.5}$$

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 11.2.12, $\operatorname{ht}(Q) \geq 1$. If $\operatorname{ht}(Q) \geq 2$, then by (S_2), $\operatorname{depth}(R_Q) \geq 2$. By Exercise 12.3.1, $\operatorname{depth}(R_Q/wR_Q) \geq 1$ and by Exercise 12.3.3, 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 (12.5), 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 8.1.3, $I = Q^{\nu}R_Q \cap R = Q^{(\nu)}$, 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 12.1.5, R is a normal ring. □

COROLLARY 12.4.6. *If R is a Cohen-Macaulay ring, then R is normal if and only if R_P is regular for all P such that* $\operatorname{ht}(P) \leq 1$.

PROOF. For every prime ideal P in R, $\operatorname{depth}(R_P) = \dim(R_P) = \operatorname{ht}(P)$, so condition (S_2) of Theorem 12.4.5 is satisfied. Therefore, R is normal if and only condition (R_1) is satisfied. □

4.2.1. *Local Complete Intersection Criteria.*

PROPOSITION 12.4.7. *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* $\operatorname{ht}(P) \leq 1$.

PROOF. (1): Since R_M is Cohen-Macaulay and $\operatorname{ht}(a_1R_M + \cdots + a_rR_M) = r$, by Theorem 12.3.15, $a_1, \dots, a_r$ is a regular sequence for R_M in MR_M. By Theorem 12.3.14, $R_M/IR_M = (R/I)_{M/I}$ is Cohen-Macaulay. By Definition 12.3.16, R/I is Cohen-Macaulay.

(2): Follows by Corollary 12.4.6 and Part (1). □

4.3. The Approximation Theorem.

LEMMA 12.4.8. *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 8.1.2, 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 $\nu_{\mathfrak{p}}(t) = 1$. □

THEOREM 12.4.9. *(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*

$$\nu_{\mathfrak{p}}(\alpha) = \begin{cases} n_i & \textit{if } \mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \\ \geq 0 & \textit{otherwise.} \end{cases}$$

PROOF. Using Lemma 12.4.8, 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 12.4.8, pick $u_1, \dots, u_s$ in R such that

$$\nu_{\mathfrak{p}}(u_j) = \begin{cases} 1 & \text{if } \mathfrak{p} = \mathfrak{q}_j, \\ 0 & \text{if } \mathfrak{p} = q_i, \text{ for some } i \neq j, \\ 0 & \text{if } \mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}. \end{cases}$$

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. □

4.4. Divisor Classes of Integral Domains.

DEFINITION 12.4.10. 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 12.4.4, there is a homomorphism of groups $\operatorname{Div} : K^* \to \operatorname{Div}(R)$ defined by

$$\operatorname{Div}(\alpha) = \sum_{P \in X_1(R)} v_P(\alpha)P,$$

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 12.4.11. *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 12.4.3, it suffices to show that the principal ideal (p) is a prime ideal. Let P be a minimal prime over-ideal of (p). By Corollary 11.2.12 (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 2.5.1. □

COROLLARY 12.4.12. *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 12.4.13. *(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* $\operatorname{Div}(f) = v_1P_1 + \cdots + v_nP_n$. *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 5.7.2), $\operatorname{coker}\delta \cong \ker\alpha$. Hence

$$1 \to R^* \to R[f^{-1}]^* \to \ker\alpha \to 0 \tag{12.6}$$

is exact. Using Exercise 6.3.9, $X_1(R[f^{-1}])$ 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 5.7.2),

$$0 \to \ker\alpha \to \ker\beta \to \ker\gamma \to 0 \tag{12.7}$$

is exact. Combine (12.6) and (12.7) to complete the proof. □

EXAMPLE 12.4.14. 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 12.4.4. 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 [**15**, pp. 28–29] for more details. Start with the equation

$$z^3 - y(y-x)(x+1)) = 0 \tag{12.8}$$

in K. Divide both sides of (12.8) by x^3 and substitute $v = y/x$ and $w = z/x$ to get

$$w^3 - v(v-1)(1+x^{-1}) = 0. \tag{12.9}$$

Solve (12.9) for x to get

$$x = \frac{v^2 - v}{w^3 - v^2 + v}. \tag{12.10}$$

Now treat v, w as indeterminates and define

$$R = \frac{k[x,y,z]}{(z^3 - y(y-x)(x+1))} \xrightarrow{\phi} k[v,w][(w^3 - v^2 + v)^{-1}] \tag{12.11}$$

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 (12.11), then

$$R[x^{-1}, y^{-1}, (y-x)^{-1}] \xrightarrow{\phi} k[v,w][v^{-1}, (v-1)^{-1}, (w^3 - v^2 + v)^{-1}] \tag{12.12}$$

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 11.3.4). Since $k[v,w]$ is a unique factorization domain, it follows from Theorem 12.4.13 that the group of units in the ring on the right hand side of (12.12) decomposes into the internal direct product

$$k^* \times \langle v\rangle \times \langle v-1\rangle \times \langle w^3 - v^2 + v\rangle. \tag{12.13}$$

Using the isomorphism (12.12) 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

$$\begin{aligned} \mathfrak{p}_0 &= (x) \\ \mathfrak{p}_1 &= (y,z) \\ \mathfrak{p}_2 &= (y-x,z) \end{aligned} \tag{12.14}$$

are each height one prime ideals of R. Using the identity (12.8) 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:

$$\begin{aligned} \operatorname{Div}(x) &= \mathfrak{p}_0 \\ \operatorname{Div}(y) &= 3\mathfrak{p}_1 \\ \operatorname{Div}(y-x) &= 3\mathfrak{p}_2. \end{aligned} \tag{12.15}$$

Since $R[x^{-1}, y^{-1}, (y-x)^{-1}]$ is factorial, the exact sequence of Nagata (Theorem 12.4.13) is

$$1 \to R^* \to R[(xy(y-x))^{-1}]^* \xrightarrow{\text{Div}} \bigoplus_{i=0}^{2} \mathbb{Z}\mathfrak{p}_i \to \operatorname{Cl}(R) \to 0. \tag{12.16}$$

From (12.16) and (12.15), 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 (12.13) and (12.16) it follows that $R^* = k^*$.

4.5. Exercises.

EXERCISE 12.4.1. 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 12.4.2. Let R be a noetherian commutative ring. The following are equivalent.

(1) $\operatorname{Assoc}_R(R)$ contains no embedded primes and for each $P \in \operatorname{Assoc}_R(R)$, R_P is a field.
(2) $\operatorname{Rad}_R(0) = (0)$.

EXERCISE 12.4.3. Let R be a noetherian integral domain. Then R is a UFD if and only if for every irreducible element p, the principal ideal (p) is a prime ideal. (Hint: Mimic the proof of Theorem 2.3.7.)

EXERCISE 12.4.4. 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 12.4.5 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 12.4.5. Let $S = \mathbb{R}[x,y]/(f)$, where $f = x^2 + y^2 - 1$. By Exercise 5.3.3, S is not a UFD. This exercise is an outline of a proof that $\operatorname{Cl}(S)$, 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 $\operatorname{Div}(x) = P_1 + P_2$ and $\operatorname{Div}(y-1) = 2P_1$.
(5) Use Theorem 12.4.13 to prove that that $\operatorname{Cl}(S)$ is generated by P_1 and has order two.

EXERCISE 12.4.6. Let R be a noetherian normal integral domain with field of fractions K. Let $W \subseteq R^*$ be a multiplicative set. Modify the proof of Theorem 12.4.13 to show that there is an epimorphism of groups $\gamma : \operatorname{Cl}(R) \to \operatorname{Cl}(W^{-1}R)$ 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 12.4.7. This exercise is a continuation of Exercise 12.4.4. 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 12.4.4 to show that $\hat{R}$ is a noetherian normal integral domain and $\operatorname{Cl}(\hat{R})$ 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 [**9**, A5] and [**18**] that p is a rational double point of type A_{n-1}.

EXERCISE 12.4.8. 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 12.4.14 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) $\operatorname{Div}(x) = \mathfrak{q}_1 + \mathfrak{q}_2$, $\operatorname{Div}(y-x) = 2\mathfrak{p}_1$, $\operatorname{Div}(y+x) = 2\mathfrak{p}_2$.
(5) $\operatorname{Cl}(R) \cong \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

EXERCISE 12.4.9. 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 $1 \le i \le n$, 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 12.4.14 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 12.4.8. The ring R was the focus of the article [**11**] where many other interesting properties of R were studied.

EXERCISE 12.4.10. 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 12.4.14 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 12.4.14.

CHAPTER 13

Divisor Class Groups

1. Lattices

Let R be an integral domain with field of fractions K. If M is a finitely generated torsion free R-module, the natural mapping $R \otimes_R M \to K \otimes_R M$ is one-to-one (Lemma 6.1.1). In this case we can identify M with the R-submodule $1 \otimes M$ of $K \otimes_R M$. Sometimes we write KM instead of $K \otimes_R M$. The *rank* of M is defined to be $\dim_K KM$.

1.1. Definition and First Properties.

PROPOSITION 13.1.1. *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-module 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 3.1.28). 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 13.1.2. 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 13.1.1 is said to be an *R-lattice in V*.

EXAMPLE 13.1.3. 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 6.6.8 and 8.2.15). By Proposition 6.5.7, $\operatorname{Hom}_R(M,N)$ 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 13.1.6 (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 9.1.10, S is an R-lattice in L.

PROPOSITION 13.1.4. *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.

PROOF. (1): Apply Proposition 13.1.1 and Corollary 6.6.12.

(2): Apply (1) and Proposition 3.2.5. □

PROPOSITION 13.1.5. *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 13.1.1 (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 13.1.1 (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. □

PROPOSITION 13.1.6. *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. *(1) If $M_0 \subseteq M_1$, and $N_0 \subseteq N_1$, then $N_0 : M_1 \subseteq N_1 : M_0$.*
2. *(2) The restriction mapping $\rho : (N : M) \to \operatorname{Hom}_R(M,N)$ is an isomorphism of R-modules.*
3. *(3) $N : M$ is an R-lattice in $\operatorname{Hom}_K(V,W)$.*
4. *(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 13.1.1 (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 5.5.13, 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, $zf \in N : M$. □

1.2. Reflexive Lattices. In the context of Proposition 13.1.6, we identify $R : M$ with the dual module $M^* = \operatorname{Hom}_R(M,R)$. By Exercise 5.5.7 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

$$\begin{tikzcd}
M \arrow[r] \arrow[d] & M^{**} = R : (R : M) \arrow[d] \\
V \arrow[r] & V^{**}
\end{tikzcd} \tag{13.1}$$

commutes and the bottom horizontal arrow is an isomorphism (Theorem 3.3.22). 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 5.5.8). If M is an R-lattice, then Lemma 13.1.7 shows that $R : M$, the dual of M, is reflexive.

LEMMA 13.1.7. *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 13.1.6 (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 (13.1). □

PROPOSITION 13.1.8. *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 13.1.1). 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

$$R : (R : M) = \bigcap_{\alpha \in (R:M)} \left(\alpha^{-1}(R) \cap F\right). \tag{13.2}$$

Let $v \in V$ and assume v is in the right hand side of (13.2). 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 13.1.1 (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 5.5.8) 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 (13.2), the left hand side is a subset of the right hand side. □

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 5.5.11 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 5.5.10) which is defined by $\phi(\theta)(u) = \theta(u \otimes \cdot)$.

LEMMA 13.1.9. *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 $\alpha((N : M)L) \subseteq N : (M : L)$.

(2) Let LM denote the image of $L \otimes_R M \to U \otimes_K V$. Then $\phi(N : LM) \subseteq (N : M) : L$, and $\phi^{-1}((N : M) : L) \subseteq N : LM$.

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 $\theta \in N : LM$. □

PROPOSITION 13.1.10. *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 13.1.9 (2),

$$\phi(R:(R:M)N) \subseteq (R:(R:M)):N = M:N$$

where the last equality is because M is reflexive. By Lemma 13.1.9 (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 13.1.11. *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 13.1.1, 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 12.4.4, this proves (1).

(2): For each $\mathfrak{p} \in X_1(R)$, $R_{\mathfrak{p}}$ is a discrete valuation ring. By Proposition 13.1.4, $N(\mathfrak{p})$ 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 $r \in R-(0)$, $ru_k \in \sum_{i=1}^n Rv_{j,i} \subseteq N(\mathfrak{q}_j)$ 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 12.4.4 (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 13.1.1, 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 13.1.12, $N(\mathfrak{p}_j)_{\mathfrak{p}} = KN(\mathfrak{p}_j) = V$, for $1 \leq j \leq w$. 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 $1 \leq j \leq w$.

(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 13.1.12. *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) $(R_{\mathfrak{p}})_{\mathfrak{q}} = K$.
(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 13.1.13. *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) $R : M = \bigcap_{\mathfrak{p} \in X_1(R)} R_{\mathfrak{p}} : M_{\mathfrak{p}}$.
(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 5.5.13). By Proposition 13.1.6 (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 13.1.11 (2) and Part (1). □

THEOREM 13.1.14. *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) $R:(R:M)=\tilde{M}$.
(2) *M is a reflexive R-lattice if and only if $M=\tilde{M}$.*
(3) *For each $\mathfrak{p}\in X_1(R)$, $\tilde{M}_{\mathfrak{p}}=M_{\mathfrak{p}}$.*
(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 13.1.13,

$$\begin{aligned} R:(R:M) &= \bigcap_{\mathfrak{p}\in X_1(R)} R_{\mathfrak{p}}:(R:M)_{\mathfrak{p}} \\ &= \bigcap_{\mathfrak{p}\in X_1(R)} R_{\mathfrak{p}}:(R_{\mathfrak{p}}:M_{\mathfrak{p}}) \\ &= \bigcap_{\mathfrak{p}\in X_1(R)} M_{\mathfrak{p}} \\ &= \tilde{M}. \end{aligned}$$

The rest is left to the reader. □

COROLLARY 13.1.15. *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

$$M\subseteq R:(R:M)=\bigcap_{\mathfrak{p}\in X_1(R)} M_{\mathfrak{p}}\subseteq \bigcap_{\mathfrak{p}\in X_1(R)} N_{\mathfrak{p}}=R:(R:N)=N.$$

□

PROPOSITION 13.1.16. *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 5.5.11 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 13.1.4). By Proposition 6.5.7 and Lemma 5.5.11,

$$N^*\otimes_R M\otimes_R R_{\mathfrak{p}}\xrightarrow{\alpha\otimes 1}\operatorname{Hom}_R(M,N)^*\otimes_R R_{\mathfrak{p}}$$

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 13.1.14, $\operatorname{Hom}_R(M,N)^{**}$ 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 13.1.15, we see that α^* is an isomorphism.

The second and third isomorphisms follow from the first and the Adjoint Isomorphisms (Theorem 5.5.10).

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 13.1.17 provides a globalization method for constructing reflexive lattices from locally defined projective lattices. A version of Theorem 13.1.17 for sheaves of modules on a ringed space was proved by B. Auslander in [**2**, Theorem VI.5]. A partial converse is [**2**, 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.

Before stating Theorem 13.1.17 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 $U(f_i) = \operatorname{Spec} R_i = \{\mathfrak{p} \in \operatorname{Spec} R \mid f_i \not\in \mathfrak{p}\}$. 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 13.1.17. *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 11.2.12, a minimal prime of f_0 has height one. By Corollary 6.6.15, 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 13.1.11 (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 13.1.11 (2).

(2): Follows from Theorem 13.1.14 (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 13.1.3 and Corollary 13.1.15, $N \otimes_R R_i = M_i$.

(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 13.1.1. 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 $KS = K\bar{S}$. If S is finitely generated, prove that $\operatorname{Rank} S = \operatorname{Rank} \bar{S}$.

EXERCISE 13.1.2. 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 13.1.3. 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. The Class Group of Rank One Projective Modules

Let R be an integral domain with field of fractions K. Viewing K as a vector space over itself, a *fractional ideal* of R is an R-lattice F in K.

LEMMA 13.2.1. *In the above context, if F is a nonzero R-submodule of K, then the following are equivalent.*

(1) F is a fractional ideal of R in 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 follows from Proposition 13.1.1. □

If E and F are fractional ideals, the product EF is defined to be the R-submodule of K generated by all products of the form xy, where $x \in E$ and $y \in F$. By Proposition 13.1.5, $E+F$, $E \cap F$ and EF are fractional ideals. If F is a fractional ideal, let

$$F^{-1} = R : F = \{x \in K \mid xF \subseteq R\}.$$

where we identify $K = \operatorname{Hom}_K(K,K)$. By Proposition 13.1.6, F^{-1} is a fractional ideal of R. The reader should verify that $F^{-1}F \subseteq R$ and $F^{-1}F$ is an ideal of R. A fractional ideal F is called an *invertible ideal* of R in case $F^{-1}F = R$. An ideal I of R is a fractional ideal.

LEMMA 13.2.2. *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 nonzero R-submodule of K which is finitely generated as an R-module, then F is a fractional ideal of R.
(3) 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 $af(b) = bf(a)$.
(4) 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 $F^{-1} \to F^* = \operatorname{Hom}_R(F,R)$.

PROOF. (3): 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 $af(b) = saf(b)s^{-1} = f(abs)s^{-1} = f(abu)u^{-1} = buf(a)u^{-1} = bf(a)$.

The proofs of (1), (2), and (4) are left to the reader. □

THEOREM 13.2.3. *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 an invertible R-module (that is, F is a rank one R-progenerator).

PROOF. (3) implies (1): Is trivial.

(1) implies (2): Let $\{(x_\alpha, f_\alpha) \mid \alpha \in S\}$ be a dual basis for F. Fix any $x_0 \in F-(0)$ and define $y_\alpha = f_\alpha(x_0)$. For each $\alpha \in S$, y_α is an element of R. For any $x \in F$, by Lemma 13.2.2 (3) we have

$$xy_\alpha = xf_\alpha(x_0) = x_0 f_\alpha(x).$$

From this it follows that $x(y_\alpha x_0^{-1}) = f_\alpha(x)$, which is an element of R. This implies $y_\alpha x_0^{-1}$ is in F^{-1}. Assume $x \in F-(0)$. Combining these results with the definition of dual basis,

$$\begin{aligned} x &= \sum_{\alpha\in S} f_\alpha(x)x_\alpha \\ x &= \sum_{\alpha\in S} x(y_\alpha x_0^{-1})x_\alpha \\ x &= x\sum_{\alpha\in S} (y_\alpha x_0^{-1})x_\alpha. \end{aligned}$$

This equation holds in the field K, so we cancel x to get $1 = \sum_{\alpha\in S}(y_\alpha x_0^{-1})x_\alpha$. Since the right-hand side is in $F^{-1}F$, F is invertible.

(2) implies (3): Because R is an integral domain, F is a faithful R-module and the left regular representation $\lambda : R \to \operatorname{Hom}_R(F,F)$ is one-to-one. As in Lemma 5.9.1, $\theta_R : F^* \otimes_R F \to \operatorname{Hom}_R(F,F)$ is defined by $f \otimes m \mapsto f(\cdot)m$. By Lemma 13.2.2 (3), it follows that the diagram

$$\begin{tikzcd} F^* \otimes_R F \arrow[rr, "\theta_R"] \arrow[dr, "\mu"'] & & \operatorname{Hom}_R(F,F) \\ & R \arrow[ur, "\lambda"'] & \end{tikzcd}$$

commutes, where μ is the multiplication map $f \otimes m \mapsto f(m)$. By Lemma 13.2.2 (4), the image of μ is $F^{-1}F = R$, so μ is onto. Then $1 : F \to F$ is in the image of θ_R. By Lemma 5.9.1, θ_R is an isomorphism and F is an R-progenerator. The rank of F is one, by Lemma 6.7.5. □

LEMMA 13.2.4. *Let R be an integral domain with field of fractions K.*

(1) If $F_1,\dots,F_n$ are fractional ideals of R, then $F = F_1F_2\cdots F_n$ 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 $P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s$, 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 8.1.1, 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. □

LEMMA 13.2.5. *Let R be an integral domain with field of fractions K. Let M be a 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 $\alpha \in K$ 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 finitely generated R-submodule of K. By Lemma 13.2.2 (2) we are done.

(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 6.6.12 that F is finitely generated. By Lemma 13.2.2 (2), F is a fractional ideal of R in K. 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 9.1.2 implies that α is integral over R. But R is integrally closed, so $\alpha \in R$. □

2.1. Exercises.

EXERCISE 13.2.1. 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 13.2.2. 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 13.2.3. 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 13.2.4. 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 $I \in \text{Invert}(R)$ is an invertible R-module, hence I represents a class in the Picard group of R. Show that this assignment defines a homomorphism $\theta : \text{Invert}(R) \to \text{Pic}(R)$.

(3) Show that θ induces an isomorphism $\text{Invert}(R)/\text{Prin}(R) \cong \text{Pic}(R)$. The group $\text{Invert}(R)/\text{Prin}(R)$ is called the class group of rank one projective R-modules.

EXERCISE 13.2.5. Let k be a field, $A = k[x]$ and $R = k[x^2, x^3]$. From Exercise 12.1.2, 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) $\text{Pic}\, R$ contains a subgroup isomorphic to the additive group k.

(4) $\text{Pic}\, R$ is generated by the classes of the modules P_α, which implies $\text{Pic}\, R \cong k$. (See [**15**, 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. 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. There is an exact sequence

$$1 \to R^* \to A^* \times (R/\mathfrak{m})^* \to (A/\mathfrak{m})^* \xrightarrow{\partial} \text{Pic}\, R \to \text{Pic}\, A \times \text{Pic}(R/\mathfrak{m}) \to \text{Pic}(A/\mathfrak{m}).$$

of abelian groups from which $\text{Pic}\, R$ can be computed.

EXERCISE 13.2.6. Let k be a field, $A = k[x,y]$, and $R = k[x^2, xy, y^2, x^3, x^2y, xy^2, y^3]$. Let $\mathfrak{m} = (x^2, xy, y^2, x^3, x^2y, xy^2, y^3)$, which is a maximal ideal in R. We know from Exercises 12.3.10 and 9.4.5 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) $\text{Pic}\, R$ contains a subgroup isomorphic to the additive group k^2.

(4) $\text{Pic}\, R$ is generated by the classes of the modules $P_{\alpha,\beta}$, which implies $\text{Pic}\, R \cong k^2$. As in Exercise 13.2.5 (4), apply the Mayer-Vietoris sequence of Milnor. Use Corollary 12.4.12 and Exercise 13.4.10 to show that ∂ is onto. Now show the image of ∂ contains each class of the form $P_{\alpha,\beta}$.

EXERCISE 13.2.7. 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 13.2.5 (4), apply the Mayer-Vietoris sequence of Milnor to show that $R^* = k^*$ and $\operatorname{Pic} R = \langle 0 \rangle$.

EXERCISE 13.2.8. 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

PROPOSITION 13.3.1. *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 8.3.8, 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 6.3.4, the ideals I_i are pairwise comaximal. By Exercise 2.2.6, $I = I_1 I_2 \cdots I_n$.

(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 8.3.5, the primary ideals I_i are uniquely determined by I. □

THEOREM 13.3.2. *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 13.2.3, 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 13.2.3, 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 13.3.2 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 Proposition 13.3.1, $I = I_1 \cdots I_n$ 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 12.4.3, I_i is equal to the symbolic power $P_i^{(v_i)}$, for some unique $v_i > 0$. By Proposition 8.1.5 (3), $P_i^{v_i}$ is a P_i-primary ideal. By Exercise 8.3.1, it follows that $I_i = P_i^{v_i}$.

(4) implies (5): If F is a fractional ideal, then $F^{-1}F$ is invertible. By Lemma 13.2.4, F is invertible.

(4) implies (2): Let I be a nonzero ideal of R. By Theorem 13.2.3, I is a rank one projective R-module. Then I is finitely generated and by Corollary 6.6.7, 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 6.4.2, $\mathfrak{m}$ is a free R_P-module of rank one. In other words, $\mathfrak{m}$ is a principal ideal and Corollary 11.2.13 says $\dim R = 1$. Theorem 12.2.9 implies R_P is a DVR.

(3) implies (4): By Lemma 13.2.4, 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 $P_1, \dots, P_m, Q_1, \dots, Q_n$. 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 13.2.2 (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 13.2.4 (1), for all i and j, the ideals $\eta(P_i)$ and $\eta(Q_j)$ are invertible prime ideals in R/P. Apply Lemma 13.2.4 (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 $i = 1, \dots, m$. By Proposition 2.1.20, $P_i = Q_{2i-1} = Q_{2i}$ for $i = 1, \dots, m$, 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 $P_1, \dots, P_m$. Then $P_1 \cdots P_m \subseteq P$. By Lemma 13.2.2 (1), Rx is invertible. By Lemma 13.2.4, each P_i in the product is invertible. By Definition 8.1.1, 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). □

THEOREM 13.3.3. *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. Factor I and J into powers of prime ideals. After inserting zero exponents if necessary, we can assume $I = \prod P_i^{e_i}$ and $J = \prod P_i^{f_i}$ where all of the exponents are nonnegative and the primes $P_1, \dots, P_n$ are distinct. Let $Q_i = P_i^{e_i+1}$. Then $Q_1, \dots, Q_n$ are pairwise relatively prime. By the Chinese Remainder Theorem 2.2.8, the natural map $R \to R/Q_1 \oplus \cdots \oplus R/Q_n$ is onto. For each i, pick $\alpha_i \in P^{e_i} - Q_i$. There exists $\alpha \in R$ such that $\alpha - \alpha_i \in Q_i$ for each i. Hence $\alpha \in P^{e_i} - Q_i$ for each i, so $\alpha \in I = \prod P_i^{e_i}$. If $R\alpha = P_1^{r_1} \cdots P_n^{r_n} P_{n+1}^{r_{n+1}} \cdots P_m^{r_m}$ is the factorization of $R\alpha$ into primes, then by Exercise 13.3.5, we have $r_i = e_i$ for $i = 1, \dots, n$. It follows from Exercise 13.3.7 that $R\alpha + IJ = I$. It follows from Exercise 13.3.6 that there exists and ideal C in R such that $R\alpha = IC$. Multiplying $IC + IJ = I$ by I^{-1} yields $C + J = R$. □

COROLLARY 13.3.4. *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. Apply Theorem 13.3.3 to the ideals $R\alpha$ and I. There exist β and C such that $R\alpha + C = R$ and $IC = R\beta$. The reader should verify that $I = R\alpha + R\beta$. □

If I is an ideal in a Dedekind domain R, by Corollary 13.3.4, $I = R\alpha + R\beta$, where $\alpha \in I$ is arbitrary. For this reason, a Dedekind domain is said to have the "one and a half generator property for ideals".

THEOREM 13.3.5. *Let R be a Dedekind domain and M a finitely generated torsion free R-module of rank n. There exist fractional ideals $F_1, \dots, F_n$ of R such that $M \cong F_1 \oplus \cdots \oplus F_n$.*

PROOF. Recall that $\operatorname{Rank} M = \dim_K KM$. 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 13.1.1, $M/\bar{S}$ is torsion free and $\operatorname{Rank} \bar{S} = \operatorname{Rank} S = 1$. By Lemma 13.2.5, there exists a fractional ideal F_1 of R such that $\bar{S} \cong F_1$. Since $\operatorname{Rank}(M/\bar{S}) = n - 1$, 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 13.3.2, each F_i is projective. Therefore the sequence $0 \to \bar{S} \to M \to M/\bar{S} \to 0$ is split exact. □

3.1. Exercises.

EXERCISE 13.3.1. Let R be a Dedekind domain and $\operatorname{Frac}(R)$ the group of fractional ideals of R.

(1) $\operatorname{Frac}(R)$ is a free abelian group on the set $\operatorname{Max}(R)$, where the binary operation is multiplication.
(2) There is an isomorphism $\operatorname{Frac}(R) \cong \operatorname{Div}(R)$ which maps a maximal ideal P to the corresponding generator of $\operatorname{Div}(R)$.

EXERCISE 13.3.2. Let R be a Dedekind domain and $\operatorname{Frac}(R)$ the group of fractional ideals of R. Let $\operatorname{Prin}(R) = \{R\alpha \mid \alpha \in K^*\}$ denote the subset of $\operatorname{Frac}(R)$ consisting of all principal fractional ideals.

(1) $\operatorname{Prin}(R)$ is a subgroup of $\operatorname{Frac}(R)$.
(2) The quotient $\operatorname{Frac}(R)/\operatorname{Prin}(R)$ is isomorphic to $\operatorname{Cl}(R)$.
(3) The following are equivalent.
   (a) R is a PID.
   (b) R is a UFD.
   (c) $\operatorname{Cl}(R) = (0)$.

EXERCISE 13.3.3. 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 13.3.4. Show that if R is a Dedekind domain, then $\operatorname{Pic}(R)$ and $\operatorname{Cl}(R)$ are isomorphic.

EXERCISE 13.3.5. 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 13.3.6. 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 13.3.7. 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 13.3.8. Suppose I and J are proper ideals in a Dedekind domain R such that $I + J = R$. Then there exists an isomorphism of R-modules $I \oplus J \cong R \oplus IJ$.

EXERCISE 13.3.9. 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 13.3.10. 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

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 13.2.3), hence reflexive. If F is a fractional ideal of R in K, then $F \subseteq (F^{-1})^{-1}$. By Lemma 13.2.2 (4), the assignment $\alpha \mapsto \ell_\alpha$ defines an isomorphism $F^{-1} \to \operatorname{Hom}_R(F,R)$. 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 12.3.4). Notice that $F^{-1} = R : F$.

LEMMA 13.4.1. *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 13.1.6, Lemma 13.1.7, Proposition 13.1.8, Lemma 13.1.9, and Proposition 13.1.10. (6): By Part (5) (a), $R : F^{-1}F = (R : F) : F^{-1} = (R : F) : (R : F)$. □

Let $\operatorname{Reflex}(R)$ 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 $\operatorname{Reflex}(R)$ by the formula $E * F = R : (R : EF)$. By Exercise 13.4.6, this operation turns $\operatorname{Reflex}(R)$ into an abelian monoid with identity R. If R is a noetherian normal integral domain, then Lemma 12.1.2 (3) implies that R is completely normal and Proposition 13.4.2 implies that $\operatorname{Reflex}(R)$ is an abelian group.

PROPOSITION 13.4.2. *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 12.1.1).*

PROOF. Assume $\operatorname{Reflex}(R)$ is an abelian group. Let I be a fractional ideal of R in K. By Exercise 13.4.5, it is enough to show $R = I : I$. Let $J = (I^{-1})^{-1}$. By Lemma 13.4.1 (3), J is a reflexive fractional ideal. By Lemma 13.4.1 (7), $J : J$ is a reflexive fractional ideal. By Exercise 13.4.3, $J : J$ 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 13.4.3,

$$R \subseteq I : I \subseteq I^{-1} : I^{-1} \subseteq J : J = R.$$

Conversely, if $I \in \operatorname{Reflex}(R)$, then so is I^{-1} by Lemma 13.4.1 (3). By Lemma 13.4.1 (6), $R : II^{-1} = I^{-1} : I^{-1} = R$. Then $R : (R : II^{-1}) = R$, so I^{-1} is the inverse of I in $\operatorname{Reflex}(R)$. □

LEMMA 13.4.3. *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 13.4.1 (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 13.4.1 (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 13.4.9, $R(a\alpha)^{-1} \cap R$ 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. □

THEOREM 13.4.4. *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 abelian group and $X_1(R)$ is a basis.*

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 13.4.3, 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 13.4.6 and Proposition 13.4.2 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 13.4.1 (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 2.1.22, 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 13.4.1, $I : P_1$ is a reflexive ideal in R. By Exercise 13.4.7, $I : P_1 = I * P_1^{-1}$. By Exercise 13.4.6, $I : P_1 = P_2 * \cdots * P_m = R : (R : (P_2 \cdots P_m))$ 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

$$I * Q_1 * \cdots * Q_n = P_1 * \cdots * P_m.$$

□

4.1. Exercises.

EXERCISE 13.4.1. 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 13.4.2. 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 13.4.3. 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 13.4.4. 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 13.4.5. 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 13.4.6. 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 13.4.7. 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 13.4.8. 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 13.4.9. 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 13.4.10. 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 13.4.11. 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 12.4.6.)

5. Reflexive Lattices over Regular Domains

In this section R denotes a noetherian regular integral domain with field of fractions K.

5.1. 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 13.5.8). The proof given here is essentially the original proof by Auslander and Goldman in [**4**].

THEOREM 13.5.1. *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 5.5.8, if M is projective, then M is reflexive. Assume M is a reflexive R-lattice. By Proposition 6.7.2, 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 12.2.9), and M is free by Proposition 13.1.4. Assume $\dim(R) = 2$. By Proposition 13.1.6, $M^* = R : M$ 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 $\operatorname{Hom}_R(\cdot, R)$ 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 13.1.6, 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

$$0 \to M \xrightarrow{\varepsilon^*} F_0^* \xrightarrow{d_1^*} F_1 \to N \to 0 \tag{13.3}$$

is exact. Since F_0 is free, so is F_0^* (Proposition 3.3.19). By Theorem 12.3.19, $\operatorname{coh.dim}(R) = \dim(R) = 2$. By Theorem 10.4.5, M is projective because it is the first syzygy of (13.3). □

PROPOSITION 13.5.2. *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* $\operatorname{Hom}_R(M, M)$ *is reflexive and* $\operatorname{Ext}^1_R(M, M) = 0$, *then $M = M^{**}$.*

PROOF. By Exercise 8.2.15, $\operatorname{Hom}_R(M,M) = \operatorname{Hom}_R(M,M)^{**}$ is torsion free. By Exercise 8.2.13, 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

$$0 \to M \xrightarrow{\nu} M^{**} \to C \to 0 \tag{13.4}$$

is an exact sequence. If $\dim(R) \leq 1$, then M is a finitely generated free R-module, hence is reflexive (Exercise 5.5.8). 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 8.2.14, to show $C = 0$, it suffices to show $\operatorname{Hom}_R(M,C) = 0$. The long exact sequence of Ext modules associated to (13.4) is

$$0 \to \operatorname{Hom}_R(M,M) \xrightarrow{\nu^*} \operatorname{Hom}_R(M,M^{**}) \to \operatorname{Hom}_R(M,C) \xrightarrow{\delta^0} \operatorname{Ext}^1_R(M,M) \to \dots \tag{13.5}$$

(Proposition 10.3.9). 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

$$\begin{tikzcd} \operatorname{Hom}_R(M,M) \arrow[r, "\nu^*"] \arrow[d, "="'] & \operatorname{Hom}_R(M,M^{**}) \\ \operatorname{Hom}_R(M,M)^{**} \arrow[r, "\alpha^*"] & (M^* \otimes_R M)^* \arrow[u, "\beta^*"'] \end{tikzcd} \tag{13.6}$$

commutes where α^* and β^* are the isomorphisms of Proposition 13.1.16. □

LEMMA 13.5.3. *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 6.6.8). By Nakayama's Lemma (Corollary 5.3.5), 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 $\mathfrak{m}$. □

LEMMA 13.5.4. *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

$$0 \to \operatorname{Hom}_R(M,N) \xrightarrow{\mathrm{H}(\ell_x)} \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(M,N/xN) \to \\ \operatorname{Ext}^1_R(M,N) \xrightarrow{\mathrm{H}^1(\ell_x)} \operatorname{Ext}^1_R(M,N) \to \dots \tag{13.7}$$

(Proposition 10.3.9). 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 10.3.10 (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 8.2.5, 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 12.3.2, $\mathfrak{m}$ 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 (13.7). Since $\mathfrak{m} \in \operatorname{Assoc}_R(K)$, by Exercise 12.3.2, $\operatorname{depth}(K) = 0$. Write H for $\operatorname{Hom}_R(M,N)$ and Q for $\operatorname{Hom}_R(M,N/xN)$. The short exact sequence

$$0 \to H/xH \to Q \to C \to 0 \tag{13.8}$$

of R-modules gives rise to the long exact sequence of the modules $\operatorname{Tor}^R_i(\cdot,k)$

$$\dots \to \operatorname{Tor}_{n+1}(Q,k) \to \operatorname{Tor}_{n+1}(K,k) \to \operatorname{Tor}_n(H/xH,k) \\ \to \operatorname{Tor}_n(Q,k) \to \operatorname{Tor}_n(K,k) \to \operatorname{Tor}_{n-1}(H/xH,k) \to \dots \tag{13.9}$$

(Lemma 10.3.2). 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 10.4.10, we have $\operatorname{Tor}_i(H/xH,k) = 0$ for $i \ge 2$. Because $n - 1 \ge 2$, the sequence (13.9) produces two isomorphisms

$$\begin{aligned} \operatorname{Tor}_{n+1}(Q,k) &\cong \operatorname{Tor}_{n+1}(K,k) \\ \operatorname{Tor}_n(Q,k) &\cong \operatorname{Tor}_n(K,k) \end{aligned} \tag{13.10}$$

Since R is a regular local ring with dimension n, by Proposition 12.3.27, $\operatorname{proj.dim}(K) = \dim(R) - \operatorname{depth}(K) = n$. By Proposition 10.4.10, we have $\operatorname{Tor}_{n+1}(K,k) = 0$ and $\operatorname{Tor}_n(K,k)$ is nonzero. By Eq. (13.10) and Proposition 10.4.10, $\operatorname{proj.dim}(Q) = n$. By Proposition 12.3.27, $\operatorname{depth}(Q) = \operatorname{depth}(\operatorname{Hom}_R(M,N/xN) = 0$. This is a contradiction to Lemma 13.5.3 (2). □

LEMMA 13.5.5. *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 13.5.1, and $\operatorname{Ext}^1_R(M,M) = 0$, by Proposition 10.3.9. 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 12.3.26, $R_\mathfrak{p}$ is a regular local ring and $\dim(R_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}) < n$. Applying Proposition 6.5.7, 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 10.3.10 (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 8.2.6, $\mathfrak{m}$ is the only associated prime of $\operatorname{Ext}^1(M,M)$. By Exercise 12.3.2, this implies $\operatorname{depth}(\operatorname{Ext}^1_R(M,M)) = 0$, which contradicts Lemma 13.5.4. □

LEMMA 13.5.6. *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 10.4.5 and Exercise 10.4.5, 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 10.2.11, 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 5.3.2), $H(d_n)$ is not onto. □

PROPOSITION 13.5.7. *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 12.3.27 and Lemma 13.5.3 (or Example 13.1.3 (2), Exercise 13.1.2 and Theorem 13.5.1).

(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 12.3.27, $\operatorname{depth}(R) = \dim(R) = 3$. Lemma 13.5.3 applied to $M = M^{**}$ gives $\operatorname{depth}(M) \geq 2$. By Proposition 12.3.27, $\operatorname{proj.dim}_R(M) \leq 1$. By Lemma 13.5.5, $\operatorname{Ext}^1_R(M,M) = 0$. Lemma 13.5.6 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 12.3.19, $\bar{R} = R/aR$ 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 10.3.9). By Lemma 13.5.5, $\operatorname{Ext}^1_R(M,M) = 0$, 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 5.5.10 (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 8.2.13, $\bar{M}$ is torsion free. By Proposition 13.1.16,

$$\operatorname{Hom}_{\bar{R}}(\bar{M},\bar{M}) = \operatorname{Hom}_{\bar{R}}(\bar{M},\bar{M})^{**} \cong \operatorname{Hom}_{\bar{R}}(\bar{M}^*,\bar{M}^*)$$

is $\bar{R}$-free. By Lemma 13.1.9, $\bar{M}^*$ 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 13.5.4, that the statement:

$$\text{If } \operatorname{Ext}^i_{\bar{R}}(\bar{M},\bar{R}) \neq 0, \text{ then } \operatorname{depth}(\operatorname{Ext}^i_{\bar{R}}(\bar{M},\bar{R})) > 0. \tag{13.11}$$

is true. The Adjoint Isomorphism (Lemma 10.3.11) induces isomorphisms

$$\operatorname{Ext}^i_{\bar{R}}(\bar{M},\bar{R}) \cong \operatorname{Ext}^i_R(M,\bar{R}) \tag{13.12}$$

for all $i \geq 0$. Therefore, the statement:

$$\text{If } \operatorname{Ext}^i_R(M,\bar{R}) \neq 0, \text{ then } \operatorname{depth}(\operatorname{Ext}^i_R(M,\bar{R})) > 0. \tag{13.13}$$

is equivalent to (13.11). The short exact sequence

$$0 \to R \xrightarrow{\ell_a} R \to \bar{R} \to 0 \tag{13.14}$$

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 10.3.9). Let $\mathfrak{p} \in \operatorname{Spec} R - \{\mathfrak{m}\}$. By Lemma 10.3.10,

$$\operatorname{Ext}^1_R(M,R)_{\mathfrak{p}} \cong \operatorname{Ext}^1_{R_{\mathfrak{p}}}(M_{\mathfrak{p}},R_{\mathfrak{p}}). \tag{13.15}$$

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 10.3.9, both groups in (13.15) 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 10.3.10 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 8.2.6 that $\mathfrak{m}$ is the only associated prime of $\operatorname{Ext}^1_R(M,\bar{R})$. By Exercise 12.3.2, this implies $\operatorname{depth}(\operatorname{Ext}^1_R(M,\bar{R})) = 0$, which is a contradiction to the statement in (13.13). 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 (13.12), $\operatorname{Hom}_{\bar{R}}(\bar{M},\bar{R}) \cong \operatorname{Hom}_R(M,\bar{R})$. 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 (13.14)), hence $\operatorname{proj.dim}_R(M^*/aM^*) = 1$. By Proposition 10.4.10, $\operatorname{proj.dim}_R(M^*) = 0$, hence M^* is R-free. Therefore, $M = M^{**}$ is R-free. □

THEOREM 13.5.8. *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 12.3.26). By Proposition 6.5.7 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 13.5.7, $M_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$-free. □

5.2. The Class Group of a Regular Domain.

THEOREM 13.5.9. *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.*

PROOF. (1): Let F be a reflexive fractional ideal of R in K. It follows from Exercise 13.4.7 that $F : F = R$ is free of rank one. By Theorem 13.5.8, F is projective. The equality $\operatorname{Pic}(R) = \operatorname{Cl}(R)$ follows from Exercise 13.4.10.

(2): For any local ring the Picard group is trivial. By (1), the class group, $\operatorname{Cl}(R)$, is trivial. By Corollary 12.4.12, R is a UFD. □

EXAMPLE 13.5.10. In this example we show how to construct a regular integral domain R such that $\operatorname{Pic}(R)$ 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 9.4.1). 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) $\operatorname{Pic}(R) = \operatorname{Cl}(R) \cong \mathbb{Z}/n$.

(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

$$\frac{x^h y^i z^j}{f^d} \frac{f^d}{y^{h+i} z^j} = \frac{x^h}{y^h} \tag{13.16}$$

shows $\mathfrak{p}R_{\mathfrak{p}}$ is generated by x/y. This also proves that $\operatorname{ht}(\mathfrak{p}) = 1$. 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 (13.16) we compute

$$\nu_{\mathfrak{p}}(x^n f^{-1}) = n. \tag{13.17}$$

Consider the localized ring $R[fx^{-n}]$. Given $p \in S_{dn}$ we multiply and divide by $(x^n f^{-1})^d$ to get

$$\begin{aligned} pf^{-d} &= (px^{-dn}f^d)(fx^{-n})^{-d}f^{-d} \\ &= p(1,y/x,z/x)\left(f(1,y/x,z/x)\right)^{-d}. \end{aligned}$$

Therefore, the assignments $x \mapsto 1$, $y \mapsto u$, $z \mapsto v$ induce an isomorphism of k-algebras

$$R[fx^{-n}] \to k[u,v][(f(1,u,v))^{-1}]. \tag{13.18}$$

The homomorphism in (13.18) is usually specified by saying "dehomogenize with respect to x". Notice that the ring on the right hand side of (13.18) is a finitely generated k-algebra, a regular integral domain, and has Krull dimension two. By the same argument used in (13.18), 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 $x^hy^iz^j$ where at least one of h,i,j is greater than n. Therefore, $1 = f^Nf^{-N}$ is in the ideal of R generated by $x^nf^{-1}, y^nf^{-1}, z^nf^{-1}$. This shows that $R[fx^{-n}] \oplus R[fy^{-n}] \oplus R[fz^{-n}]$ is a faithfully flat extension of R (Exercise 6.5.13) By Proposition 6.5.12, 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 12.4.13) to the ring R, the sequence

$$1 \to R^* \to (R[fx^{-n}])^* \xrightarrow{\text{Div}} \mathbb{Z}\mathfrak{p} \to \operatorname{Cl}(R) \to \operatorname{Cl}(R[fx^{-n}]) \to 0 \tag{13.19}$$

is exact. By the isomorphism in (13.18), we see that $R[fx^{-n}]$ is a UFD. Hence $\operatorname{Cl}(R[fx^{-n}])$ is equal to (0) by Corollary 12.4.12. Using (13.18) and the fact that $k[u,v]$ is a UFD, we see that

$$(R[fx^{-n}])^* = k^* \times \langle x^nf^{-1}\rangle$$

is an internal direct sum. This and (13.17) shows that the image of Div in (13.19) is $n\mathbb{Z}\mathfrak{p}$. Therefore, $\operatorname{Cl}(R)$ is generated by $\mathfrak{p}$ and has order n. Part (2) follows from Theorem 13.5.9, and the reader is asked to prove Part (3) in Exercise 13.5.1.

5.3. Exercises.

EXERCISE 13.5.1. If R is the ring of Example 13.5.10, prove the following.

(1) $R^* = k^*$.
(2) $\mathfrak{p}^n$ is equal to the principal ideal generated by x^nf^{-1}.

EXERCISE 13.5.2. 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 $T = k[x,y,z]/(z^n - x^{n-1}y + 1)$, 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 $\operatorname{Div} x = Q_1 + \cdots + Q_n$.
(5) $\operatorname{Cl}(T) = \mathbb{Z}Q_1 \oplus \cdots \oplus \mathbb{Z}Q_{n-1}$.

EXERCISE 13.5.3. 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 $\operatorname{Div}(T)$ we have $\operatorname{Div} x = P_1 + \dots + P_n$, and $\operatorname{Div} \ell_i = (n-1)P_i$.

(5) $\operatorname{Cl}(T)$ 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 2.5.17). Let $G = \langle \sigma \rangle$. Then G is a cyclic group of order n which acts on $\operatorname{Cl}(T)$ by $\sigma P_1 = -P_1 - P_2 - \dots - P_{n-1}$, $\sigma P_2 = P_1, \dots, \sigma P_{n-1} = P_{n-2}$.

6. The Class Group of a Graded Ring

Most of the results in this section were originally published in [**26**]. For additional results on this subject, the interested reader is referred to [**26**], [**12**, § 10], and [**23**, § B.II.1]. Throughout this section all rings are commutative. The reader is referred to Section 9.4 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 13.6.1. *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
$$\alpha_0 t^r + \alpha_1 t^{r-1} + \dots + \alpha_{r-1} t + \alpha_r = 0 \tag{13.20}$$

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 (13.20) by yw^r, we get

$$b_0 a^r + b_1 w a^{r-1} + \cdots + b_{r-1} w^{r-1} a + b_r w^r = 0 \tag{13.21}$$

which is a relation in R. The left hand side of (13.21) is a sum of homogeneous elements. Since $\deg a^r > \deg w a^{r-1} > \cdots > \deg w^{r-1} a > \deg w^r$, no two terms in (13.21) 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 13.6.2. *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 13.6.1, $W^{-1}R = K_0[t, t^{-1}]$. Since $K_0[t]$ is factorial, so is the localization $W^{-1}R = K_0[t, t^{-1}]$. By Exercise 12.4.6, $\operatorname{Cl}(R)$ 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 11.1.2 (4). □

LEMMA 13.6.3. *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 13.2.1, 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 13.6.1, 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 13.1.6, 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 13.6.1, 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 13.6.4. *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 $\gamma \colon \mathrm{Cl}(R) \to \mathrm{Cl}(R_{\mathfrak{m}})$ is onto, by Exercise 12.4.6. 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 13.6.2, 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 13.6.3 (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 13.6.3 (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 6.4.2, $I_{\mathfrak{m}}$ 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 $I = \xi R$. □

CHAPTER 14

Zariski's Main Theorem

1. Zariski's Main Theorem

The proof we give is from [**24**, Chapter IV]. Throughout this section all rings are commutative.

1.1. Quasi-finite Algebras.

PROPOSITION 14.1.1. *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 7.4.4. Since B_f has only one prime ideal, B_f is local with maximal ideal qB_f. By Exercise 9.2.5, 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 6.1.7, 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 14.1.2. *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 14.1.1 to the algebra B/pB over k_p. □

DEFINITION 14.1.3. If A and B are as in Proposition 14.1.2 and either (1) or (2) is satisfied, then we say B is *quasi-finite* over A at q. If this is true for all $q \in \operatorname{Spec} B$, then we say B is *quasi-finite* over A.

PROPOSITION 14.1.4. *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 6.6.12) and semilocal (Proposition 7.4.3). By Theorem 7.4.6, the natural homomorphism $B \to \bigoplus B_q$ is an isomorphism, where q runs through $\operatorname{Spec} B$. Each B_q is finite dimensional over k. By Proposition 14.1.1, 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 14.1.1. Therefore B is finite dimensional over k. □

LEMMA 14.1.5. *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. □

EXAMPLE 14.1.6. (1) If B is a commutative A-algebra that is finitely generated as an A-module, then B is quasi-finite over A.

(2) If $f \in A$, then A_f is quasi-finite over A.

1.2. Zariski's Main Theorem.

LEMMA 14.1.7. *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

$$b^n + \frac{f a_{n-1}}{y_{n-1}} b^{n-1} + \cdots + \frac{f^n a_0}{y_0}.$$

Let $y = y_0 \cdots y_{n-1}$ and multiply both sides by y^n to get

$$\begin{aligned} y^n b^n + \frac{f y a_{n-1}}{y_{n-1}} y^{n-1} b^{n-1} + \cdots + \frac{f^n y^n a_0}{y_0} &= 0 \\ (yb)^n + \alpha_{n-1} (yb)^{n-1} + \cdots + \alpha_0 &= 0 \end{aligned}$$

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 14.1.3, $\bar{x}$ 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 9.5.4. 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 $A = B$. □

LEMMA 14.1.8. *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 9.5.4 (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 9.5.4 (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 9.5.4 (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 9.5.4 (2), $\tilde{q}_1 \cap B \subsetneq q$ so q is not a minimal prime lying over p. □

LEMMA 14.1.9. *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 3.1.4).

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 $y \in A$. □

LEMMA 14.1.10. *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 $\alpha/\beta \in c_p$. □

LEMMA 14.1.11. *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 14.1.7 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 14.1.10 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 9.5.4, 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 14.1.9 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 14.1.8, so Case 2 cannot occur. □

PROPOSITION 14.1.12. *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 14.1.5, B is quasi-finite over $\tilde{A}$ at q. We are in the setting of Lemma 14.1.11, 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 $A_p = B_p$. □

THEOREM 14.1.13. *(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 14.1.5, B is quasi-finite over $\tilde{A}$ at q. Let $\tilde{p} = q \cap \tilde{A}$. By Proposition 14.1.12, $\tilde{A}_{\tilde{p}} = B_{\tilde{p}}$. 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. □

COROLLARY 14.1.14. *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 14.1.13 (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 14.1.6, $(A_\alpha)_f$ is quasi-finite over A. The open set $V = \operatorname{Spec} B_f$ is a neighborhood of q. □

EXAMPLE 14.1.15. 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 6.4.4). Then C is quasi-finite over A. The next corollary says every quasi-finite homomorphism factors in this way.

COROLLARY 14.1.16. *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 14.1.14 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 14.1.14, 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. □

1.3. Exercises.

EXERCISE 14.1.1. (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 14.1.2. If S is a commutative finitely generated separable R-algebra, then S is quasi-finite over R.

EXERCISE 14.1.3. 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.)

Acronyms

ACC	Ascending Chain Condition
DCC	Descending Chain Condition
GCD	Greatest Common Divisor
PID	Principal Ideal Domain
UFD	Unique Factorization Domain
DVR	Discrete Valuation Ring

Bibliography

[1] A. A. Albert, *Cyclic fields of degree p^n over F of characteristic p*, Bull. Amer. Math. Soc. **40** (1934), no. 8, 625–631. MR 1562919

[2] Bernice Auslander, *The Brauer group of a ringed space*, J. Algebra **4** (1966), 220–273. MR 0199213 (33 #7362)

[3] 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)

[4] Maurice Auslander and Oscar Goldman, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1–24. MR 0117252 (22 #8034)

[5] Hyman Bass, *Algebraic K-theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR 0249491 (40 #2736)

[6] 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)

[7] Frank DeMeyer, *Another proof of the fundamental theorem of Galois theory*, Amer. Math. Monthly **75** (1968), 720–724. MR 0244208 (39 #5525)

[8] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons Inc., Hoboken, NJ, 2004. MR 2286236 (2007h:00003)

[9] 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)

[10] Timothy J. Ford, *Separable algebras*, Graduate Studies in Mathematics, vol. 183, American Mathematical Society, Providence, RI, 2017. MR 3618889

[11] 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

[12] Robert M. Fossum, *The divisor class group of a Krull domain*, Springer-Verlag, New York, 1973. MR 0382254 (52 #3139)

[13] A. Grothendieck, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11, 167. MR 0163910 (29 #1209)

[14] ______, *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)

[15] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. MR 0463157 (57 #3116)

[16] John L. Kelley, *General topology*, Springer-Verlag, New York-Berlin, 1975, Reprint of the 1955 edition [Van Nostrand, Toronto, Ont.], Graduate Texts in Mathematics, No. 27. MR 0370454 (51 #6681)

[17] T. Y. Lam, *Serre's problem on projective modules*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006. MR 2235330

[18] 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)

[19] 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.

[20] Hideyuki Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980. MR 575344 (82i:13003)

[21] 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)

[22] 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)

[23] 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

[24] Michel Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Mathematics, Vol. 169, Springer-Verlag, Berlin-New York, 1970. MR 0277519 (43 #3252)

[25] 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)

[26] 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